Faster Payments QIAT

Proposer:

Kalypton Group Limited and The Electronic Check Clearing House Organization

February 21, 2017

TABLE OF CONTENTS

In Pursuit of a Better Payment System

Faster Payments Task Force

Faster Payments Task Force Proposal

Tereon Real-time Payments

April 30th, 2016

Submitted by: Alun Thomas, Kalypton Group Limited
Jenny Johnson, The Electronic Check Clearing House Organization

CONTENTS

FIGURES

EXECUTIVE SUMMARY

Tereon, Kalypton's electronic payments solution, takes its name from the Koine Greek verb for protecting or safeguarding value, a word that is also the root of the word for Treasure. The root of the name Tereon aptly describes the design ethos behind the solution.

In the payments industry today, there seems to be an acceptance in the work to date that faster or real-time payments offer value in specific use cases only. The consensus further seems to be that speed can be at the expense of security and cost penalties. This is not so different to the industry perception that there is a trade-off between security and usability.

Kalypton believes that this trade-off between security and usability is simply not applicable anymore. Existing payment schemes were developed when the communications landscape and the availability of IT tools was very, very different to that of today. Using the "clean sheet of paper" approach, Kalypton has developed, real-time "rails", a toolkit, and a comprehensive baseline set of 31 services that offer benefits in terms of speed and cost savings and security improvements and greater usability. There is no need for any more trade-offs. There is simply "then" and "now".

Tereon consists of a central core, which is bank grade and sets a new standard against all of the resilience and security and compliance measures. That bank grade core is fully integrated into the banking system. On top of that sits a skin that is readily configurable to a full range of devices and use cases. There is no longer a dichotomy between security and usability, because both perspectives can now be fully reconciled.

Ultimately banks and technology companies are all in the IT services business. The CEO of BBVA, Francisco Gonzalez is a software engineer and he said "In the future BBVA will be a software business"[1]. Amish Bhihani, Chief Information Risk Officer of JP Morgan observed "JP Morgan has more software development engineers than Google"[2]. Everyone has been waiting for a set of "rails" and a software toolset that leverages modern tools to support all use cases and to meet the security and compliance requirements unique to payments.

Tereon is an extremely powerful and flexible transaction processing tool. It can be configured to support all transaction types. The common factor is that the transaction is completed in a single real-time session and moves funds, or bank money, from account to account. As this proposal will show, these accounts do not need to be restricted just to bank accounts; accounts with non-bank service providers or one-time use accounts can also be supported just as easily in order to

[1] https://www.finextra.com/news/fullstory.aspx?newsitemid=27080

[2] http://wallstreetonparade.com/2014/04/jamie-dimon-jpmorgan-employs-30000-programmers/

achieve the policy goals for financial inclusion. Tereon was designed to service both the banked and the unbanked. Facilitating financial inclusion for all was a core design aim for Tereon. For preference, Kalypton deploys Tereon to process fiat money rather than e-money or cryptocurrency.

Tereon consists of payment rails and services and the ability to develop new services where –

- the rails are secure real-time sessions established over the Internet or over the top of mobile data networks;
- the services supported from day one can and will include all of the use cases that the Faster Payments Task Force envisaged; and
- every Tereon server comes with a toolkit to develop new payment services, supporting ongoing innovation and innovation based competition between payment service providers.

Tereon supports 31 baseline functions or use cases. Some of these involve a "push" payment, while involve a "pull". The distinction is that where the initiator of a transaction also initiates a payment, then that is a "push" transaction. Where the initiator does not initiate a payment, then the transaction is a "pull" transaction. The discussion at the start of Part A, Section 2 on page 59 discusses this in detail.

Tereon is not based on the blockchain or on other legacy systems. It does not rely on a central payments hub. It does not discriminate between the banked or the unbanked. Tereon was designed from the ground up to provide genuine real-time payment and settlement system that could transact any value, support virtually any use case, and provide a full set of services to the banks and the unbanked without discriminating between them. Regulation and legislation will determine the services that the banked and the unbanked can access, not the technology.

Kalypton is in the process of securing patents for a number of ground-breaking innovations which explain how it has been able to deliver such a simple and powerful solution. As requested, Kalypton does not reveal any confidential information in this proposal. For example, Tereon incorporates into its audit processes a solution that delivers all of the anticipated benefits of the blockchain but without the delays and processing overheads that blockchain entails. This document does not explain how the audit process does that as the technology is subject to a patent application.

In parallel with the QIAT evaluation process, Kalypton will be implementing its first commercial deployment in Central America that will demonstrate that these capabilities are real and immediately available.

The USA is a uniquely complex and fragmented market. Many incumbents are understandably eager to protect their revenue streams and Kalypton sees some challenges in achieving the goal of ubiquity. To the degree that these challenges can be minimized through technology, Kalypton has done so. Tereon is uniquely scalable (processing millions of transactions per second on commodity servers), can be virtualized or run on any hardware and is easily integrated. Kalypton is delighted to be working closely with ECCHO, who understand many of these challenges.

Kalypton notes that the Faster Payments Task Force envisages work groups to address, inter alia, the governance model and the post-paper implementation plan. Their work will be critical. Kalypton hopes to have the opportunity to work closely with the Task Force on these matters.

ECCHO will manage the effort to implement the legal framework for Faster Payments meeting the Legal Criteria developed in the Faster Payments Legal Work Group—which was chaired by ECCHO. ECCHO's experience is unrivalled—building a new rules scheme from concept to rapid adoption in a transitioning, complex, multi-operator, many-vendor environment. For Faster Payments, ECCHO proposes to use the ECCHO methodology that combines teleconferences with in-person meetings, using technology to combine the physical with the virtual. ECCHO's approach enables creation of various groups to facilitate the communication and education within the subcommittees, operations committee and Board. ECCHO's network will be a vehicle to communicate with consumers to deliver education as well as seek input on important issues.

Appendix A sets out further information about Kalypton.

Appendix B sets out further information about ECCHO.

Alun Thomas, Kalypton Group Limited
alun.thomas@kalypton.com

Jenny Johnson, The Electronic Check Clearing House Organization
jjohnson@eccho.org

Copyright Statement

USE CASE COVERAGE

Supported Use Case Coverage Summary

The table below identifies some of the use cases that Tereon will support for payments.

Supported use case coverage summary				
Use case	**Supported (Y/N)**	**Cross-border (Y/N)**	**Examples of payments supported**	**Notes**
Business to Business (B2B)	Y	Y	The solution supports business and governments to make all forms of payments, from instantaneous micropayments, just-in-time, and deferred payments through to deferred invoices, and other ad hoc payments of any value.	This supports ad hoc transfers or payments as well as scheduled transfers or payments. Tereon imposes no upper or lower limit of the value of a transfer or payment.
Business to Person (B2P)	Y	Y	This solution supports business and governments to make forms of payments from employment wages, pensions, and social security payments through to refunds, insurance claims, and other ad hoc payments of any value.	This supports ad hoc transfers or payments as well as scheduled transfers or payments. Tereon imposes no upper or lower limit of the value of a transfer or payment.
Person to Business (P2B)	Y	Y	The solution supports all forms of payments from a consumer to a business, from standard merchant and bill payments, through to deferred, emergency payments and other ad hoc payments of any value.	This supports ad hoc transfers or payments as well as scheduled transfers or payments. Tereon imposes no upper or lower limit of the value of a transfer or payment.
Person to Person (P2P)	Y	Y	The solution supports all forms of peer-to-peer transfers or payments of any value, from transfers between friends or family members through to remittances to individuals in other countries.	This supports ad hoc transfers or payments as well as scheduled transfers or payments. Tereon imposes no upper or lower limit of the value of a transfer or payment.

Cross-border Use Case Coverage

The table below identifies the use cases that support cross-border, and the jurisdictions and systems with which the solution can interoperate.

Cross-border use case coverage		
Use Case	**Non-US Corridor(s) and Systems**	**Notes**
Business to Business (B2B)	Global	Tereon can interface with most third-party payments systems, and can operate in any non-embargoed territory.
Business to Person (B2P)	Global	Tereon can interface with most third-party payments systems, and can operate in any non-embargoed territory.
Person to Business (P2B)	Global	Tereon can interface with most third-party payments systems, and can operate in any non-embargoed territory.
Person to Person (P2P)	Global	Tereon can interface with most third-party payments systems, and can operate in any non-embargoed territory.

Proposal Assumptions

1. ECCHO will be the main rule-making body. Tereon can, however, be configured to interoperate with multiple rule making bodies in order to promote competition.
2. One or more systems integrators will provide the technology infrastructure, that is the data centers, network connections, and end-point hardware in order to promote competition. Tereon does not seek to restrict either consumer choice or the providers' choices as to what hardware or network they use.
3. One or more consultancies will provide services to potential providers to enable those providers to design and implement their services that they wish to offer to their customers.
4. One or more third-parties will design and offer value-added services that operate on top of and alongside the baseline services on the Tereon "rails".
5. Kalypton may or may not be the real-time payments scheme operator. Kalypton will be the main technology provider and will fully support the scheme operator if that is the preference.
6. Individual payment service providers may or may not be banks, subject to regulatory requirements. These providers may install a Tereon server as physical equipment in their environment as a "plug and play" appliance or they may have a dedicated virtual server at a multi-user service provider, again subject to regulation.
7. It is essential that there is access to APIs to connect Tereon to banks' and other PSPs' existing core systems. Kalypton assumes that the providers of these core systems will provide those APIs.
8. For ease of evaluation and comparison with other proposals to the QIAT, Kalypton has followed closely the established template, even though the solution, Tereon, is much more flexible in terms of use cases and process flows than the template implies.
9. The Federal Reserve System has not in any way committed to provide any of the services referenced in this document to Kalypton, and Kalypton makes no assumptions that the Federal Reserve System will do so.

PART A: DETAILED END-TO-END PAYMENTS FLOW DESCRIPTION

Part A, Section 1: Solution Description

Tereon is designed to provide real-time clearing and settlement processes. In order to support real-time payments, Tereon is usually configured to follow the payment lifecycle illustrated below, where settlement comes immediately after clearing and before receipt.

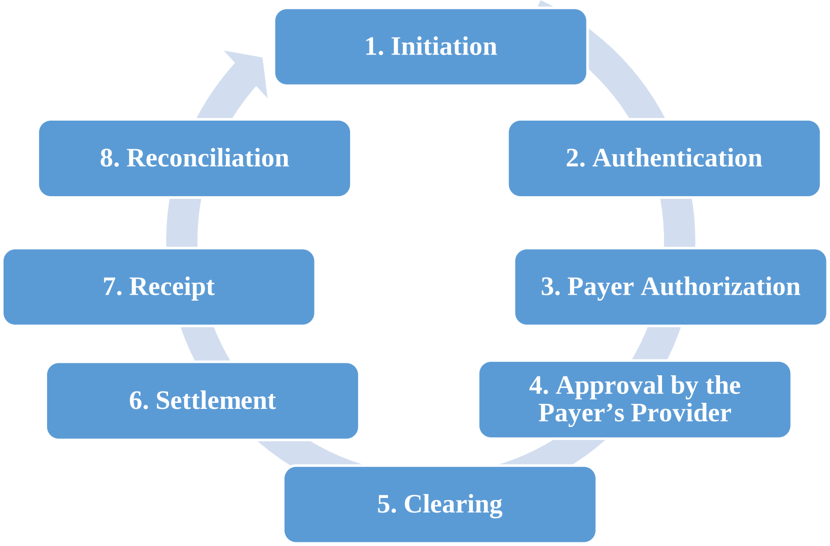


Figure 1 - Payment lifecycles for Tereon

There are some circumstances, where this configuration is not appropriate, such as a cross-border multi-currency payment that may take time to settle. In such a case, Tereon can operate in a mixed mode or mixed cycle configuration, where it supports settlement both pre- and post-receipt, depending on the payment or transaction type.

Tereon can implement multiple configurations to support the requirements of specific payments use cases where necessary. Tereon's configuration for a particular use case can be amended even after it has been rolled-out and implemented as payment rules, legislation, or market needs evolve. Tereon can, therefore, allow a payments network to transition from a lifecycle, where settlement occurs sometime after receipt, to the lifecycle where payments occur in real-time.

In reality, a Tereon payments lifecycle has nine stages, where the devices must first authenticate themselves to the system before a user can initiate a payment. This must happen at least once (when a device is first activated) and then at predefined intervals whilst that device remains active. This document will discuss this pre-authentication as part of stage 2, even though it occurs before stage 1, as the method of authentication prior to initiation is closely related to the method of authentication post initiation.

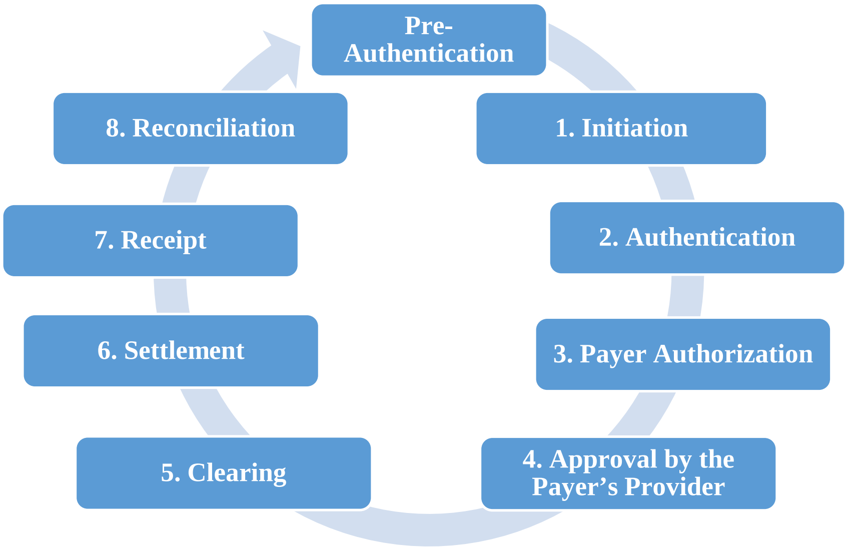


Figure 2 - Lifecycles with pre-authentication

For the purposes of this proposal, the description of Tereon in this part A will follow the lifecycle that represents real-time payments and settlement, where payments are settled before receipt. Figure 2 lists the order of those numbered lifecycle stages.

1. Initiation

The flow diagram below illustrates an example configuration for Tereon that illustrates an example of a P2B payment. Part A, Section 2, which starts on page 59 sets out a walk-through for this and a few other example use cases.

Tereon defines users as consumers or merchants, depending on their roles within a particular payments use case. In the diagram below, the user on the left is a merchant as she is taking payments for goods or services. The other user is a consumer, as she is consuming those goods or services. Immediately, it becomes apparent that the consumer can be an individual or a business. The consumer here is simply the end user of the good or service provided by the merchant. Both have bank accounts with their respective banks.

In the figure below, the gray lines illustrate the information and communication flows for transactions that need to involve a separate clearing or settlement house (the term "*Clearing House*" in this document is generic and does not refer to the organization called Clearing House or imply that Clearing House is working or will work with the solution). One such transaction might be check processing. The gray lines also illustrate additional third-party valued added services, such as a CRM service. Tereon does not need a central payment hub.

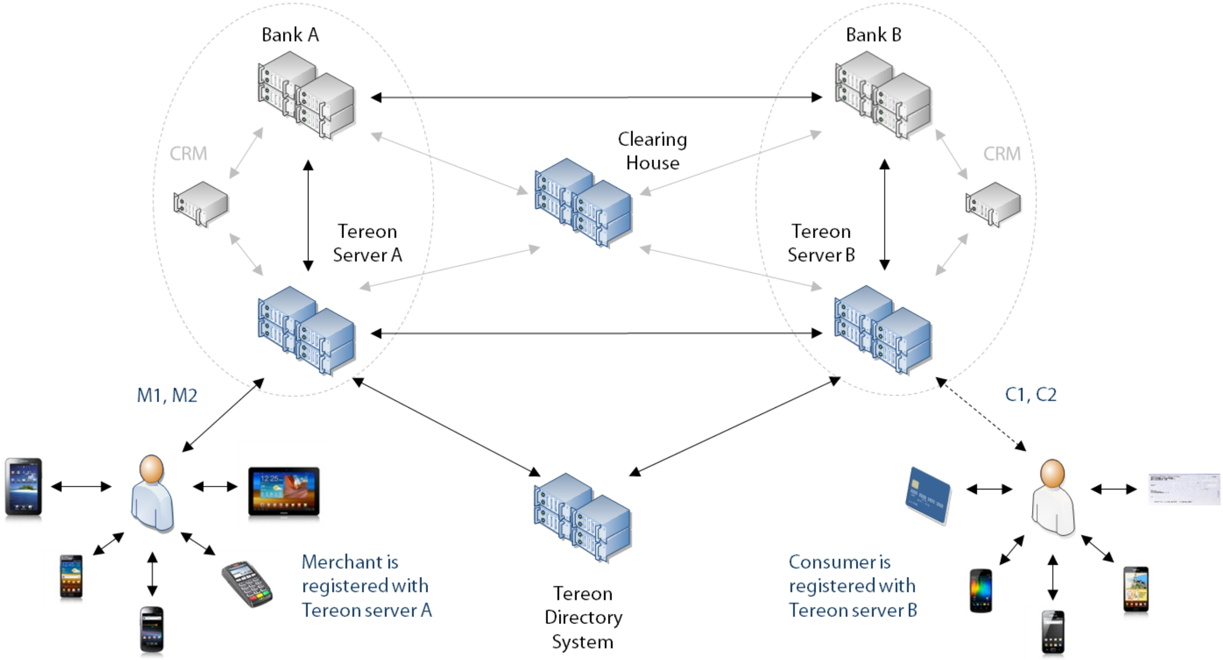


Figure 3 - Example configuration with two bank customers

Figure 3 also illustrates the fact that each service can be provided by a different provider. Bank A operates Tereon server A, and bank B operates Tereon server B. Third-parties, or the providers themselves can provide value added services, such as CRM services, marketing services, or add new functions and services. The different providers can connect to each other via the communications protocols provided by Tereon. They discover and validate each other via the directory system, which is a mesh of servers that link users to services and servers, and the licensing system (not illustrated for the sake of simplicity. The structure of the licensing service is similar to that of the look-up service).

Tereon facilitates payments to and from all types of accounts. Though the diagram above presupposes that the users are bank customers, users do not need to be banked. In the diagram below, the consumer is not banked. Instead, the consumer has an account with service provider B. Service provider B is not a bank. It operates a ledger with individual “accounts” for each of its customers. However, the funds to which the ledger refers are held in one or more control accounts in bank B. This ensures therefore, that the funds are always maintained within the existing banking system.

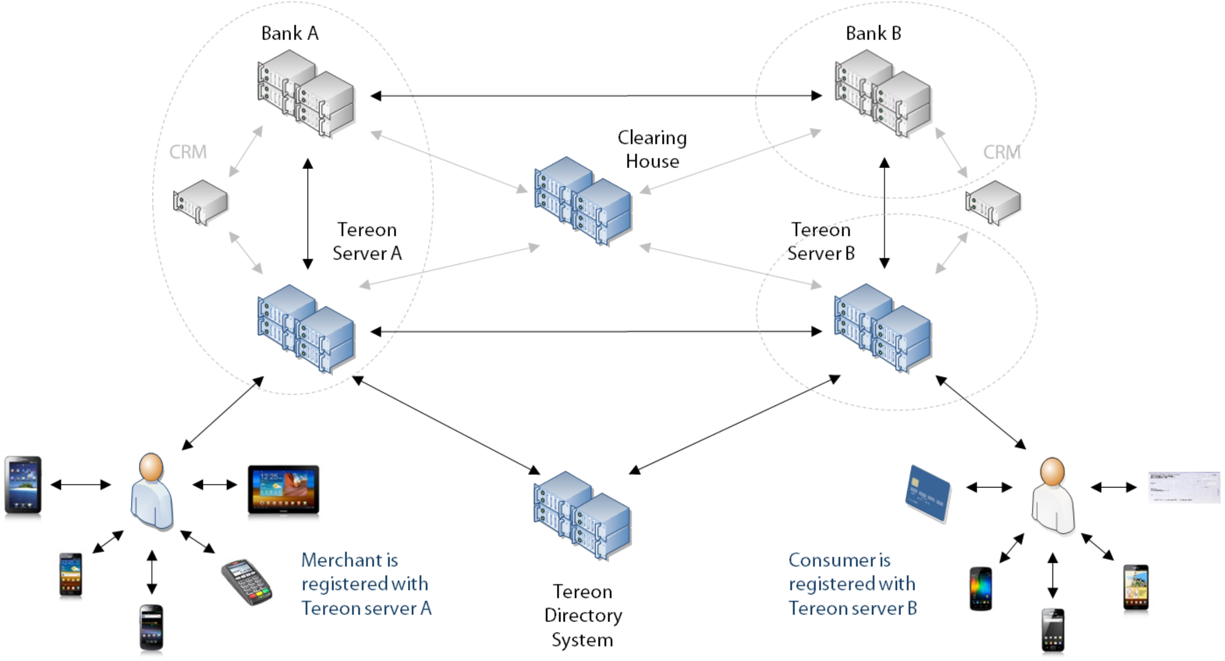

Bank A
Bank B
CRM
CRM
Clearing House
Tereon Server A
Tereon Server B
Merchant is registered with Tereon server A
Tereon Directory System
Consumer is registered with Tereon server B

Figure 4 - Example configuration with one banked and one unbanked user

Figure 4 above also illustrates a third-party providing the CRM service to the provider of the Tereon server B, and to bank B, while bank A provides that service itself. The consumers of those services might be the providers themselves, or they might be some of the users. For

example, the merchant may use the service to target offers to certain consumers. They can do this, however, without needing to know any of that consumer's personal data, as briefly discussed later on page 34.

Tereon can go further and operate in an environment where neither user participating in a transaction is a bank customer. Tereon will simply ensure that all funds and funds transfers operate within the regulated banking environment to ensure that the funds are protected and regulated. This is not illustrated here, but it is easy to visualize. Figure 4 would change to show each of bank A and Tereon server A within a separate ellipse. Tereon's design simply means that any provider can connect to any other provider so long as those providers are licensed and authorized to use the technology; the users of those providers can transact with each other.

Tereon supports transfers or payments from one user to another. As mentioned above, Tereon categorizes these users depending on the payment or transaction that they are entering into. In any transaction there must be a transferor and a recipient. Thus in a P2P transaction, both users are consumers, but one is a transferor and one is a recipient. In a B2B transaction, both users are merchants, but one is a transferor or payer and one is a recipient. In a P2B transaction, the transferor or payer is a consumer, while the merchant is the recipient. In a B2P transaction, the merchant is the transferor or payer, and the consumer is the recipient. In this proposal, the term merchant is used to describe any actor that is not a consumer. Thus a government agency distributing social security funds to recipients would be classed as a "merchant" for the purpose of this document.

In Tereon, a user must initiate a transaction. That user may not be the same as the user who initiates a transfer or payment. In Tereon a transaction includes the transfer or payment, but the transfer or payment does not include the transaction. The default position is that in a –

- P2P or a B2P transaction, the transferor or payer initiates the transaction and initiates the transfer or payment that the recipient will receive;
- B2B or a P2B transaction, the recipient initiates the transaction, but the transferor or payer initiates the transfer or payment that the transferor or payer will make.

A couple of examples will make this clear:

- In a peer-to-peer transfer, the transferor will initiate the transaction by selecting the transaction type, and then entering or selecting the recipient and the amount that she wishes to transfer to the recipient. The transferor may need to enter additional details that enable the providers to identify that the recipient, if the recipient is not registered with Tereon and she has not transferred funds to the recipient before.

Once the transferor has entered the recipient’s details, she enters the amount she wants to transfer to her, agrees to the transaction fees and exchange rate, if any, and then enters her credential to authorize the transfer; this might be a PIN, for example. That is the point at which she initiates the transfer. This is a “pull” transaction.

- In a business-to-business transfer, the recipient will initiate the transaction by sending the payer (a business) a request for payment via Tereon, such as an invoice. This may be an invoice that the payer must pay on demand, or it may be an invoice for payment after a term. This will not start a payment process, as the payer will accept or decline the invoice.

  If the payer accepts the invoice, then the payer’s employee will enter the credential to authorize payment, or accept payment if the business pre-authorizes payments to the recipient (it may be a long-standing trading relationship). If the invoice is for immediate payment, then that initiates the payment. If the invoice is for payment after a term, then Tereon will notify the payer on a periodic basis that it will pay the invoice and amount on the payment date. At the payment date and time, Tereon will initiate the payment for the authorized invoice and make the payment to the recipient unless the payer cancels the payment beforehand. This is a “push” transaction.

A user initiates a transaction by first selecting the transaction type and then identifying the other party. If that party is present and both parties use NFC-capable devices, then the parties can use NFC (Near Field Communications) to identify devices to each other automatically. Here the user does not need to tell the merchant her Tereon ID. Instead of telling the merchant her Tereon ID, she simply taps her device, be it an NFC-capable mobile or NFC-capable card, to the merchant’s device, and the merchant’s device will identify the user’s device automatically. It will see the device’s Tereon ID and pass that to the merchant’s provider’s Tereon server.

If either party does not use an NFC device, or if they are not in each other’s presence, then the initiator simply enters the other party’s Tereon ID, or requests that other party to enter her Tereon ID. For example, a user may want to purchase something from an e-commerce website. The website will initiate the transaction once the user selects checkout; the website will ask her to enter her Tereon ID, if she has not already registered that with the site. The e-commerce website will take the user’s Tereon ID and pass that to the merchant provider’s Tereon server.

The Tereon IDs are designed to be easy to use. They are simply the user’s mobile number, email address, card PAN (provided that the PAN does not contain the user’s bank account number), or another unique credential that the user can remember and which the user’s provider will accept. What is important is that the user’s Tereon ID is never her bank account number, or an account number of any sort.

To initiate a transaction, the initiator needs only to know the Tereon ID used by the other party. A transferor or payer never ever sees the recipient’s account details, and a recipient never sees the transferor’s or payer’s account details. The one exception is where Tereon supports check processing where, by the very nature of the data in the MICR code on the check, the recipient may see the payer’s account number as the recipient needs to photograph the check in order to submit it. However here, Tereon includes logic to defend against multiple presentations of the same check.

Neither party requires the other party’s account details in any circumstance. Tereon generates internal reference numbers and uses these to account for, audit, and process a transaction. Thus, the transferor’s or payer’s provider will know that user’s account, but will process a payment and pass that payment to the recipient’s server using the recipient’s Tereon ID, the transaction number, and the sum. If the transaction requires the server to pass on other information to the recipient’s server, such as the name and address of the transferor and the recipient in the case of a cross-border remittance, then it will pass on that information and no more.

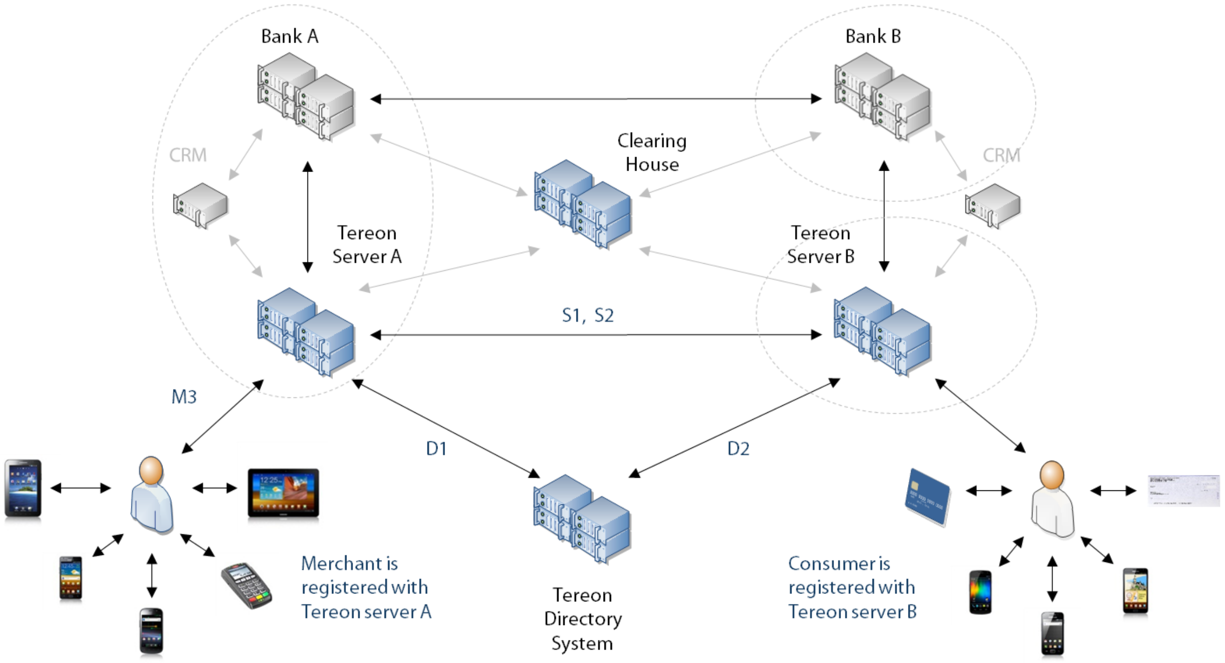


Figure 5 - Initiation flow

Figure 5 above illustrates the initiation flow in a P2B transaction. Here a consumer and merchant are in each other's presence, and they want to conclude a transaction where the consumer purchases good from the merchant.

M3 The merchant presses the "*Receive payment*" button, and then enters the consumer's mobile phone number, which is the ID that the consumer has chosen to use. The application asks if the consumer is present. The merchant confirms that the consumer is present.

The merchant application now contacts Tereon server A and passes the consumer's ID and the fact that the consumer is present to the server.

The server checks to see if it has transacted with this consumer ID before. It has not. It does this by checking its own records and then its local directory server that operates as a cache.

D1 Tereon server A's internal directory server contacts the external directory system and asks it for the server that the consumer is registered with. The directory system verifies that the consumer ID exists and responds with server B's ID and its address.

S1 Tereon server A caches the information it has received in its internal directory server and then contacts Tereon server B directly to verify that it manages the consumer's Tereon ID, and passes the merchant's Tereon ID to Tereon server.

D2 Tereon server B contacts the external directory system and establishes that Tereon server A manages the merchant's Tereon ID, and that the server is correctly licensed and authorized to operate.

S2 Tereon server B confirms to server A that the consumer's ID is registered with it.

If the consumer and merchant both used NFC-capable devices, then the flow would be slightly different. Here the consumer would tap her device against the merchant's device and they would obtain one another's Tereon ID. Figure 6 below illustrates this flow.

M3 The merchant and consumer want to conclude a transaction, where the consumer wants to pay for goods. The merchant presses the "*Receive payment*" button, and confirms that the consumer is present.

The merchant asks the user to tap her device against the merchant's terminal, and she does so. The device and terminal identify themselves to each other.

The merchant application now contacts Tereon server A and passes the consumer's ID and the fact that the consumer is present to the server.

The server checks to see if it has transacted with the consumer ID before. It has not. It does this by checking its own records and then its local directory server that operates as a cache.

D1 Tereon server A's internal directory server contacts the external directory system and asks it for the server that the customer is registered with. The directory system verifies that the consumer ID exists and responds with the server ID and its address.

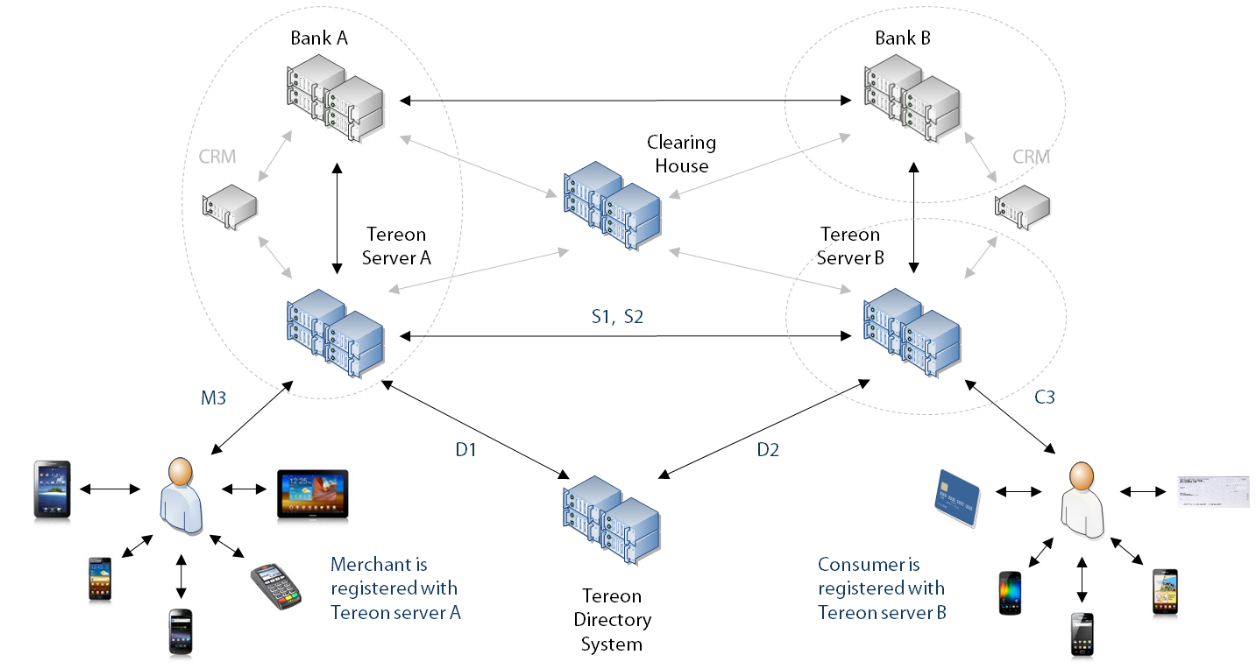


Figure 6 - Initiation flow with NFC

C3 The consumer's device contacts Tereon server B and passes the merchant's ID to the server. The server checks to see if it has transacted with the merchant ID before. It has not. It does this by checking its own records and then its local directory server that operates as a cache.

D2 Tereon server B contacts the external directory system and establishes that Tereon server A manages the merchant's Tereon ID, and that the server is correctly licensed and authorized to operate.

S1 Tereon server A caches the information it has received in its internal directory server and then contacts Tereon server B directly to verify that it manages the consumer's Tereon ID, and passes the merchant's Tereon ID to Tereon server. Tereon server B confirms that the information that it has received from Tereon server A matches the information it received from the consumer's device and the directory system.

S2 Tereon server B caches the information that it has received from the directory system in its internal directory server and then contacts Tereon server A directly to confirm that the consumer's ID is registered with it. Tereon server A confirms that the information that it has received from Tereon server B matches the information it received from the merchant's device and the directory system.

Interoperability is key to Tereon's design. Though a single service provider can operate a Tereon system as a closed-loop payments service, its default is to connect to any other authorized Tereon system to enable any authorized use on one system, to transact with a user on another. As shown above, it does this via the directory system. Tereon requires the minimum information necessary to transact and in a way that supports full authentication of the transferor or payer on one side and the receiver on the other.

The directory system enables one Tereon-based system, no matter where it is established, to link to any Tereon-based system via the look-up service, provided that those Tereon systems are licensed, authorized, and not embargoed. The Tereon-based systems can also link to third-party systems, where the provider trusts those systems and accepts the risks that those systems pose. Its internal addressing and authentication models ensure that all entities can be sure that their solutions can reach any and all payees.

Both the transferor and the recipient are free to choose which channels they will use. Tereon is completely agnostic about payment channels. It is designed to support any number of channels, and can extend its support to new channel types as those channels become available or as they are required. Tereon is available to users in a variety of circumstances and through a variety of channels as it is designed to support ubiquitous payments. Tereon's design enables it to support virtually any device or form factor, including –

- smart phones;
- feature phones (using USSD in a process that supports secure, real-time sessions. This is subject to a patent application);
- e-commerce portals;
- PoS card terminals;
- micro-processor cards;
- NFC or RFID tags;
- magnetic cards; and

- checks.

Tereon is designed to ensure that all processes are pared down to the basics. Providers can use any interface and any authentication methods appropriate to their users on a granular basis, where they can tailor the interface and authentication method for each type of device or form factor to each user. Tereon's support of UTF-8 means that providers can offer multi-lingual and graphical interfaces if required.

Tereon supports multiple devices associated with one account. Each device can have separate spending limits, and be assigned to different people. For example, a user may give her daughter a smart phone that is also registered to her account, but which has a daily spending allowance of $10, and a weekly allowance of $50. Tereon puts the user back in control of her payments services.

Tereon provides the following baseline functions to enable consumers and merchants to –

- make payments;
- receive payments;
- transfer funds;
- receive funds;
- make refunds;
- receive refunds;
- deposit funds;
- withdraw funds;
- view account data; and
- view mini-statements of past transactions.

Tereon can support virtually any use case, which can be segmented into the modes in the list below. Section 2 on page 59 illustrates a few of these. The nomenclature in the list is ordered so that the channel comes before the user. Thus –

- check consumer to mobile merchant means that a consumer uses a check at a merchant who uses a mobile or tablet device;

- a non-registered user is simply a user who is not registered with a Tereon provider, and who therefore needs to go to a merchant device to make or receive payments or transfers; and
- mobile consumer to mobile consumer peer-to-peer, simply means that two consumers use mobile or tablet devices to make a peer-to-peer transfer.

The baseline modes or standard use cases are:

- Make and receive payments
  - mobile consumer to mobile merchant;
  - mobile consumer to online merchant portal;
  - mobile consumer to mobile merchant where the customer is not present;
  - check consumer to mobile merchant;
  - consumer account to merchant account from within the account portal;
  - NFC-Tereon card consumer to mobile merchant; and
  - NFC or other card consumer to card merchant.
- Transfer and receive funds
  - consumer account to consumer account from within the account portal;
  - mobile consumer to mobile consumer peer-to-peer;
  - mobile consumer to card consumer peer-to-peer;
  - card consumer to mobile consumer peer-to-peer;
  - card consumer to card consumer peer-to-peer;
  - mobile consumer to non-registered user peer-to-peer;
  - card consumer to non-registered user peer-to-peer;
  - non-registered user to non-registered user peer-to-peer;
  - non-registered user to mobile consumer peer-to-peer; and
  - non-registered user to card consumer peer-to-peer.

- Make and receive refunds
    - mobile merchant to mobile consumer;
    - card merchant to mobile consumer;
    - mobile merchant to NFC-Tereon card consumer;
    - card merchant to NFC or other card consumer; and
    - merchant account to consumer account from within the account portal.
- Deposit and withdraw funds

    These functions, by necessity, are restricted to users with a Tereon account, except for one case. Where non-registered users have received a funds transfer, then they too can opt to claim part of a transfer, and retain the rest within Tereon until they want to claim the remaining funds. The funds will remain held within a bank or a regulated non-bank account provider.

    - mobile consumer to mobile merchant;
    - mobile consumer to card merchant;
    - card consumer to card merchant;
    - check to mobile merchant;
    - check to mobile consumer;
    - NFC-card consumer to mobile merchant;
    - NFC or other card consumer to card merchant;
    - non-registered user to mobile merchant (with printer); and
    - non-registered user to card merchant.

Tereon can associate multiple devices and multiple users with a single account. Tereon can also associate multiple accounts in different currencies with a single device. This allows a payer to decide which currency and which account she wishes to use to make a payment. It also supports the use case of a user making a single swipe at a merchant to make a payment in currency or loyalty points or mix of the two and to earn loyalty points while making a payment.

Each provider will provide a defined core level of services, each of which will operate in a predictable manner. It is important to note that the baseline features are consistent, irrespective of the channel that a user decides to use. The baseline features are designed to be easy to understand to the extent that the applications become self-documenting. If a user must pay a fee, then the system will display that fee to the user, together with the total for a transaction, i.e., the value, the fee, and the total of the value and fee. If multi-currency, then the system will also display the sum that the recipient will receive, and the cost to the transferor of making that payment, including the exchange rate.

A user can transfer her account from one provider to another with the minimum of delay. Any user can change providers by using the account switching function built in to Tereon. She can switch at any time, without fear of losing any in-air payments and continue to use the services provided by the new provider in a seamless and transparent manner. Tereon's account switching system is designed to enable a user to switch providers in minutes, and to capture and redirect all in-air payments. In-air payments are payments that a party might make to a user after the user has switched accounts or while her account is being transferred from one provider to another. Tereon's directory look-up system facilitates this function, the exact details of which are currently subject to a patent application.

The account switching function also allows a regulator or other party to close a provider and transfer its users to another provider if the first provider materially breaches any governance or payment rules or other applicable regulations. The regulator can also maintain continuity of service to the consumer in the event of a system failure within a provider.

Tereon's architecture is designed to support massively concurrent transactions, each of which is managed individually and in real-time. This enables it to authorize, clear, settle, and deliver transactions within a second, once the transferor or payer initiates a transfer or payment. It is designed to operate 24x7x365, with built-in resilience, automated audit, and accounting functions that operate in real-time.

Tereon uses a set of standard messaging and security protocols. Depending on the user case, the system will transfer the relevant contextual information between servers so that the providers retain the information required to identify the transaction type and the parties. Where the providers are not banks, their servers will transmit the information to the banks holding their funds so that the banks can, themselves, monitor the behavior of the providers. Figure 5 above is an example of this. Tereon can tailor the data to that which a recipient is entitled to see. In doing so it protects the data privacy of all parties to a transaction. No sensitive information that could be used to initiate a transaction is ever revealed to the non-initiating party.

Tereon can provide the contextual data in any format and to any schema. It simply translates its internal data to the required format and scheme as it transfers that data to the intended recipient. Thus it can feed a user's transaction history to that user's accounting software in one format, to the user's bank in another format if necessary, and to a government agency, where that agency has issued a warrant for that data, in a third format if necessary.

Tereon is designed to operate on high-end commodity hardware. Its security model automatically manages the secure communications between devices and servers, and between the servers themselves. Providers do not need, and thus do not need to incur the expense of, dedicated networks or dedicated devices.

There is no system that Kalypton or its business partners know of that is similar to Tereon. For that reason, Tereon was designed to be able to interface with third-party systems, either within a single country, or in separate countries to enable users on Tereon to transfer funds to and receive funds from users on those third-party systems. The directory service facilitates the interoperability between these services. A provider using Tereon can decide whether or not to interoperate with a third-party system, based on that system's risk profile.

Tereon implements Undeniable, Kalypton's data management controls, to define the roles of each administrator, and limit the access according to that administrator's role. Kalypton can tailor the administration policies to the provider's policies and procedures, so long as those policies and procedures are consistent with the need to protect the data and privacy of users at all times. This, in no way, prevents administrators or investigators from investigating or accessing a user's data if that user is suspected of wrong-doing. It simply means that the administrator or investigator can only investigate that user with lawful authorization to do so.

Tereon does not expose any personal data or any data that an attacker might use to make a fraudulent or unauthorized transaction to any entity. The recipient only sees the transaction number, date, time, and amount of each transaction. The recipient can use its ERP system to associate that transaction with other data, such as the description of the goods or services to which that transaction relates, but the merchant cannot ascertain the payers' Tereon ID from that data.

Tereon assumes that the network is open (it does not trust the security of the network) and so signs and encrypts all communications to forestall the majority of attempted attacks, with all used ports shut down. A denial of service (DoS) attack can be countered, both by secure routing (only traffic from known, validated sites is allowed through) and by falling back to secondary sites and to tertiary sites in extreme cases.

Tereon monitors its own performance to ensure that it meets its performance targets. Where the load increases beyond a predetermined limit, the system will scale horizontally to manage the additional load. It is designed to operate in a virtual environment. This allows the

administrator to migrate live servers from one hardware platform to another in order to carry out hardware upgrades or maintenance. It is also designed to operate across replicated locations, so that a secondary or tertiary location can continue to serve users in the event that a primary location fails. Tereon is designed to withstand the internal failure of one or more components. Its transactions are set to pessimistic ACID (Atomicity, Consistency, Isolation, Durability) consistency where necessary in order to provide the guarantee that a transaction has been recorded when it is marked as completed. It is designed to remove the need to run reconciliation checks that are prevalent with batched processes.

By avoiding a hub and spoke design, except for services such as check clearing where legislation may mandate such a design, Tereon servers communicate on a peer-to-peer basis. Thus the failure of one server does not affect the overall network or mesh of Tereon servers. The language used to code the services is hardened against common coding errors, such as buffer overloads, memory allocation errors, and so forth, so dramatically reducing the risk of a solution-related event. The transactions themselves comprise a set of defined modules, each of which is self-contained, in order to provide predictable performance, and repeatable results. The mathematical libraries, for example, are defined to use decimal floating point as opposed to binary floating point. As such, the system obviates the issue of rounding and reconciliation errors that would otherwise occur with accounting calculations.

Tereon is not an exclusive system. It can operate alongside existing payment systems, and it can interoperate with other new or legacy payment schemes at a number of levels:

- A multi-function payment device can host a Tereon app as well as e.g., an EMV (Europay, MasterCard, Visa) capability. This can all be transparent to the user and the merchant;
- A Tereon server can interoperate with the EMV environment via an EMV gateway and similarly with other new payment schemes providing hybrid payment processes beginning in Tereon and being completed in some other environment or vice-versa;
- The Tereon directory system can also interoperate with another scheme via a gateway; and
- The bank core systems can direct a transaction to start in Tereon and finish in another environment or vice versa.

The governance and payments rules for the system can tie a user's transaction limits to the level of KYC (Know Your Customer) that the provider had carried out with that user. Banked customers, and non-banked customers that the provider has thoroughly accredited will have higher transaction limits than users who have enrolled themselves, Tereon's ability to

integrate to existing account management systems means that a provider will be able to enroll any of its existing account holders simply by adding the Tereon service to its users' accounts.

Non-registered users are not necessarily un-banked, as Tereon can serve banked and non-banked users. A non-registered user is simply a user who does not have a Tereon ID.

Non-registered users will be able to transfer small sums to other users by going to a merchant whose provider allows her to provide services to non-registered users. However, once the user exceeds a certain limit, then she will need to provide additional information to the merchant before she can transfer or receive additional funds. A non-registered user can always elect to enroll as a Tereon user.

2. Authentication

Tereon provides a robust framework that providers can use to authenticate other providers and entities. It carries out both pre-authentication (see page 13), when a user starts his or her application, and then a second set of authentication steps as a user initiates a transaction. Both modes of authentication are similar, and so are described in this section.

If a user has an interactive device that runs an application, such as a tablet, phone, or terminal, then it will immediately attempt to authenticate with the Tereon server or servers that it is registered with (a device can be registered to more than one Tereon server if the user has accounts with more than one provider).

The authentication ensures that users and providers can be assured that any participant in a Tereon transaction is authorized to act as a participant and follows the governance and participation rules. Tereon's authentication model actively prevents an unauthorized provider or user from taking part in a transaction, irrespective of the country within which that provider, server, or user is located.

The authentication process also enables users and providers to isolate any lost or compromised device in real-time. The payer authorization model protects the user's device, even if that device is discovered with an authenticated application running. Additionally, the user can isolate and lock that device remotely by revoking its authorization. This works even if the user has set her application to request periodic authentication. With periodic authentication, the user authenticates herself periodically. However, the device must also authenticate itself to the Tereon server that provides a particular service every time that application initiates or takes part in a transaction.

Users must authenticate themselves whenever they start the application. Either the user or the provider can require the user to re-authenticate herself on a periodic basis. Irrespective of whether or not the user has had to authenticate herself prior to a transaction, she will still need to authorize the transaction as described in the next section. The device does not store the user's authentication credential or her authorization credential on the device. The authentication process depends on the device type that the user has. It uses a set of credentials that are unique to both the device and the user, in the form of a non-violable data string such as a hard-coded serial number, a unique registration key provided by Tereon, and a user provided credential such as a password, pattern recognition, or some other credential that the user's provider accepts.

If the communications network provides additional authentication tools, such as the ability to perform reverse HLR (home location register) lookups on a mobile network, then Tereon can use these as well, in order to verify and authenticate the device.

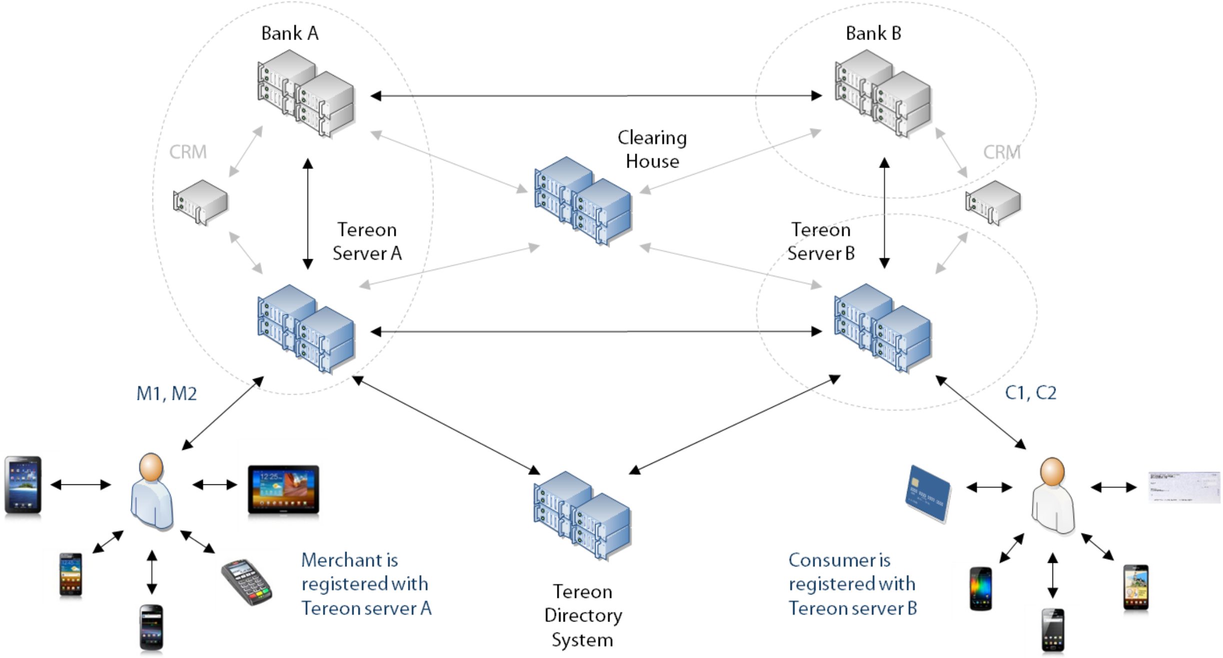


Figure 7 - Pre-authentication flow

Figure 7 above illustrates the pre-authentication flow for both a merchant and a consumer, each of whom uses an interactive, but non NFC-capable, device that run Tereon applications. The flow includes the initiation flows as these include the standard port-initiation authentication checks as well. If the two users used NFC-capable devices, then the flow below would include the step C3 (see page 20).

M1,C1 The user starts up her device. It communicates with its respective Tereon server, which confirms that the device is correctly registered and that neither the server nor the bank has blocked it.

M2,C2 The server now communicates with the application and displays an identification string that the user registered with her account. This step (which is optional) allows the user to confirm that her application is authenticated to her server. The application asks the user to enter her application password to access the application. She enters the password, which the device now confirms is correct with its respective Tereon server.

Following on from these pre-authentication steps, the users can initiate a transaction in the normal way as described in the previous section.

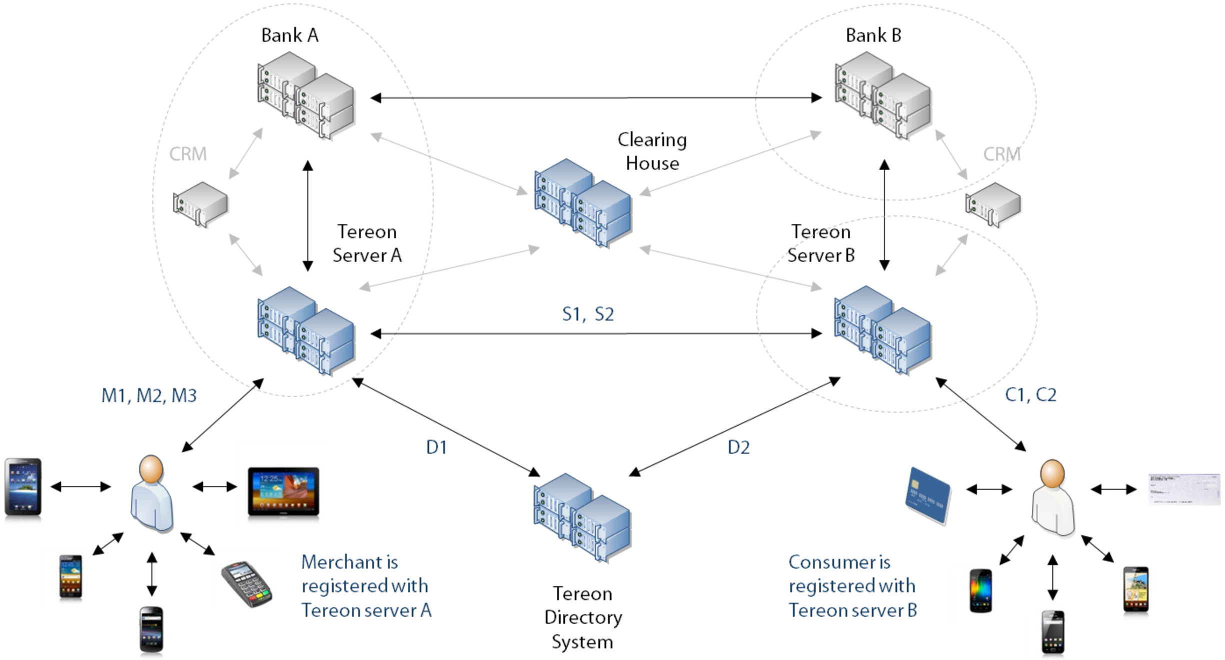


Figure 8 - Pre-authentication, initiation, and authentication flow

Figure 8 above illustrates how the pre-authentication process combines with the initiation and authentication processes.

M3 The merchant presses the "*Receive payment*" button, and then enters the consumer's mobile phone number, which is the ID that the consumer has chosen to use. The application asks if the consumer is present. The merchant confirms that the consumer is present.

The merchant application now contacts Tereon server A and passes the consumer's ID and the fact that the consumer is present to the server.

The server checks to see if it has transacted with the consumer ID before. It has not. It does this by checking its own records and then its local directory server that operates as a cache.

D1 Tereon server A's internal directory server contacts the external directory system and asks it for the server that the consumer is registered with. The directory system verifies that the consumer ID exists and responds with server B's ID and its address.

S1 Tereon server A caches the information it has received in its internal directory server and then contacts Tereon server B directly to verify that it manages the customer’s Tereon ID, and passes the merchant’s Tereon ID to Tereon server.

D2 Tereon server B contacts the external directory system and establishes that Tereon server A manages the merchant’s Tereon ID, and that the server is correctly licensed and authorized to operate.

S2 Tereon server B confirms to server A that the consumer’s ID is registered with it.

The flows above assume that the users are registered to separate providers. If the users are registered to the same provider, then the process is far simpler as there is need to refer to the directory system or have any inter-server communications. Figure 9 below illustrates this.

M1,C1 The user starts up her device. It communicates with its Tereon server, which confirms that the device is correctly registered and that neither the server nor the bank has blocked it.

M2,C2 The server now communicates with the application and displays an identification string that the user registered with her account. This step (which is optional) allows the user to confirm that her application is authenticated to her server. The application asks the use to enter her application password to access the application. She enters the password, which the device now confirms is correct with its Tereon server.

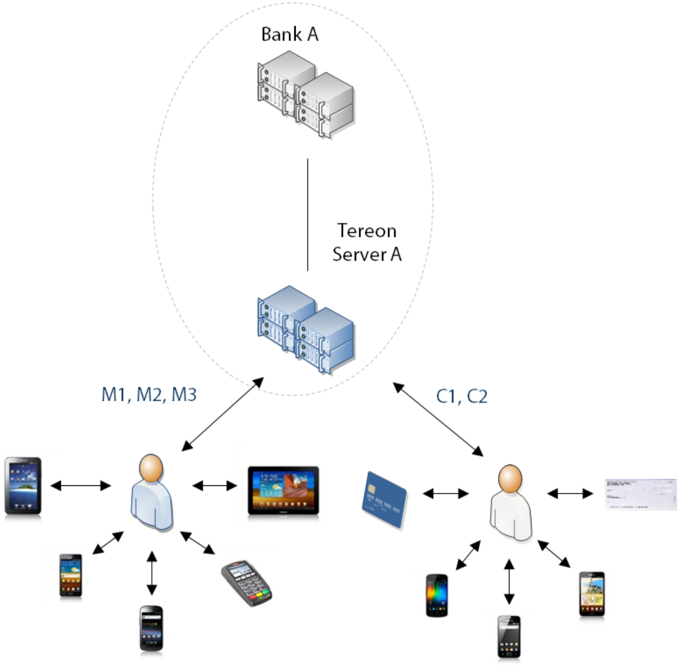


Figure 9 - Pre-authentication, initiation, and authentication flow with a single provider

M3 The merchant presses the "*Receive payment*" button, and then enters the consumer's mobile phone number, which is the ID that the consumer has chosen to use. The application asks if the consumer is present. The merchant confirms that the consumer is present.

The merchant application now contacts Tereon server A and passes the consumer's ID and the fact that the consumer is present to the server.

The server checks to see if it has transacted with the consumer ID before. It sees that the consumer is registered with it and that the consumer's device is authenticated.

This document will not consider the flows that involve a single provider further, as they are just simplified versions of the multi-provider flows without the inter-provider communications. In a single provider configuration, the provider's server authenticates the users. In a multi-provider configuration, the bidirectional handshake between the Tereon servers confirms the existence of the transferor or payer and the recipient, and that they and the providers are authorized users.

The participation requirements will be tied to the governance model so that the providers and users understand their obligations. A provider that loses its authentication to operate simply cannot connect to the wider Tereon ecosystem to transact payments. If that provider's users are blameless, then the governance body or other regulatory authority can migrate those users and their funds to other providers by using the Tereon account switching mechanism. Thus a provider that fails to abide by the governance model or the participation requirements will lose its business entirely.

The authentication protocols are identical for all transactions, except for checks, where the payer's bank is responsible for the final authentication of a check once it receives the check to process, and for cards, where the user's card is authenticated by her provider after the transaction is initiated.

Tereon's strict authentication controls are such that third-parties can create new value-added services, such as targeted marketing, that they can offer consumers, and merchants can extend offers to their customers without ever needing to know the consumers' real identities. The merchants and third-party service providers can analyze and address their offers to users without needing access to those customers' details (the way that this is done is subject to a patent application). The consumers have full control over when and whether to receive such offers or services.

For example, a café owner may want to create a loyalty scheme that offers, say, a free cup of coffee after every seven purchases. She can implement this either herself, or via a third-party,

and offer the scheme to her customers without ever having to collect those customers' personal details.

Tereon would inform the customers that they can partake of the scheme. It would be for the customers to decide whether to accept or refuse. In any event, the merchant would never see, or need to see, the customers' details.

3. Payer Authorization

The payer authorization process, as with the authentication process, provides a way of enforcing the governance rules.

No personal data or other data that could be used to initiate a transfer or payment is ever exposed to the recipient or the recipient's Tereon system. That just simply cannot happen. The only data that would be exposed is the data required by legislation or regulation, such as the transferor's and recipient's name and address for remittances. However, some of these details can be restricted to the recipient's server, and kept from the recipient if necessary and if it is lawful to do so.

No personal data or other financial data is exposed to any party. Even on an e-commerce website, all the merchant ever gets to see is the consumer's Tereon ID. Tereon is designed explicitly not to require or expose to anyone the data that PCI-DSS (Payment Card Industry Data Security Standard) attempts to protect. Quite simply, Tereon's heritage means that it is designed from the ground up to protect all personal and financial data. This has the advantage to all users in that it defrays the significant costs that they would otherwise incur with PCI-DSS compliance.

A transferor or payer can always identify herself to a recipient if she chooses to do so, much in the way that a telephone or mobile user can enable or disable caller line identification, but that is ultimately her choice to do so.

Tereon always displays any fee or exchange rate, where the transferor or payer is engaging in a multi-currency transaction, and will display the total cost of any transaction to the transferor or payer before that user can authorize the transaction.

If the provider levies a number of charges for different services, for example to allow the user to select one of a number of check clearing services that may levy separate charges, or if the user wants to remit funds and the service offers the option to pay all of the charges, pay half of the charges and charge half to the recipient, or charge all of the fees and costs to the recipient, then Tereon will display these to the user. Tereon will display the provider's default option for that service, and enable the user to select any of the other options and confirm that selection before the user can authorize the payment.

The transferor or payer authorizes her payment using a PIN, a pattern recognition, or some other form of payment authorization credential that the user's provider accepts. The device does not store the payer's authentication credential.

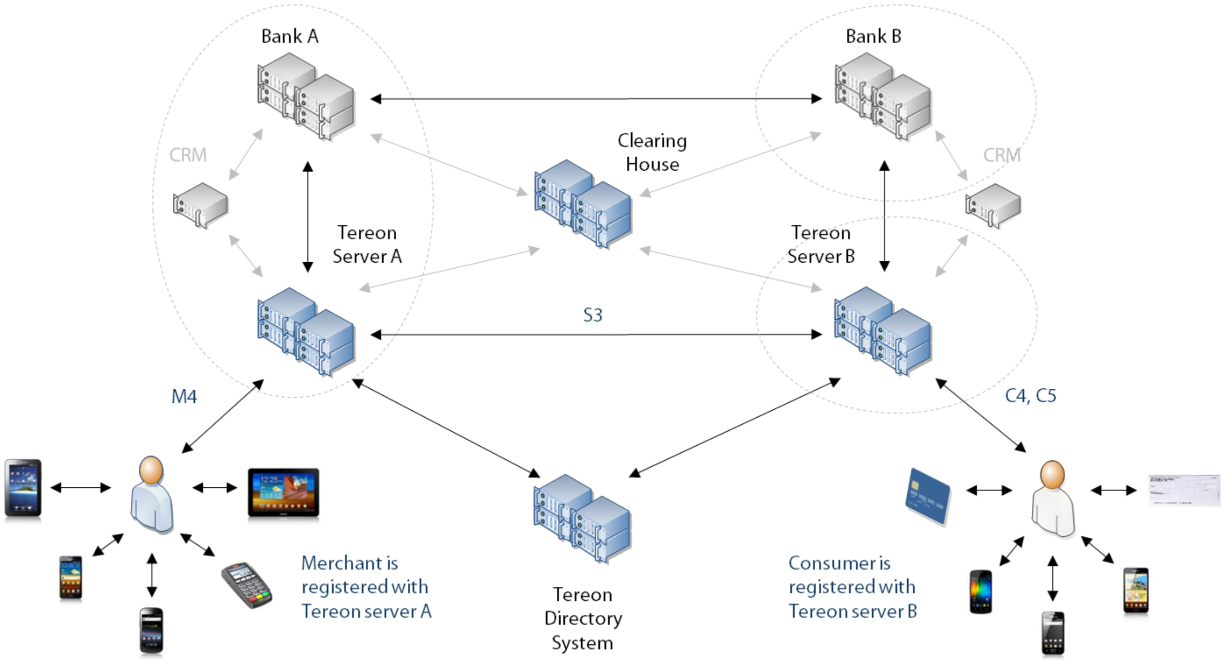


Figure 10 - Payer authentication flow

M4 The merchant’s application now asks for the amount that the consumer must pay. The merchant enters $256.95 and presses “*Sell*”. The application now asks the merchant to enter her PIN (the provider can remove the need to enter a PIN, though it does enable the merchant to track exactly which of her sales assistants took a particular payment).

If the transaction incurs any fees over those that the merchant has accepted in her contract with her provider, then her application will display the fee. She can always cancel the transaction if she refuses to pay the fee.

The application now sends these details to Tereon server A. If the merchant has entered a PIN, then the server first checks the PIN against its one-way record of the merchant’s or her sales assistant’s PIN.

S3 Tereon server A now passes the payment currency and amount to Tereon server B. Tereon server B confirms receipt and Tereon server A waits for the consumer’s response.

C4 Tereon server B checks to see if the consumer is paying in the same currency as the merchant has requested. If so, then the server simply sends the payment amount and the currency code to the customer’s application. If not, then the server first contacts

bank B for a quote for the payment amount in the consumer's currency, and then passes that amount and the currency code to the consumer's application.

C5 The consumer's application displays the merchant's name or some other identification string that the merchant has registered (never the merchant's Tereon ID), the amount to pay in the consumer's currency, and, if her currency is different to that of the merchant's, the amount in the merchant's currency, the exchange rate and any transaction fee.

The consumer reviews the amount and presses "*Buy*" to make the payment. The application now asks the consumer to enter her payment authorization credential, such as a PIN. This is to prevent an unauthorized payment from the consumer's account.

The consumer enters the PIN and presses "*OK*". The application now sends the customer's PIN to Tereon server B, which confirms it against its one-way record of that consumer's PIN. (If the provider was bank B, then the Tereon server could communicate with that bank's core systems and ask the bank to verify the PIN against its one-way record of the consumer's PIN. The Tereon server would not have a record of the PIN in that case.)

The payer has now authorized the payment.

Tereon can also authenticate the recipient, such as where the recipient is a merchant using a PoS card terminal or a mobile device. Here the merchant can configure Tereon so that the merchant, or one of the merchant's assistants or staff members has to enter her PIN when taking a payment or making a refund. This enables the merchant to track exactly who made the transaction for internal audit purposes. This feature is optional.

Unless the user decides otherwise, she must actively authorize every transaction. Thus, for example, even if she has authenticated her application on her smart phone and then lost her device, anyone finding her smartphone cannot make a transaction unless that person also knows the user's authorization credential.

Pre-authorization is slightly different. A PIN-less transaction, for example a contactless NFC-based transaction, is a pre-authorized transaction, as is a deferred utility bill or invoice payment. Tereon provides the ability for the user to pre-authorize both amounts and transaction types. For example, rather than configure a blanket level below which her device does not need to authorize specifically a transaction, the user may configure her devices and account to pre-approve transit tickets of up to $5 a journey, with a cumulative daily total of $20, for example, and yet still require her to authorize a coffee costing $3.50. A user can revoke or change these settings at any time, and those changes will take effect immediately.

Another form of pre-authorization would occur for utility or trade bills, where the merchant or payee presents an invoice, either via Tereon or by another method, that the payer must pay within a certain time. The payer can accept the invoice in Tereon and then authorize Tereon to pay that invoice on or before the due date, or even in installments if that option is offered. If presented with an invoice or bill by another means, the user simply enters the payee’s details as normal, and then the invoice reference number, the payment amount, and the date by which she must pay that invoice. If the payee has integrated its billing system to Tereon, then the user may only need to enter a reference number and Tereon will retrieve her bill. In either case, she will then enter her authorization credential and Tereon will register the payment to be made by the date that she entered or the date that it retrieved from the payee’s system. In all of the three cases above, Tereon will inform the user periodically of the amount that it will pay to the payee. The user always has the option to cancel the pre-authorized payments at any time, and to re-instate them at any time.

A provider may wish to allow the user to configure her account to send a message to her mobile every time she makes a pre-authorized payment. Thus, she would receive an SMS or in-application notification every time she purchased a transit ticket, or when she had paid an invoice or utility bill. These messages would act both as reminders, and also to act as a security feature so that she could take immediate action if someone had managed to obtain her device, and her authorization and authentication credentials.

Tereon’s security model means that a nefarious individual could not scan or remotely read a user’s device, be that a mobile or card, that is set to support pre-approved contactless payments and obtain any meaningful information. That attacker would see only encrypted material. Tereon never transmits any data in the clear.

Tereon’s pre-authorization model is based on a hierarchy of permissions. The provider can set an upper limit for each payment type or service that it will allow a user to make a pre-authorized payment. The provider can reduce those limits, if it decides to do so. The user has the final say, and can reduce those limits further, as in the PIN-less transaction above, or even decline pre-authorization altogether. The user can always choose to use a service, even after previously declining a service, just as she can decline a service at any time after having used it on other transactions.

Tereon’s pre-authorization model can go further. With Tereon, an initiator need not be an organization or a natural person. It could be an appliance connected to the Internet of Things. One of the exciting prospects of the Internet of Things is that a complex machine can order a service or a refrigerator can order groceries. Tereon supports this kind of vision with extreme scalability to support an explosion in transaction volume. The Tereon initiation and authentication model also supports this vision in a two-tier structure akin to the process

whereby a subscriber's Skype account tops up when it hits a pre-determined minimum balance:

- the owner of the machine establishes the rights of the machine to pre-authorize it to "automatically" re-order goods and services. This is reflected in the Tereon business rules engine; and
- the machine making the "automated order" is authenticated just as any other device is authenticated to the Tereon server to ensure that this is the machine that is under the control of the identified account holder.

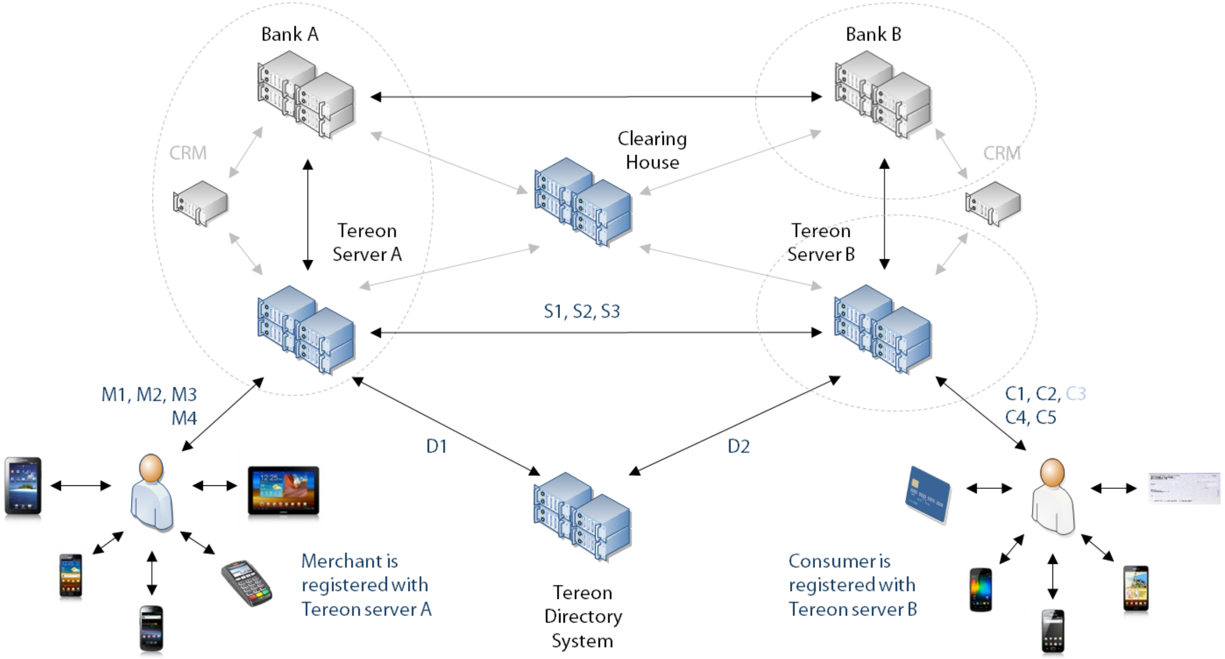


Figure 11 - Pre-authentication, initiation, authentication, and payer's authorization flow

Figure 11 above illustrates the flow of all of the lifecycles discussed to this point. In the figure, the step C3 is dimmed as this applies only where both the merchant and the consumer use NFC-capable devices.

4. Approval by the Payer’s Provider

As discussed briefly above in the section on initiation, the payer’s or transferor’s provider will first check that the payer or transferor’s account has sufficient funds or an approved credit line to cover a transaction before it will authorize the transaction itself. This is to prevent the very real danger of allowing a settlement liquidity issue to arise, where the user goes overdrawn before a payment is settled, leaving the provider to either draw on its own funds, or block the payment and so place the recipient at a disadvantage.

Tereon’s approval process removes the settlement liquidity risk for all transfers and payments. It means that Tereon itself enforces the financial solvency requirements for providers. Figure 12 below illustrates this process.

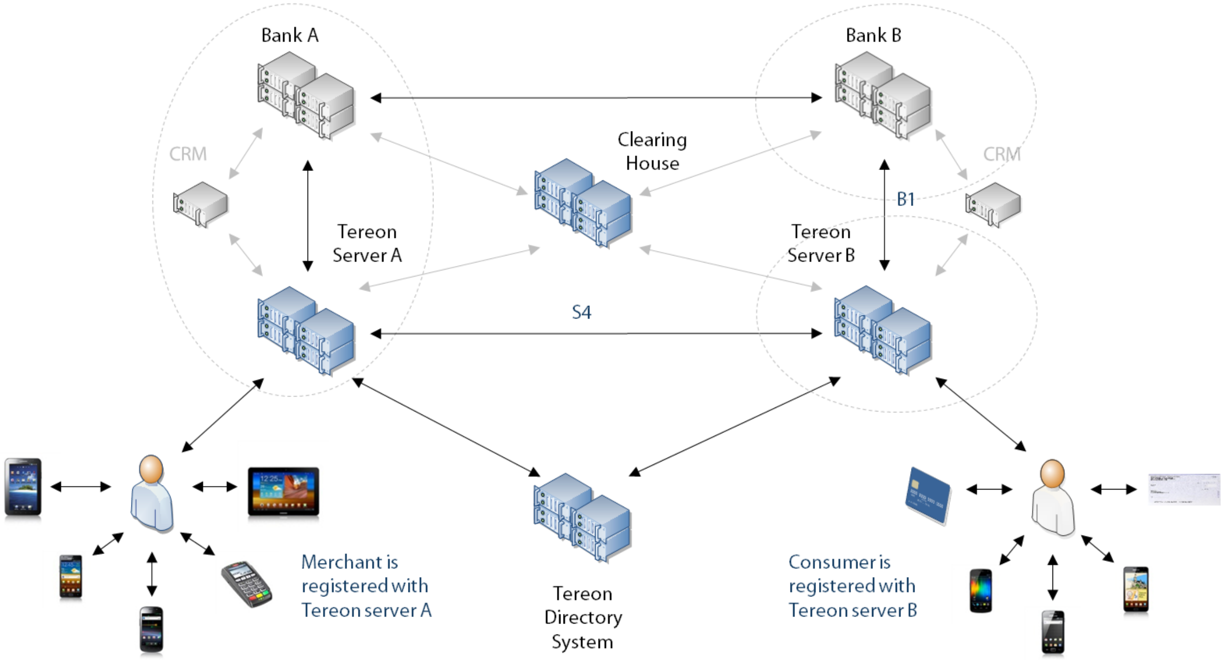


Figure 12 - Approval by the payer's non-bank account provider

B1 Tereon server B confirms that the user has sufficient funds in her account or an approved credit facility to cover the payment. It now communicates with the bank to confirm that the bank will be transferring funds from the control account that the bank holds on the provider’s behalf, and the bank confirms that the account holds sufficient funds, or has sufficient credit from an approved credit facility to transfer funds to the recipient’s provider.

S4 Tereon server B communicates with Tereon server A to inform it that the consumer has authorized the payment.

A user cannot make a transaction unless she has sufficient funds or an approved credit line in her account to cover that transaction. Tereon does not allow transfers that are unsupported by funds or approved credit lines (see pages 41 and 56). The reason that the consumer's Tereon server does not confirm to the recipient's Tereon server that she has authorized the payment until now is that if she does not have sufficient funds or credit, then her server will terminate the transaction at this point. It will inform her that she has insufficient funds or credit, but it will simply inform the merchant's Tereon server that the consumer cancelled the transaction. The merchant does not need to know why.

If the transferor's or payer's provider is a bank then the process is very slightly different, as shown on the next page.

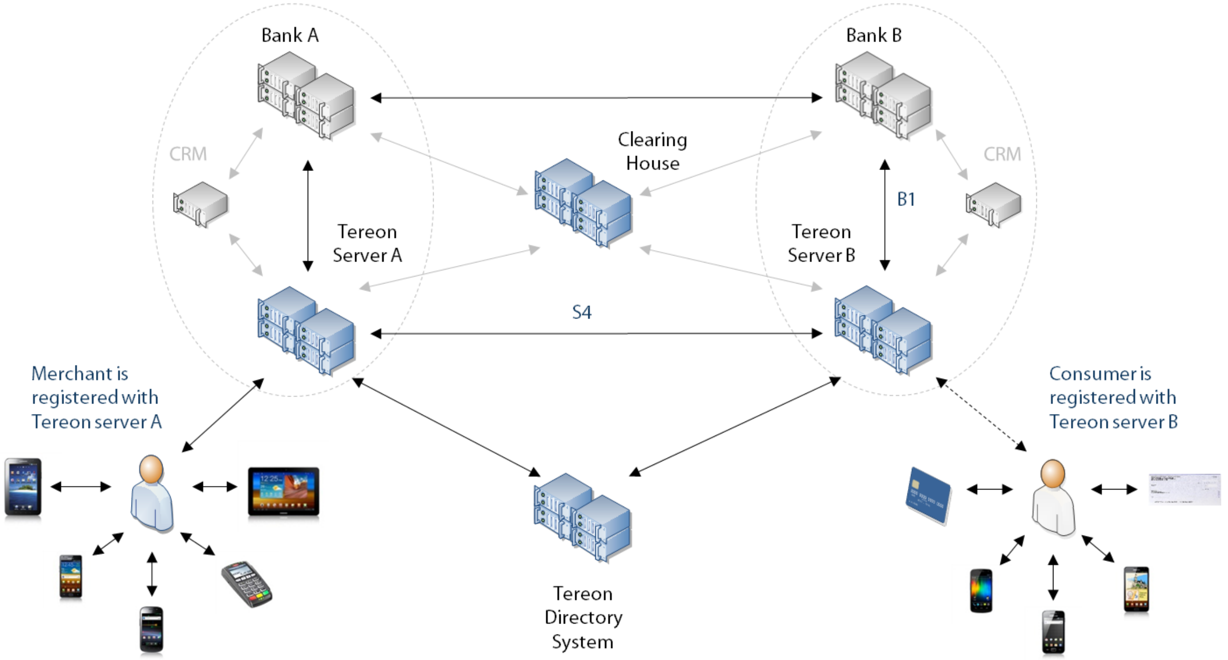


Figure 13 - Approval by the payer's bank account provider

B1 Tereon server B communicates with the bank to confirm that the user has sufficient funds in her account or an approved credit facility to cover the payment.

S4 Tereon server B communicates with Tereon server A to inform it that the consumer has authorized the payment.

The user can, at any time, see a running total of the funds and any credit that she has available. Tereon does not have a reconciliation process that incurs a time delay between making or receiving a payment and displaying the account balance. Each transaction, other than a deferred payment or deferred remittance, is completed in real-time and both users will be able to see the results of the transaction in real-time. Any user can therefore quickly check that she has sufficient funds or credit in her account to cover a payment or transfer before she enters into a transaction.

The provider receives a real-time data feed of each and every transaction that is sufficiently anonymized and formatted for its systems. The Tereon server still retains a complete audit trail and can provide any historical data that the provider may require for any subsequent investigation. This is not just so that it can perform its AML (anti-money laundering) or anti-fraud monitoring obligations. This also allows the provider, and, if separate, the bank, to know immediately and before any transaction, whether the user has sufficient funds or credit to cover a transfer or payment.

Both the payer's and the recipient's providers will see the status of the payment at this stage during the bilateral negotiation between them.

Where a payment may be deferred, such as where legislation imposes a delay, the provider or others need to follow reporting and examination requirements on a transaction, or a user has made a remittance payment to a recipient who has not yet collected that transfer, then the users will be informed of the payment's status. In most cases, however, the users will be informed later in the process, as the system will move in real-time to the clearing, settlement, and receipt stages in that payment's lifecycle.

If a payment has been deferred or delayed, then the transferor or payer can cancel the payment at any time, and will receive the funds, less any fees or exchange costs (if a multi-currency transaction) that the provider cannot reclaim on behalf of the user. If the governance rules require the user to be reimbursed in full, then the provider will not be able to charge any fees on the transaction or exchange the transferor's currency to the recipient's currency until the provider authorizes the payment to move to clearing, settlement, and receipt. If the delay means that the user incurs a different set of charges or exchange rate, then the system will notify the user of that new charge or rate immediately, and the user then has the option to cancel or proceed with the transaction.

Once the payer's provider authorizes a payment to move to clearing, settlement, and receipt, that payment becomes final as the funds are immediately hypothecated to the settlement account for immediate clearing and settlement.

Provided that the account provider has the requisite systems, a payer's system should be able to approve a payment in less than one second from the moment that the payer or transferor has initiated the payment. This is subtly different to the user who has initiated a transaction. For example, in the flows in this section, it is the merchant who initiates the transaction in the P2B transaction. However, it is the payer, once she accepts to pay the transaction and then authorizes the payment with her PIN or other authorization credential that initiates the payment. Her provider's Tereon system will authorize that payment in less than a second after she has submitted her authorization credential.

Figure 14 on the next page shows the flow for the pre-authentication and the four lifecycles to this stage.

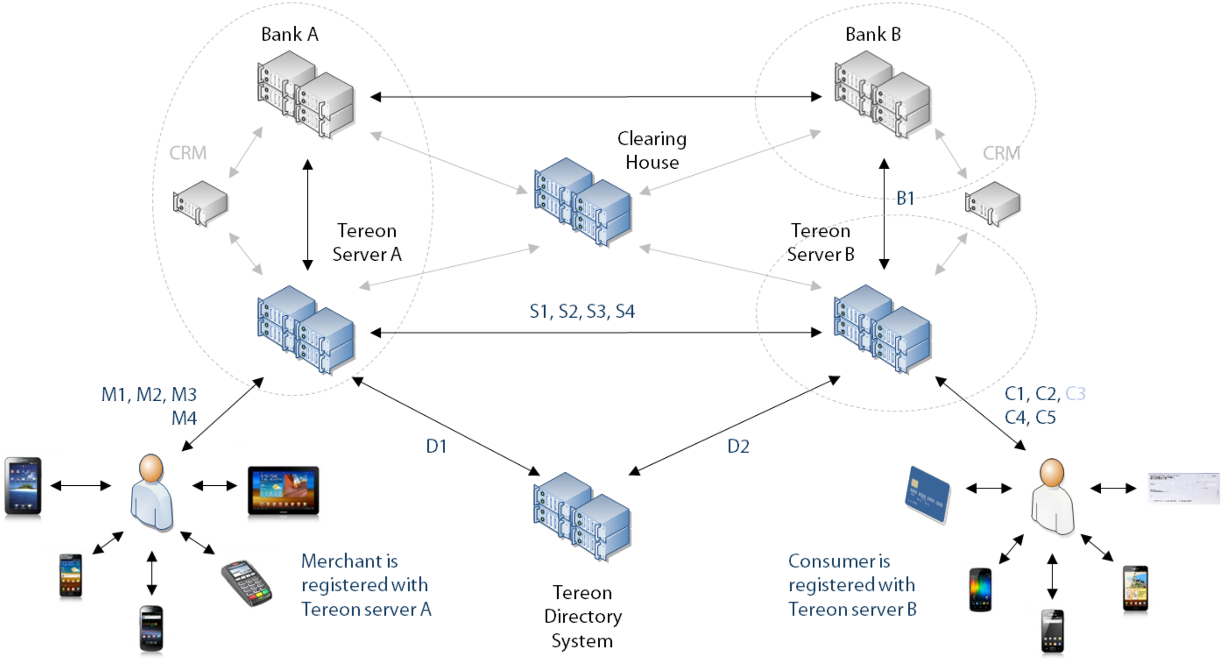


Figure 14 - Pre-authentication, initiation, authentication, payer's authorization, and approval by the payer's provider flow

5. Clearing

Tereon uses its own internal message format by default in order to communicate between servers and devices. This is part of its security model to avoid the security threat posed by passing structured message formats, whether or not they are encrypted, between servers across any network accessible to a third-party. However, Tereon can use any existing message format, such as ISO 20022, or ISO 8583, if one of these formats is required by regulation. Tereon can, and does use message formats when it communicates between its servers and a bank's core systems. That format will be dictated by the bank's core systems provider. Tereon simply translates between its format and the required format using a scheme defined for that purpose. In this way, Tereon can use any existing or future data format as and when required to do so.

Tereon immediately instructs the bank to clear the transfer or payment once the payer's provider has approved that transfer or payment.

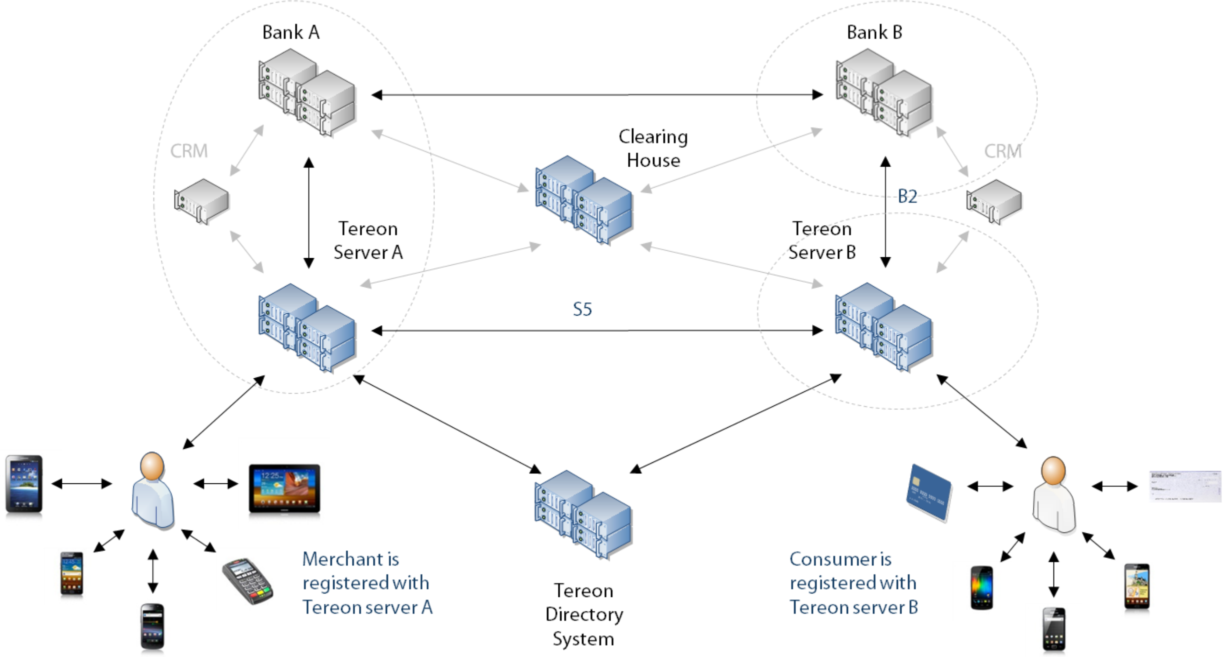


Figure 15 - Clearing with a non-bank account provider flow

B2 Tereon server B instructs the bank to make the transfer or payment to the recipient, and provides the transaction number for the transaction, and the recipient's bank details (these are not the recipient's bank account but the bank at which the recipient holds her account), and to debit the consumer's account.

Tereon server B updates the ledger entry for the consumer to show that her account has been debited, and credits its internal control ledger for payments that will leave the control account.

S5 Tereon server B informs Tereon server A that it has cleared the transfer or payment.

If the transferor's or payer's provider is a bank then the process is very slightly different, as shown on the next page.

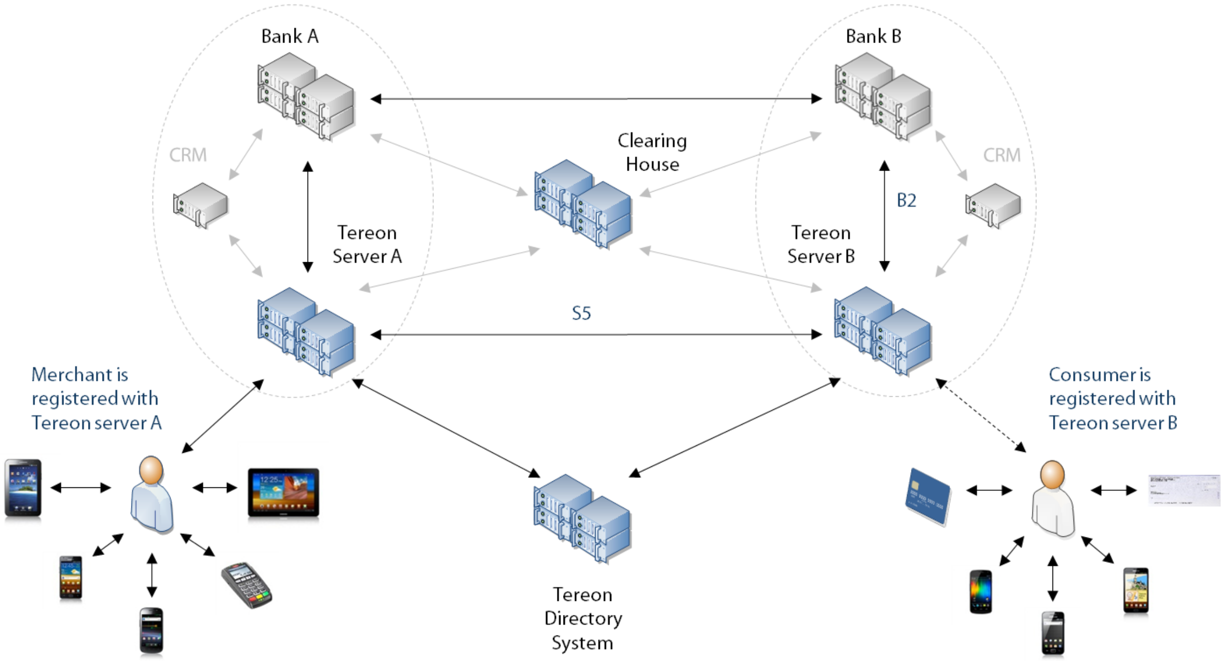


Figure 16 - Clearing with a bank account provider flow

B2 Tereon server B instructs the bank to make the transfer or payment to the recipient, and provides the transaction number for the transaction, and the recipient's bank details (these are not the recipient's bank account but the bank at which the recipient holds her account), to debit the consumer's account, and to credit its internal control account for payments that will leave the bank.

S5 Tereon server B informs Tereon server A that it has cleared the transfer or payment.

The bank (or non-bank account provider if it holds the funds itself rather than in a control account at a bank) can choose to associate the user's Tereon ID with that user's account, or it can allow the Tereon server to associate the user's Tereon ID with the user's account number. Tereon will only use this latter option if the account provider also operates the Tereon server within its infrastructure. Where the Tereon server sits outside of the bank account provider's infrastructure, then it will pass the Tereon IDs to the account provider, and use a secondary server operated by the account provider to translate the user ID and service to the requisite user's bank account number. A user may have more than one account with an account provider, and choose to associate different services with different accounts.

Tereon does not allow personal or sensitive financial or account data to leave the provider's perimeter, except where the recipient's server must receive personal information in order to satisfy regulatory requirements, such as the transferor's name and address in the case of a cross-border remittance.

The payer's provider's system will almost always clear the payment for settlement and receipt within a second of the payer submitting her payment authorization credential. There are circumstances where there might be a delay, but these are due to the need to follow additional regulatory steps, when the actual authorization to make the payment occurs once the user or the system administrator has completed her steps.

For example, suppose a user elects to transfer or remit $10,000 to her relative. Once she has submitted her authorization credential, the Tereon system will flag the payment for reporting, check that she has sufficient funds or a credit line, and if so will display a dialog box on the device that she used to make the transfer. That dialog box will ask her to enter the reason for the transfer. She might enter "loan repayment" or "gift" for example, and then press OK or Submit. That is the point at which the payer has authorized the payment, and her provider's system will log the reason, authorize the payment, and then clear the payment for settlement and receipt within a second.

Another example might be where a merchant presents a check for payment via Tereon. That check will, provided it is not a duplicate or fraudulent check, be transmitted to the payer's bank within seconds. The payer's bank's processes will then determine how quickly its systems and processes can authorize that check to clear. This may be seconds, depending on the speed of its OCR and signature processing, if any signature processing does occur, all the way through to the time it takes two administrators to review and approve or deny the check. Once approved, Tereon will clear the check for settlement and receipt in less than a second. As mentioned before, check presentation is the only process where Tereon allows the recipient to see the payer's bank details. It must do so as these are printed on the check and therefore beyond Tereon's control. Tereon can encode the MICR code on a check so that it does not display any account information at all, using a Tereon ID instead, but that would require wholesale cooperation from the banks to do so.

The exact moment that a payment in a transaction is cleared will depend on the payment system rules that apply to that transaction type. The rules will ensure that neither the payer's account provider nor the recipient face a settlement liquidity risk that can occur when there is a time gap between a payer authorizing a payment and that payment being cleared for settlement and receipt.

Figure 17 below shows the flow for the pre-authentication and the five lifecycles to this stage.

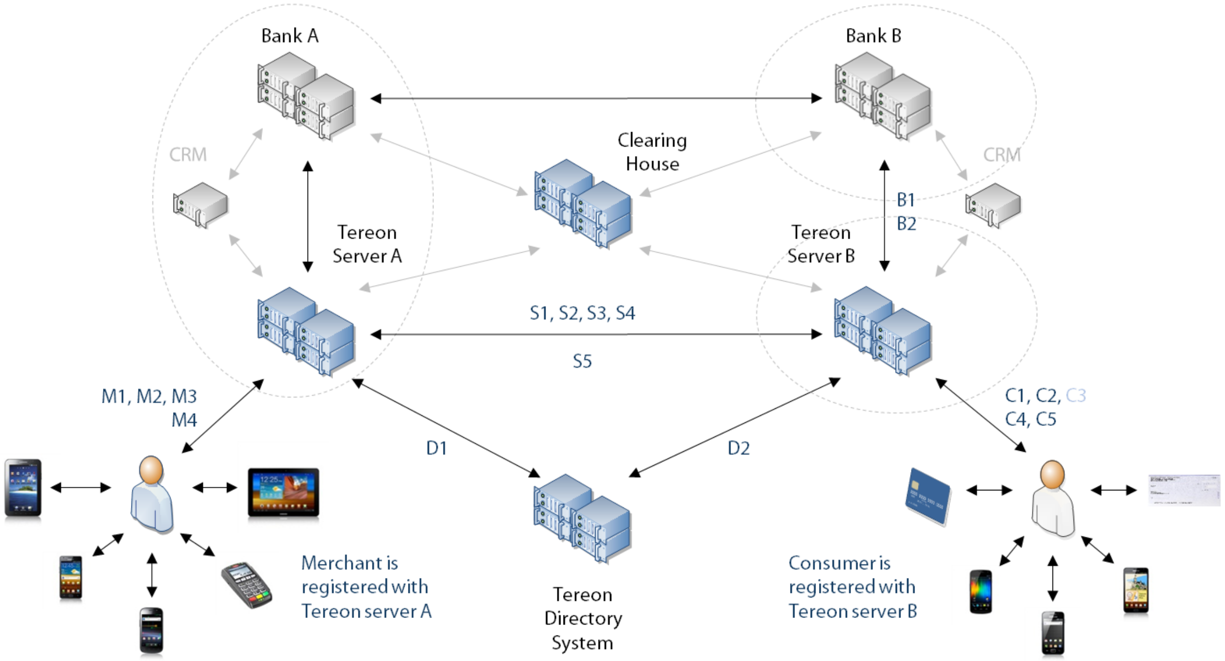


Figure 17 - Pre-authentication, initiation, authentication, payer's authorization, approval by the payer's provider, and clearing flow

6. Settlement

In virtually all cases settlement in Tereon occurs immediately after the payer's provider's Tereon server has cleared the payment. The only cases where settlement may occur sometime after a payment has been cleared is where a payment has been deferred, such as when it is being investigated or requires manual intervention due to regulatory requirements (check processing can sometime require manual intervention from administrators, even after the payer's bank has cleared a check for settlement, though this is very rare), or when a user has transferred or remitted funds to an unregistered user who has not collected that transfer, and where that remittance does not involve an exchange of currencies.

The internal operation of Tereon is modeled on the premise of electronic bills of exchange, where for the most part the "bill of exchange" is presented for immediate payment within a second of its creation. Each payment, once cleared becomes an irrevocable promise to pay.

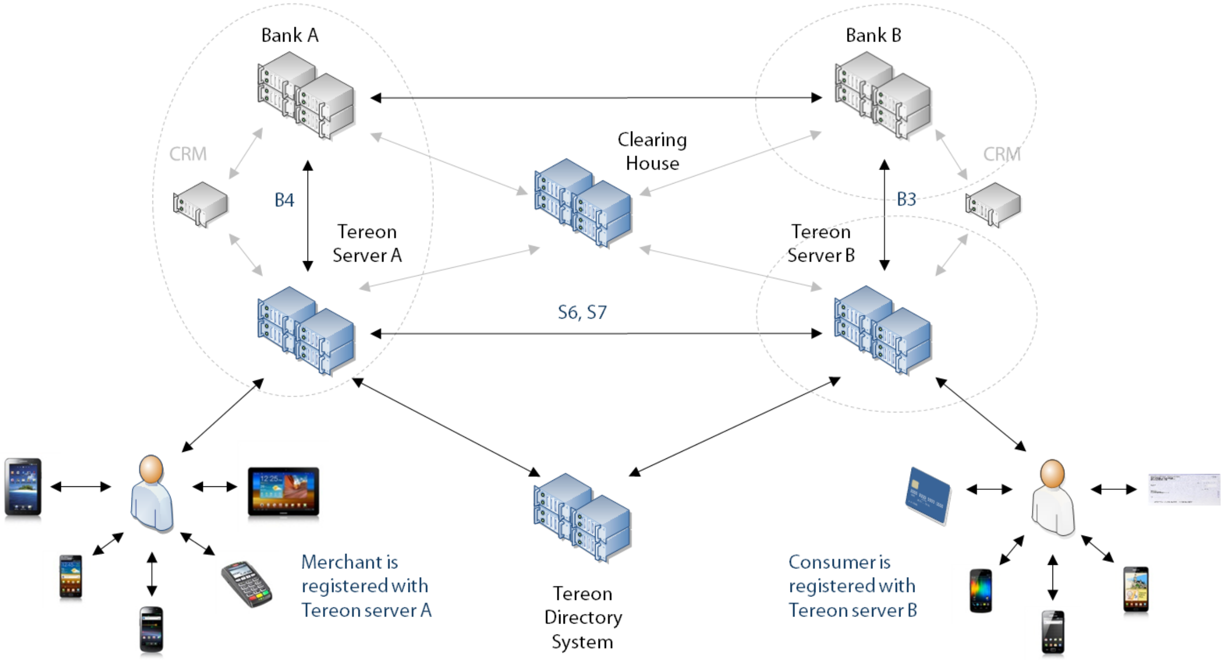


Figure 18 - Settlement flow

S6 Tereon server B informs Tereon server A to settle the payment.

B3 Tereon server B instructs the bank to update its settlement accounts in favor of bank A with the transaction number as the reference.

B4 Tereon server A instructs the bank to update its settlement accounts to account for the payment from bank B with the transaction number as the reference, and to credit the account of the merchant with the sum, less any transaction charges.

Tereon instructs the bank to credit the transaction account with the transaction charges (if any) levied on the merchant.

Tereon identifies both the payer or transferor and the recipient uniquely, and only authorized users, regardless of whether they are registered or unregistered, can be party to a transaction.

Once the payment is cleared the funds to settle the transaction are hypothecated to the settlement account. Unless the user or provider cancels the transaction, neither the user nor the provider can access those funds for any other purpose. In this way, Tereon removes the settlement risks that may arise from a lag between funds availability to the payee and settlement between providers.

Tereon can settle a transaction in a number of ways, depending on the providers and any existing settlement mechanism that they wish and are permitted to use for the proposed faster payments system. Most settlement systems are batched, and for consumers, the recipient's account provider using such a system will sometimes credit funds to a recipient before the provider receives those funds via the settlement system. This creates a settlement liquidity risk whereby the recipient's provider fails to receive the funds to cover the earlier credit of funds to the recipient. The UK's Faster Payments system is just one such batched system that settles transactions up to three times a day. Consumers will usually receive credited funds within seconds of a payment being initiated, though the settlement may take hours. Businesses, on the other hand, often have to wait until their payment is settled before they receive funds.

When Tereon settles a transaction it will instruct the transferor's or payers' account provider to hypothecate the funds for settlement, by crediting a settlement account in favor of the receiving account provider with a transaction reference number that enables that account provider to identify the end recipient. It will instruct both the transferor's or payer's account provider and the recipient's account provider to debit and credit the user's account, and it will instruct those account providers to debit and credit their settlement accounts. This will usually trigger a settlement using the account providers' existing settlement mechanism, but this may be a batched system and so, even though Tereon has hypothecated the funds, present a theoretical risk to the receiving account provider.

Tereon can go further. If the account providers settle via a third-party commercial bank, then, if that settlement bank operates a Tereon server, Tereon can also update the settlement accounts in real-time at the settlement bank. If the settlement bank is a central bank, then Tereon can carry out the same process if that central bank opts to operate a Tereon server.

Tereon will update the settlement accounts, or instruct an account provider’s core systems to update its settlement accounts, within one second of the payment process being initiated. Tereon can also update the settlement accounts at the settlement bank (a commercial bank or a central bank) for the two account providers in a multi-party transaction.

The ability to update all of the settlement accounts up to, and including, the accounts held in the settlement bank, removes the liquidity of credit risk that the providers face with other settlement processes. Tereon will also hypothecate funds to settlement accounts where the providers use a batched settlement system in order to reduce the settlement risk. However, it cannot control that batched system and so some risk may still exist with such a system.

Figure 19 below shows the flow for the pre-authentication and the six lifecycles to this stage.

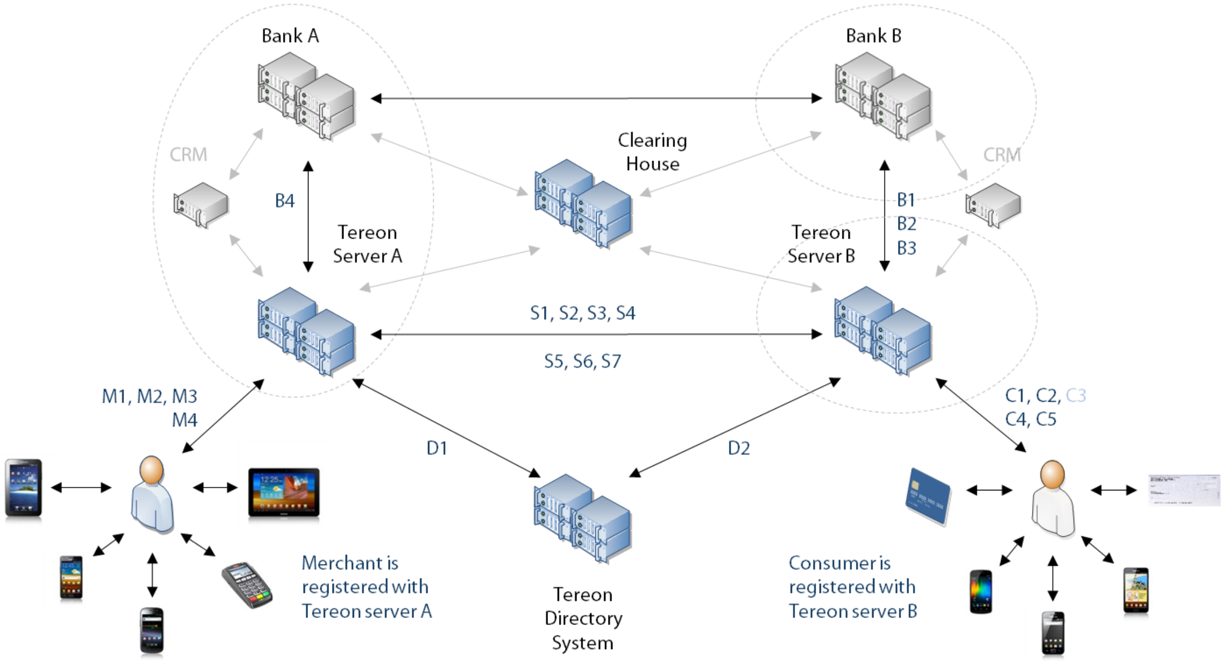


Figure 19 - Pre-authentication, initiation, authentication, payer's authorization, approval by the payer's provider, clearing, and settlement flow

The settlement process differs slightly where the recipient of a remittance payment is a non-registered user.

In the case of a mono-currency transaction, the amount remains in the merchant’s account provider’s control account until the recipient claims the sums. The money is hypothecated to

that account, and the payment is settled and irrevocable once the recipient accesses the funds at a merchant.

In the case of a multi-currency transaction, the amount sits in the control account of the settlement bank in the country of the recipient and in the currency of that country. The money is hypothecated to that account, and the payment is settled and irrevocable once the recipient accessed the funds at a merchant.

7. Receipt

The usual mode of operation for Tereon is that the moment it settles a transaction, it informs the transferor or payer that she has made a payment and the funds have been debited from her account, and it informs the recipient that she has received the funds, which have now been credited to her account.

Tereon identifies all merchants by the name that they have registered, so that a consumer can identify the merchant in any transaction. If consumers elect to do so, then they can allow Tereon to identify them by the name that they too register. However, this is the only information about a consumer that a merchant may see, and consumers can elect only to reveal their registered names to known contacts, or to any party on a case-by-case basis. The default position is that Tereon does not reveal a consumer's registered name, irrespective of whether that is her real name or some other name. The consumer is always in control.

A user with an interactive device, such as a smart phone, feature phone, tablet, web portal, or PoS card terminal can see immediately that the funds have been credited to or debited from her account. A non-interactive device, such as a micro-processor card or magnetic stripe card, cannot display that information. However, a user can take her card to any interactive device capable of reading her card and use that device to see that funds have been debited from or credited to her account. If the user has two or more devices registered to the same account, and one of those devices is an interactive device, then that device will show all of the transactions, unless she has decided to separate the devices for separate purposes. The user can also access her account via a portal and see exactly the same information.

One of the design aims behind Tereon was to create a payments system that could support both the banked and the non-banked. Unbanked users with accounts in non-bank account providers can use Tereon in exactly the same way as banked users. Tereon does not differentiate between them. The only difference is the institution that holds the user's account. The real difference is the way that Tereon treats an unregistered user.

An unregistered user may or may not know that she has received funds unless she is standing at an interactive merchant device while the transferor is transferring the funds to her. Instead, the transferor will simply tell the recipient that she can now go and collect the funds from a merchant within a certain period of time, say 30 days. The transferor will also pass to the recipient, a transaction number that she can give to, or enter into, any merchant device, and the retrieval PIN to access and retrieve the funds. Once the recipient accesses the funds, the transferor, if she is a registered user, will see a report on her interactive device that the recipient has accessed the funds. If the user does not have an interactive device, then she can, of course, view that information via her portal to her account.

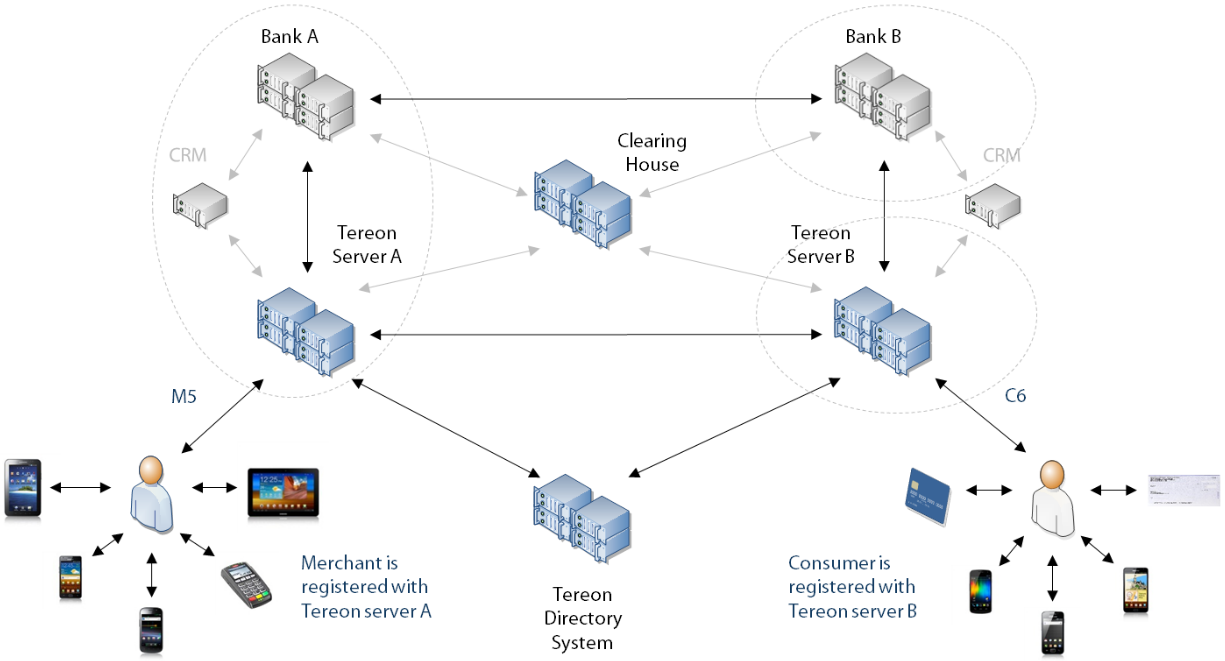


Figure 20 - Receipt flow

M5 Tereon server A informs the merchant that she has received the funds into her account.

C6 Tereon server B informs the consumer that she has completed the payment.

Figure 20 above shows the receipt process, which is simply to inform the users that they have now completed the transaction. It informs the merchant that she has received the funds, and the consumer that she has made the payment.

An unregistered transferor can view the status of any transfer by going to a merchant device and entering the transaction number and the transferor's cancellation code. She can cancel a transfer at any time up until the recipient accesses the funds, but she can use the same process to see whether or not the recipient has accesses those funds. The transferor simply declines the opportunity to cancel the transaction when she views its status.

Figure 21 on the next page shows the flow for the pre-authentication and the seven lifecycles to this stage.

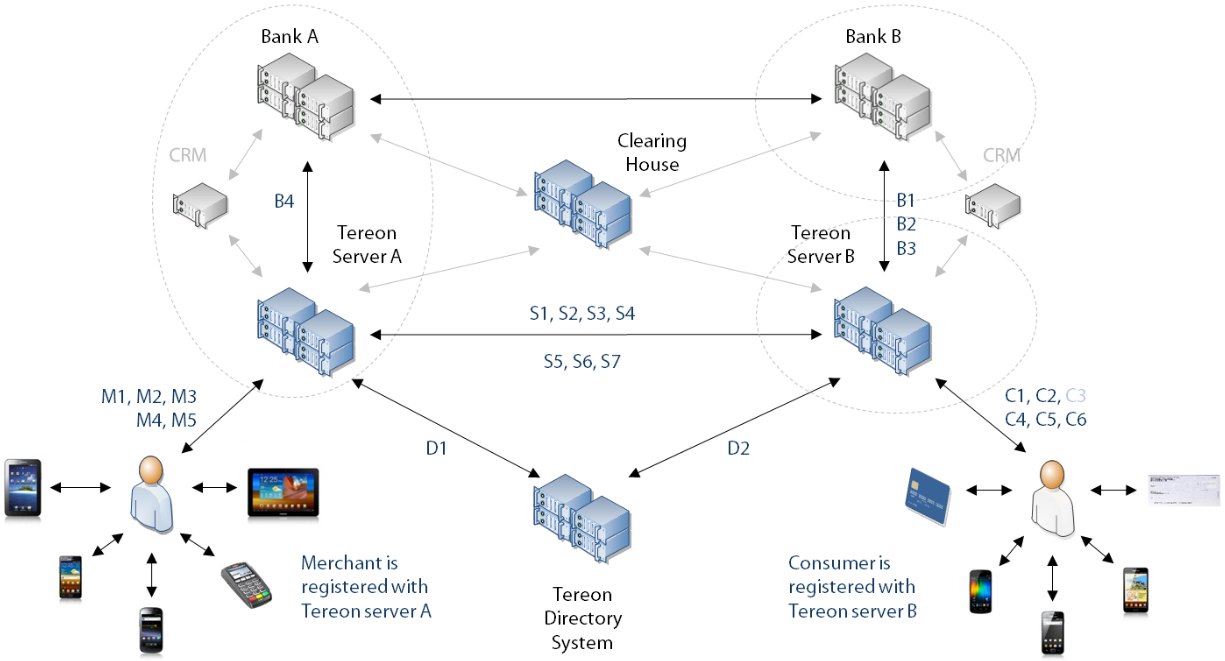


Figure 21 - Pre-authentication, initiation, authentication, payer's authorization, approval by the payer's provider, clearing, settlement, and receipt flow

Tereon does not impose any delay between settlement and receipt of funds in order to minimize the risk of disputed payments. A user cannot, for example, make a payment to a merchant in receipt for some goods and then, later, cancel that payment before settlement, keep the goods, and dispute whether any payment was made. The time lag between clearing and settlement, and between settlement and receipt just does not exist for payments that require the user to interact with the merchant to authorize that payment.

A time lag will occur with a check, where that lag exists between the payer handing her check to a merchant, the merchant submitting that check, and the payer's bank clearing that check for settlement and payment. This lag may only be a few seconds, or could be as long as a week if the merchant processes the check in batches. Here the user will have signed her check, and so her intention to pay is clear. The standard rules for check payments will apply to any payment made by check should the user cancel the check after leaving the merchant's premises.

8. Reconciliation

The audit trail and profile history that Tereon creates for a user is structured identically for any user, whether that user is banked or unbanked. Unbanked users may be unbanked because they simply chose to be, or because they do not have a financial profile and history that allows them to be banked users. Every user's profile treats that user as if she was a banked user. This is to remove the distinction between those types of users, and enables an unbanked user to become a banked user once that user has grown her financial transaction profile and history and can qualify to become a banked user.

Tereon does not have a reconciliation process that runs after the event. It audits and records every transaction in real-time in a manner that guarantees ACID consistency for every transaction. Tereon does not rely on eventual or BASE (Basically available, Soft state, Eventual Consistency) consistency, and so does not need to run reconciliation checks. Tereon keeps a running total of each account. It needs to do so in order to conform to the requirement to clear, settle, and receipt a transaction in real-time.

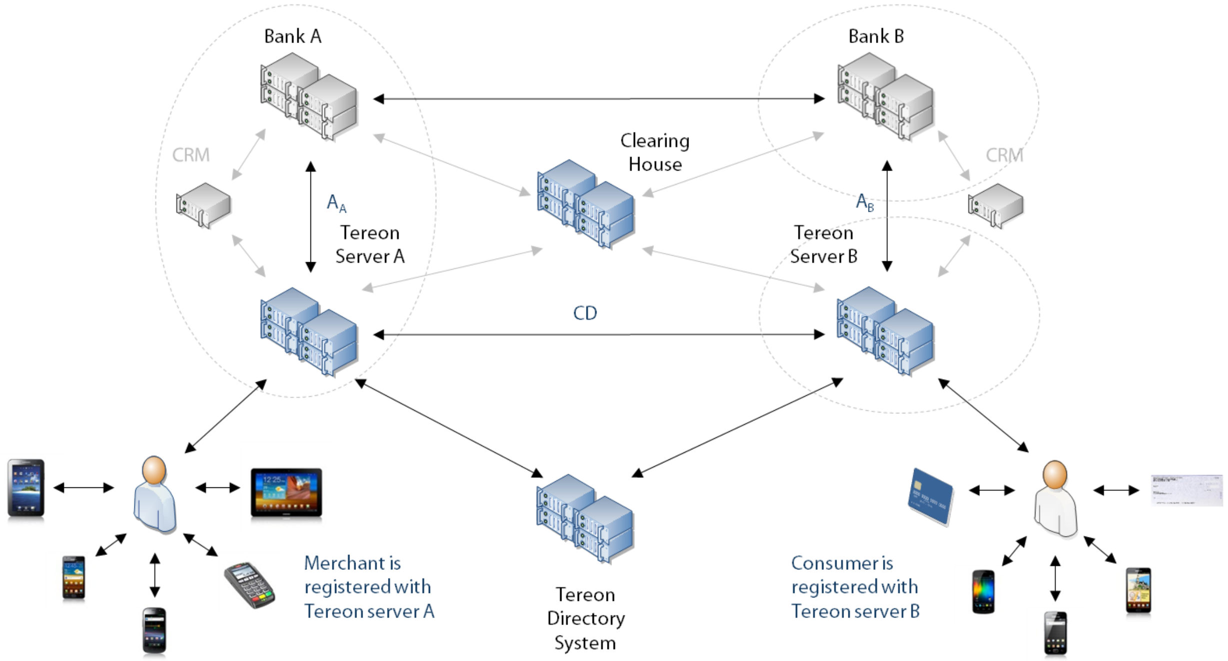


Figure 22 - Audit and contextual data flows

A_A Tereon server A feeds the audit information to bank A's core systems in real-time.

A_B Tereon server B feeds the audit information to bank B's core systems in real-time.

CD Tereon server A and B exchange contextual data.

Figure 22 on the previous page illustrates the data flow for audit information and inter-server contextual data exchanges. These will occur contemporaneously with any transaction and with any action that the servers are involved with. The figure does a poor job of representing the contemporaneous flows, as these will be contemporaneous with every step of every action taken by a server. Nevertheless, the labels identify the connections over which that data will flow.

Tereon does not use the blockchain. The blockchain has far too many issues and flaws in its design to enable it to support real-time transactions at scale. Instead, Tereon has an audit mechanism, for which Kalypton is currently applying for a patent. This mechanism allows it to audit every transaction in real-time and verify each transaction. It does not, unlike the blockchain, need to assume the honesty of any provider, or indeed assume that the majority of providers operate honestly. The audit system audits each and every transaction in a way that means that it will disclose any fraudulent transaction if that transaction is later investigated.

The audit system can capture every action, except the key strokes for a user's password or PIN. (This is a security feature implemented by design. The audit system simply captures the fact that a PIN or password were entered correctly or not.) If a provider enables geolocation functionality on end-devices, then it will capture that data as well, so that the audit will have a full list of the locations of the end-points in any transaction. Though the audit trail captures all of the contextual data surrounding every transaction, the administration system can anonymize that data until the provider or regulator launches a formal investigation. On presentation of a warrant from a competent court, the provider can provide authorities with a full transaction record for the suspect users or transactions. Only authorized administrators or investigators may access the audit trail in detail.

Though the audit system will provide a complete history of transactions, it does allow an administrator to amend or delete a record should that administrator be ordered to do so by a competent court. The administrator can do so without damaging the validity of the audit trail itself, so that all records up to and subsequent to the deleted or amended record remain valid.

Figure 23 on the next page shows the flow for the pre-authentication and the eight lifecycles to this stage.

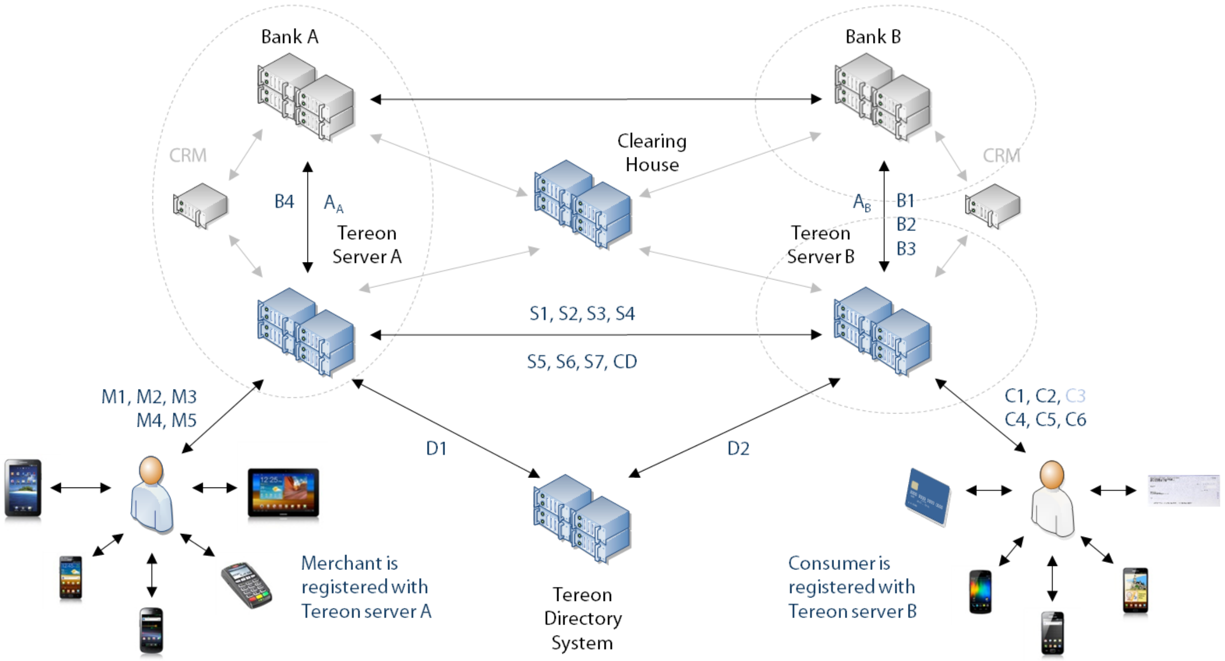


Figure 23 - Pre-authentication, initiation, authentication, payer's authorization, approval by the payer's provider, clearing, settlement, receipt, and the audit and contextual data flows

Part A, Section 2: Use Case Description

This section sets out nine examples of use cases that demonstrate what Tereon does in B2B, B2P, P2B, P2P, and IoT transactions. These are examples only, and reflect examples of the configurations that Tereon can take.

Though these flows set out many individual steps, Tereon can concatenate and combine these steps in order to speed the process where possible. For example, Tereon will often combine some or all of the steps that comprise the inter-provider communications that occur in the lifecycle stages of "*approval by the payer's provider*", "*clearing*", "*receipt*", and "*settlement*".

In each of the figures in this section, the gray lines indicate communication lines that are not involved in the transaction type that the use case is illustrating. The dashed or dotted lines illustrate a communications line that may be offline. For example, the payer in user case 4, the remote emergency bill payment' on page 69, may occur when the recipient is out of hours and so out of communication. Where the dashed lines are to the directory system, then this signifies that the directory system may not be involved in the steps being described. User case 1 on page 60 is one example of this.

Tereon supports 31 baseline functions or use cases. Some of these involve a "push" payment, while involve a "pull". The distinction is that where the initiator of a transaction also initiates a payment, then that is a "push". Where the initiator does not initiate a payment, then the transaction is a "pull". For example –

- in user case 5, the "consumer to merchant payment", on page 72, the merchant initiates the transfer, but the consumer initiates the payment. That is a "pull" transaction, where the merchant "pulls" the eventual payment from the consumer (though the underlying mechanism is that the consumer's bank pushes the payment to the merchant after the consumer accepts the merchant's request for that payment); and
- in user case 9, the "peer-to-peer transfer", on page 90, the transferor both initiates the transaction and initiates the transfer. That is a "push" transaction, where the transferor "pushes" the transfer to the recipient.

It is, of course, possible to reconfigure the business logic for any of the use cases to change all "pull" transactions to operate as "push" transactions, or vice versa. The current flows simply use the affordances of existing familiar payment processes so that the process flows become second nature to the users.

1. B2B – Small value ad hoc payments

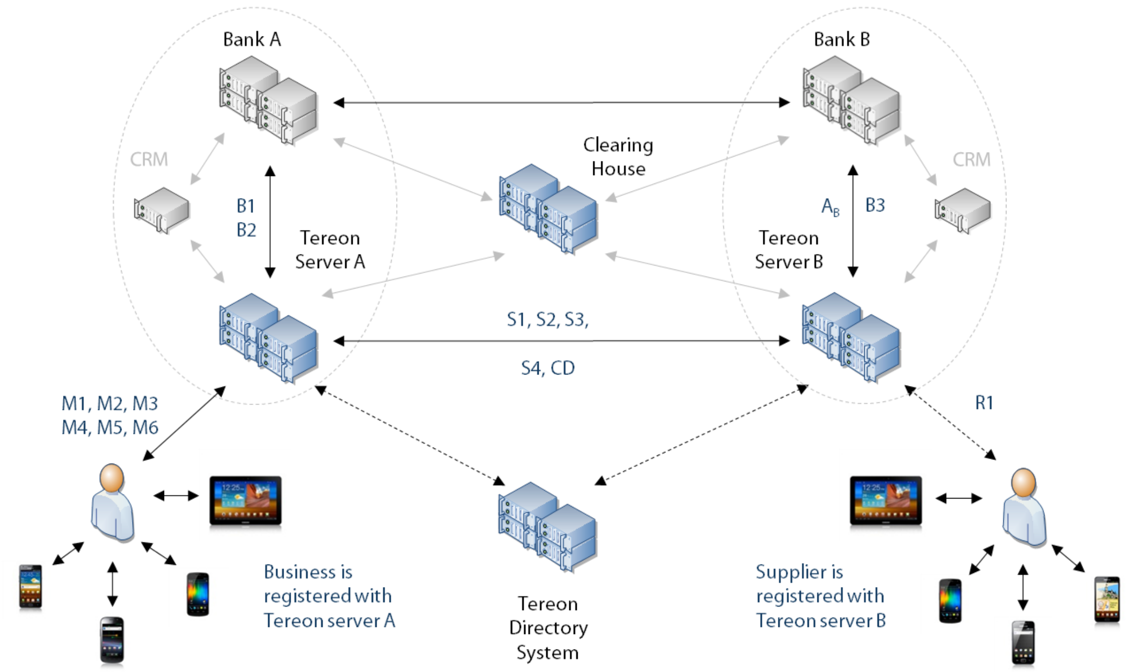


Figure 24 - B2B Small value ad hoc payments

Figure 24 above sets out an example configuration for small value ad hoc payments, such as a low value just-in-time payment to a supplier. This example also shows a deferred payment, in that the payer defers the payment for 14 days as per the invoice terms.

M1 The business owner starts up her device. It communicates with its respective Tereon server, which confirms that the device is correctly registered and that neither the server nor the bank has blocked it.

M2 The server now communicates with the application and displays an identification string that the business owner registered with her business account. This step (which is optional) allows the business owner to confirm that her application is authenticated to her server. The application asks the business owner to enter her application password to access the application. She enters the password, which the device now confirms is correct with its respective Tereon server.

M3 The business owner wants to set up a just-in time payment for $36.78 to cover the cost of a small deliver from her supplier. She must pay that bill in 14 days. She enters the “*Bill payment*” option, and then enters the supplier’s Tereon ID.

The merchant application now contacts Tereon server A and passes the suppliers' ID to the server.

The server checks to see if it has transacted with the supplier's ID before. It has. It does this by checking its own records and then its local directory server that operates as a cache.

M4 The business owner's application now asks for the amount that she needs to pay. The merchant enters $36.78. She then selects the date by which she needs to pay. The application now asks the business owner to enter her PIN.

If the transaction incurs any fees over those that the business owner has accepted in her contract with her provider, then her application will display the fee. She can always cancel the transaction if she refuses to pay the fee.

The application now sends these details to Tereon server A, which checks the PIN against its one-way record of the business owner's PIN.

M5 The business owner's application now confirms that she has configured her account to pay her supplier £36.78 against the invoice in 14 days.

The business owner has now authorized the payment.

S1 As the business owner has not cancelled the pending payment, Tereon server A now contacts Tereon server B to confirm that server B manages the supplier's ID and passes the business's Tereon ID to Tereon server B.

S2 Tereon server B contacts Tereon server A to confirm that it manages the supplier's ID and waits for a response.

B1 Tereon server A instructs bank A to make the payment to the supplier, and provides the transaction number for the payment and the supplier's bank's details (these are not the supplier's bank account but the bank at which the supplier holds its account), and to debit the business's account.

S3 Tereon server A informs Tereon server B that it has cleared the payment.

S4 Tereon server A informs Tereon server B to settle the payment.

B2 Tereon server A instructs the bank to update its settlement accounts in favor of bank B with the transaction number as the reference.

B3 Tereon server B instructs the bank to update its settlement accounts to account for the payment from bank A with the transaction number as the reference, and to credit the account of the supplier with the sum, less any transaction charges.

Tereon instructs the bank to credit the transaction account with the transaction charges (if any) levied on the supplier.

M6 Tereon server A informs the business owner’s system that she has paid the $36.78.

R1 Tereon server B now informs the supplier’s system that it has received a payment from the business with the transaction number and invoice number as references.

During the transaction, the two Tereon servers exchange audit and contextual information.

A_A Tereon server A feeds the audit information to bank A’s core systems in real-time.

A_B Tereon server B feeds the audit information to bank B’s core systems in real-time.

CD Tereon server A and B exchange contextual data.

2. B2P – Wages for a temporary worker

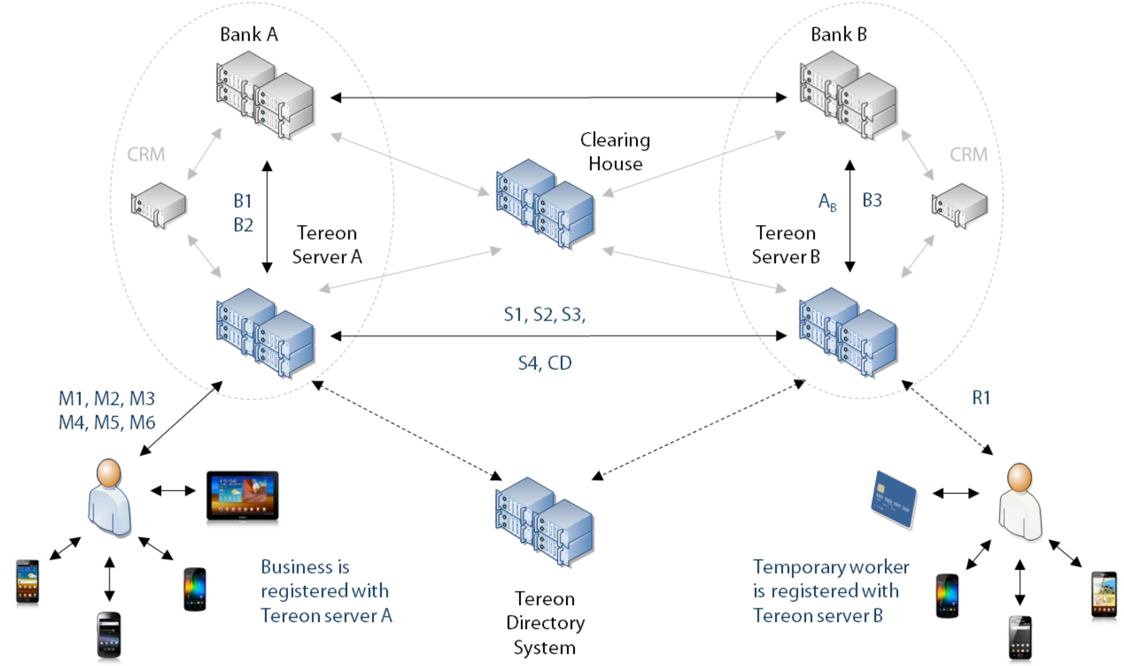


Figure 25 - B2P Wages for a temporary worker

Figure 25 above sets out an example configuration for a business to pay the wages of a temporary worker. This is identical to the first use case, except that in this example the business owner pays the temporary worker immediately. The dotted line between the Temporary worker's device and Tereon server B signifies that the customer may be offline.

M1 The business owner starts up his device. It communicates with its respective Tereon server, which confirms that the device is correctly registered and that neither the server nor the bank has blocked it.

M2 The server now communicates with the application and displays an identification string that the business owner registered with his business account. This step (which is optional) allows the business owner to confirm that his application is authenticated to his server. The application asks the business owner to enter his application password to access the application. He enters the password, which the device now confirms is correct with its respective Tereon server.

M3 The business owner wants to pay the wage of his temporary worker immediately. He enters the "*Bill payment*" option, and then enters the worker's Tereon ID.

The merchant application now contacts Tereon server A and passes the worker's ID to the server.

The server checks to see if it has transacted with the worker's ID before. It has, as he paid his worker last month as well. It does this by checking its own records and then its local directory server that operates as a cache.

M4 The business owner's application now asks for the amount that he needs to pay. The business owner enters $580.00. He then selects the date by which he needs to pay, enters the worker's name as a reference, and selects the option to pay immediately. The application now asks the business owner to enter his PIN.

If the transaction incurs any fees over those that the business owner has accepted in his contract with his provider, then his application will display the fee. He can always cancel the transaction if he refuses to pay the fee.

The application now sends these details to Tereon server A, which checks the PIN against its one-way record of the business owner's PIN.

M5 The business owner's application now confirms that he has configured his account to pay his worker £580.00 immediately.

The business owner has now authorized the payment.

S1 Tereon server A now contacts Tereon server B to confirm that server B manages the worker's ID and passes the business's Tereon ID to Tereon server B.

S2 Tereon server B contacts Tereon server A to confirm that it manages the worker's ID and waits for a response.

B1 Tereon server A instructs bank A to make the payment to the worker, and provides the transaction number for the payment and the worker's bank's details (these are not the worker's bank account but and bank at which the worker holds his account), and to debit the business's account.

S3 Tereon server A informs Tereon server B that it has cleared the payment.

S4 Tereon server A informs Tereon server B to settle the payment.

B2 Tereon server A instructs the bank to update its settlement accounts in favor of bank B with the transaction number as the reference.

B3 Tereon server B instructs the bank to update its settlement accounts to account for the payment from bank A with the transaction number as the reference, and to credit the

account of the worker with the sum. There are no transaction charges levied by this bank or provider to receive transfers.

M6 Tereon server A informs the business owner’s system that he has paid his temporary worker’s wage of $580.00.

R1 Tereon server B now informs the worker’s application that he has been paid $580.00 by the business and that the funds are now in his account.

During the transaction, the two Tereon servers exchange audit and contextual information.

A_A Tereon server A feeds the audit information to bank A’s core systems in real-time.

A_B Tereon server B feeds the audit information to bank B’s core systems in real-time.

CD Tereon server A and B exchange contextual data.

If the business owner employed more than one temporary worker then he could configure his system to pay them on the same day (if that is what he had agreed) using his business’s account portal, or by adding the workers and setting up a deferred payment as per the use case on page 60. He could also link his Tereon system to an accounting package and use that package to instruct Tereon to make the payments.

3. B2P – Ad hoc high-value payments

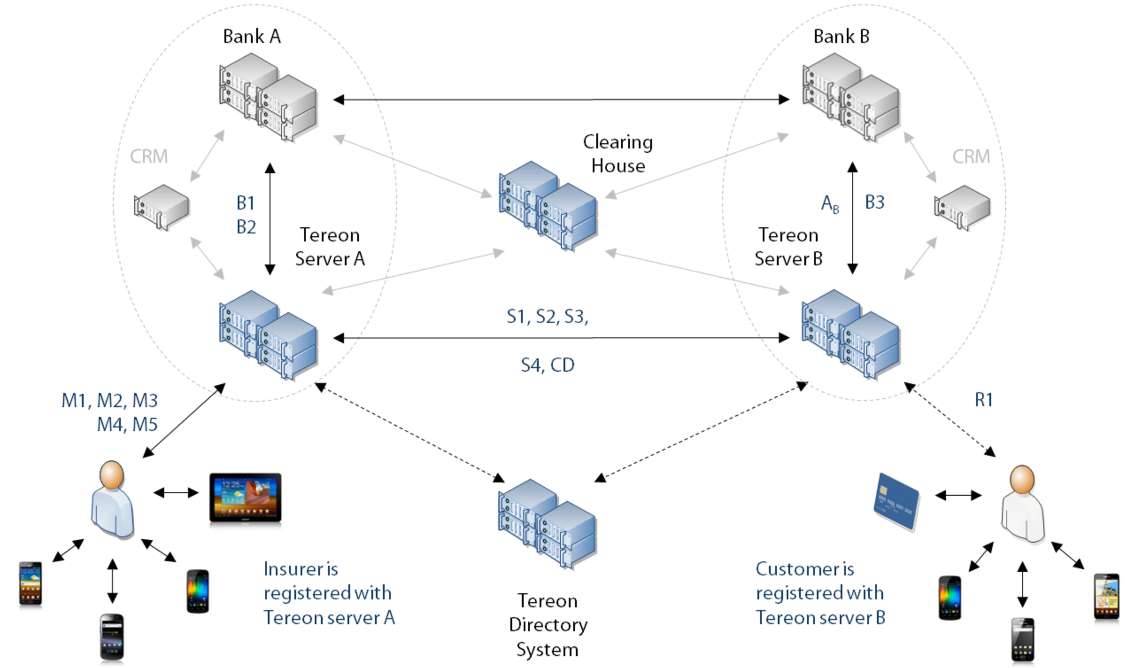


Figure 26 - B2P Ad hoc high-value payments

Figure 26 above sets out an example configuration for an insurance company to pay out an insurance claim to an individual. This is very similar to the first two use cases, except that here the payment is immediate and the value of the payment is high. The dotted line between the customer's device and Tereon server B signifies that the customer may be offline.

M1 The insurance company's systems and payments portal authenticate themselves to Tereon server A and the payments portal confirms that it is authorized and certified.

M2 The insurance company wants to pay out on its customer's claim. The claims clerk enters the "*Claim payment*" option, and then enters the customer's Tereon ID.

The insurance company's systems now contact Tereon server A and passes the customer's ID to the server.

The server checks to see if it has transacted with the customer's ID before. It has, as the customer paid her premiums to the company using Tereon. It does this by checking its own records and then its local directory server that operates as a cache.

M4 The claims clerk enters the customer’s policy number and claim number, and the system automatically enters the amount of the claim, which is $37,096.58. The clerk confirms the amount, and then submits this to her supervisor to approve.

The clerk’s supervisor approves the payment and enters her PIN (for all payments over $10,000 – a business rule that the provider or user can readily adjust).

M5 The insurance company’s system now confirms that it will pay the customer’s claim immediately.

The insurance company has now authorized the payment.

S1 Tereon server A now contacts Tereon server B to confirm that server B manages the customer’s ID and passes the company’s Tereon ID to Tereon server B.

S2 Tereon server B contacts Tereon server A to confirm that it manages the customer’s ID and waits for a response.

B1 Tereon server A instructs bank A to make the payment to the customer, and provides the transaction number for the payment and the customer’s bank’s details (these are not the customer’s bank account but a bank at which the customer holds her account), and to debit the company’s account.

S3 Tereon server A informs Tereon server B that it has cleared the payment.

S4 Tereon server A informs Tereon server B to settle the payment.

B2 Tereon server A instructs the bank to update its settlement accounts in favor of bank B with the transaction number as the reference.

B3 Tereon server B instructs the bank to update its settlement accounts to account for the payment from bank A with the transaction number as the reference, and to credit the account of the customer with the sum. There are no transaction charges levied by this bank or provider to receive transfers.

M6 Tereon server A informs the company’s system that sit has now paid the customer’s claim and that the customer received the payment of $37,096.58.

R1 Tereon server B now informs the customer’s application that she has received her insurance claim of $37,096.58 against the policy and that the funds are in her account.

During the transaction, the two Tereon servers exchange audit and contextual information

A_A Tereon server A feeds the audit information to bank A’s core systems in real-time.

AB Tereon server B feeds the audit information to bank B’s core systems in real-time.

CD Tereon server A and B exchange contextual data.

4. P2B – Remote emergency bill payment

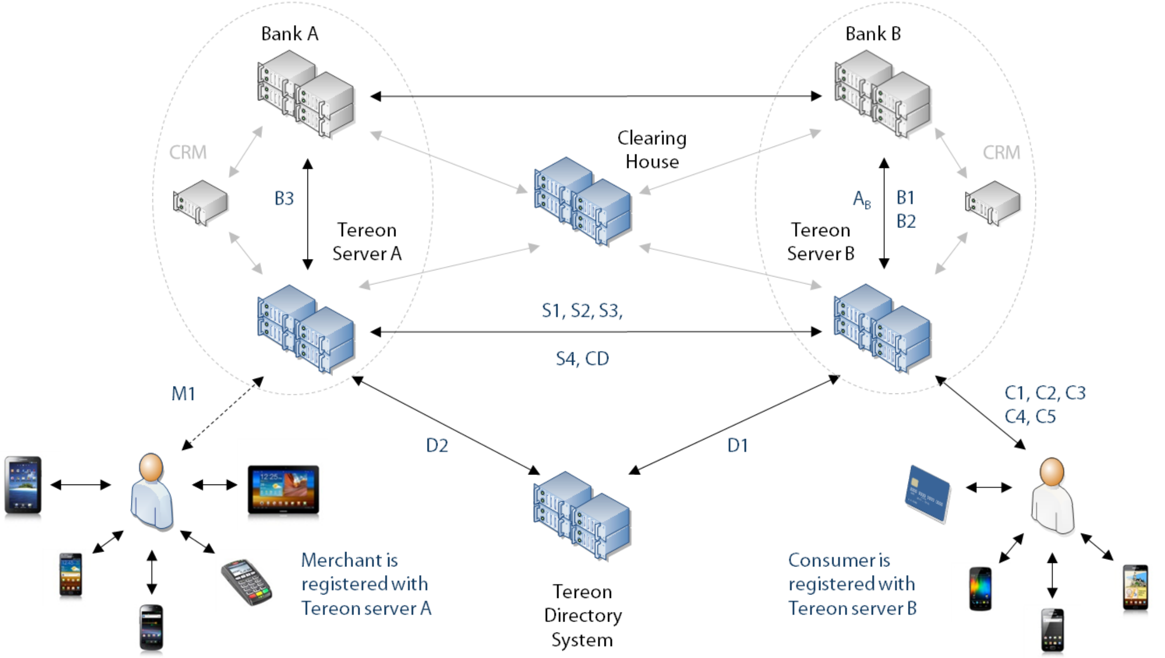


Figure 27 - P2B Remote emergency bill payment

Figure 27 above sets out an example configuration for a consumer to make a remote emergency bill payment. The dotted line between the merchant's device and Tereon server A signifies that the merchant's device is offline, perhaps because it is now out of hours.

C1 The consumer starts up his device. It communicates with its respective Tereon server, which confirms that the device is correctly registered and that neither the server nor the bank has blocked it.

C2 The server now communicates with the application and displays an identification string that the consumer registered with his account. This step (which is optional) allows the consumer to confirm that his application is authenticated to his server. The application asks the consumer to enter his application password to access the application. He enters the password, which the device now confirms is correct with its respective Tereon server.

C3 The consumer needs to pay a bill quickly, as it is now overdue. He enters the "*Bill payment*" option, and then enters the merchant's Tereon ID, which is printed on the overdue invoice.

The consumer’s application now contacts Tereon server A and passes the merchant’s ID to the server.

The server checks to see if it has transacted with the merchant’s ID before. It has not. It does this by checking its own records and then its local directory server that operates as a cache.

D1 Tereon server B’s internal directory server contacts the external directory system and asks it for the server that the merchant is registered with. The directory system verifies that the merchant ID exists and responds with the server ID and its address.

S1 Tereon server B caches the information it has received in its internal directory server and then contacts Tereon server A directly to verify that it manages the merchant’s Tereon ID, and passes the consumer’s Tereon ID to Tereon server.

D2 Tereon server A contacts the external directory system and establishes that Tereon server B manages the consumer’s Tereon ID, and that the server is correctly licensed and authorized to operate.

S2 Tereon server A caches the information that it has received from the directory system in its internal directory server and then contacts Tereon server A directly to confirm that the merchant’s ID is registered with it.

C4 The consumer’s application now asks for the amount that he needs to pay. The consumer enters $67.90. He enters the invoice number as a reference and then selects the option to pay immediately. The application now asks the consumer to enter his PIN.

If the transaction incurs any fees over those that consumer has accepted in his contract with his provider, then his application will display the fee. He can always cancel the transaction if he refuses to pay the fee.

The application now sends these details to Tereon server B, which checks the PIN against its one-way record of the consumer’s PIN.

The consumer has now authorized the payment.

B1 Tereon server B instructs bank B to make the payment to the merchant, and provides the transaction number for the payment and the merchant’s bank’s details (these are not the merchant’s bank account but a bank at which the merchant holds his account), and to debit the consumer’s account.

S3 Tereon server B informs Tereon server A that it has cleared the payment.

S4 Tereon server B informs Tereon server A to settle the payment.

B2 Tereon server B instructs the bank to update its settlement accounts in favor of bank A with the transaction number as the reference.

B3 Tereon server A instructs the bank to update its settlement accounts to account for the payment from bank B with the transaction number as the reference, and to credit the account of the merchant with the sum less any transaction charges.

Tereon instructs the bank to credit the transaction account with the transaction charges levied on the merchant.

C5 Tereon server B informs the consumer that he has paid the merchant $67.90 and that the merchant has received the funds.

M1 Tereon server A will inform the merchant’s application that he has been paid $67.90 when he next starts the application.

During the transaction, the two Tereon servers exchange audit and contextual information.

A_A Tereon server A feeds the audit information to bank A’s core systems in real-time.

A_B Tereon server B feeds the audit information to bank B’s core systems in real-time.

CD Tereon server A and B exchange contextual data.

5. P2B – Consumer to merchant payment

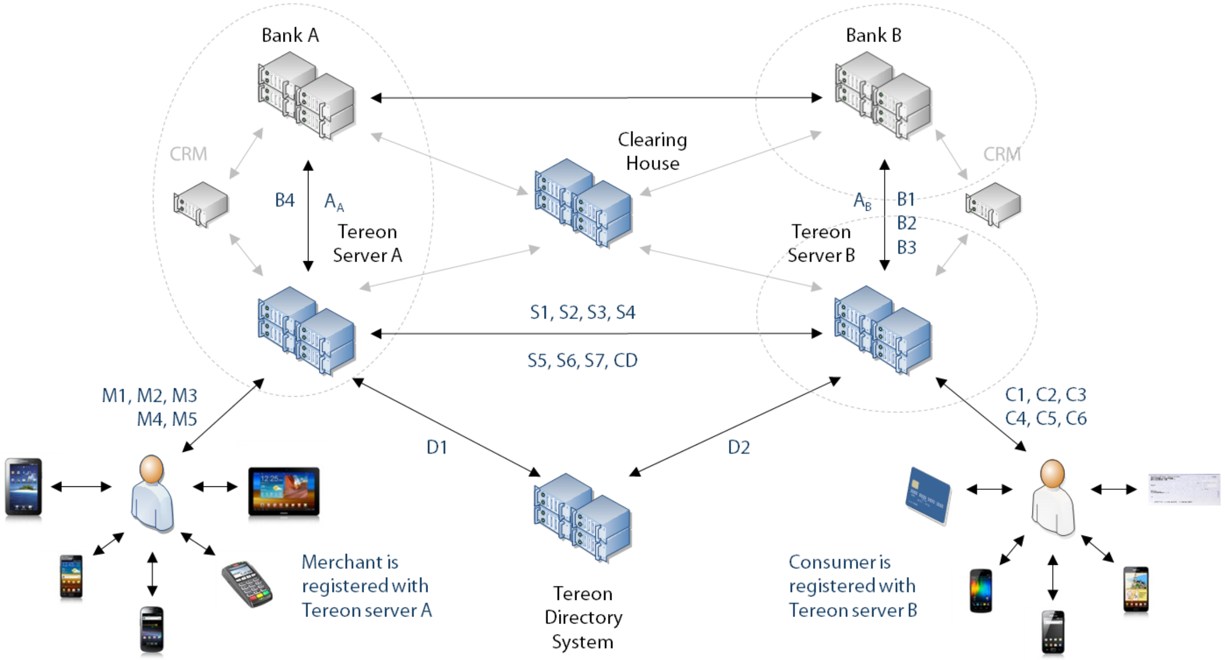


Figure 28 - P2B Consumer to merchant payment

Figure 28 above sets out the flow that was build up in Part A, Section 1 of this document, except that in this flow, both users have NFC-capable devices. The merchant uses a bank that also acts as its provider. The consumer uses a non-bank account provider that holds its funds in a bank. The consumer does not enter her payment details in the browser. Instead, the user enters her payment details via her mobile or tablet. This works whether or not she uses the same device to browse the website and run her application, such as her tablet or smart phone, or two separate devices.

M1,C1 The user starts up her device. It communicates with its respective Tereon server, which confirms that the device is correctly registered and that neither the server nor the bank has blocked it.

M2,C2 The server now communicates with the application and displays an identification string that the user registered with her account. This step (which is optional) allows the user to confirm that her application is authenticated to her server. The application asks the user to enter her application password to access the application. She enters the password, which the device now confirms is correct with its respective Tereon server.

M3 The merchant and consumer want to conclude a transaction, where the consumer wants to pay for goods. The merchant presses the “*Receive payment*” button, and confirms that the consumer is present.

The merchant asks the user to tap her device against the merchant’s terminal, and she does so. The device and terminal identify themselves to each other.

The merchant application now contacts Tereon server A and passes the consumer’s ID and the fact that the consumer is present to the server.

The server checks to see if it has transacted with the consumer ID before. It has not. It does this by checking its own records and then its local directory server that operates as a cache.

D1 Tereon server A’s internal directory server contacts the external directory system and asks it for the server that the customer is registered with. The directory system verifies that the consumer ID exists and responds with the server ID and its address.

C3 The consumer’s device contacts Tereon server B and passes the merchant’s ID to the server. The server checks to see if it has transacted with the merchant ID before. It has not. It does this by checking its own records and then its local directory server that operates as a cache.

D2 Tereon server B contacts the external directory system and establishes that Tereon server A manages the merchant’s Tereon ID, and that the server is correctly licensed and authorized to operate.

S1 Tereon server A caches the information it has received in its internal directory server and then contacts Tereon server B directly to verify that it manages the consumer’s Tereon ID, and passes the merchant’s Tereon ID to Tereon server. Tereon server B confirms that the information that it has received from Tereon server A matches the information it received from the consumer’s device and the directory system.

S2 Tereon server B caches the information that it has received from the directory system in its internal directory server and then contacts Tereon server A directly to confirm that the consumer’s ID is registered with it. Tereon server A confirms that the information that it has received from Tereon server B matches the information it received from the merchant’s device and the directory system.

M4 The merchant’s application now asks for the amount that the consumer must pay. The merchant enters $256.95 and presses “*Sell*”. The application now asks the merchant to enter her PIN (the provider can remove the need to enter a PIN, though it does enable the merchant to track exactly which of her sales assistants took a particular payment).

If the transaction incurs any fees over those that the merchant has accepted in her contract with her provider, then her application will display the fee. She can always cancel the transaction if she refuses to pay the fee.

The application now sends these details to Tereon server A. If the merchant has entered a PIN, then the server first checks the PIN against its one-way record of the merchant's or her sales assistant's PIN.

S3 Tereon server A now passes the payment currency and amount to Tereon server B. Tereon server B confirms receipt and Tereon server A waits for the consumer's response.

C4 Tereon server B checks to see if the consumer is paying in the same currency as the merchant has requested. If so, then the server simply sends the payment amount and the currency code to the customer's application. If not, then the server first contacts bank B for a quote for the payment amount in the consumer's currency, and then passes that amount and the currency code to the consumer's application.

C5 The consumer's application displays the merchant's name or some other identification string that the merchant has registered (never the merchant's Tereon ID), the amount to pay in the consumer's currency, and, if her currency is different to that of the merchant's, the amount in the merchant's currency, the exchange rate and any transaction fee.

The consumer reviews the amount and presses "*Buy*" to make the payment. The application now asks the consumer to enter her payment authorization credential, such as a PIN. This is to prevent an unauthorized payment from the consumer's account.

The consumer enters the PIN and presses "*OK*". The application now sends the customer's PIN to Tereon server B, which confirms it against its one-way record of that consumer's PIN. (If the provider was bank B, then the Tereon server could communicate with that bank's core systems and ask the bank to verify the PIN against its one-way record of the consumer's PIN. The Tereon server would not have a record of the PIN in that case.)

The payer has now authorized the payment.

B1 Tereon server B confirms that the user has sufficient funds in her account or an approved credit facility to cover the payment. It now communicates with the bank to confirm that the bank will be transferring funds from the control account that the bank holds on the provider's behalf, and the bank confirms that the account holds sufficient

funds, or has sufficient credit from an approved credit facility to transfer funds to the recipient's provider.

S4 Tereon server B communicates with Tereon server A to inform it that the consumer has authorized the payment.

B2 Tereon server B instructs the bank to make the transfer or payment to the merchant, and provides the transaction number for the transaction, and the merchant's bank details (these are not the merchant's bank account but the bank at which the merchant holds her account), and to debit the consumer's account.

Tereon server B updates the ledger entry for the consumer to show that her account has been debited, and credits its internal control ledger for payments that will leave the control account

S5 Tereon server B informs Tereon server A that it has cleared the transfer or payment.

S6 Tereon server B informs Tereon server A to settle the payment.

B3 Tereon server B instructs the bank to update its settlement accounts in favor of bank A with the transaction number as the reference.

B4 Tereon server A instructs the bank to update its settlement accounts to account for the payment from bank B with the transaction number as the reference, and to credit the account of the merchant with the sum less any transaction charges.

Tereon instructs the bank to credit the transaction account with the transaction charges (if any) levied on the merchant.

M5 Tereon server A informs the merchant that she has received the funds into her account.

C6 Tereon server B informs the consumer that she has completed the payment.

During the transaction, the two Tereon servers exchange audit and contextual information.

A_A Tereon server A feeds the audit information to bank A's core systems in real-time.

A_B Tereon server B feeds the audit information to bank B's core systems in real-time.

CD Tereon server A and B exchange contextual data.

6. P2B – E-commerce payment

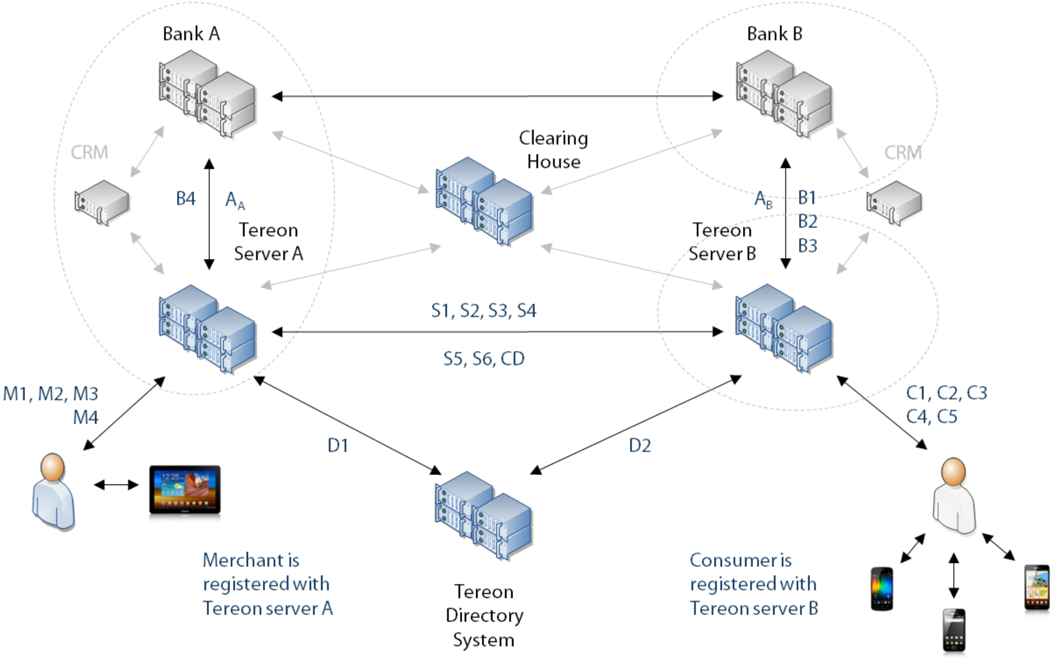


Figure 29 - P2B E-commerce payment

Figure 29 above sets out the flow for a typical e-commerce payment, where the consumer purchases goods or services that are available immediately on payment. The consumer uses a non-bank account provider that holds its funds in a bank.

M1 The merchant's e-commerce site and payments portal authenticate themselves to Tereon server A and the payments portal confirms that it is authorized and certified.

C1 The consumer starts up his device. It communicates with its respective Tereon server, which confirms that the device is correctly registered and that neither the server nor the bank has blocked it.

C2 The server now communicates with the consumer's application and displays an identification string that the consumer registered with his account. This step (which is optional) allows him to confirm that his application is authenticated to his server. The application asks the consumer to enter his application password to access the application. He enters the password, which the device now confirms is correct with its respective Tereon server.

M3 The consumer wants to purchase some goods from the merchant's e-commerce site. He selects the goods, which come to $89.50 and then selects checkout. In the payment options, the consumer selects Tereon and enters his mobile phone number, which is the ID that he has chosen to use. (He has the option to register a Tereon ID with the e-commerce site but he has not done this yet.)

The merchant's e-commerce site now contacts Tereon server A and passes the consumer's ID to the server.

The server checks to see if it has transacted with the consumer ID before. It has not. It does this by checking its own records and then its local directory server that operates as a cache.

D1 Tereon server A's internal directory server contacts the external directory system and asks it for the server that the customer is registered with. The directory system verifies that the consumer ID exists and responds with the server ID and its address.

S1 Tereon server A caches the information it has received in its internal directory server and then contacts Tereon server B directly to verify that it manages the consumer's Tereon ID, and passes the merchant's Tereon ID to Tereon server.

D2 Tereon server B contacts the external directory system and establishes that Tereon server A manages the merchant's Tereon ID, and that the server is correctly licensed and authorized to operate.

S2 Tereon server B caches the information that it has received from the directory system in its internal directory server and then contacts Tereon server A directly to confirm that the consumer's ID is registered with it. Tereon server A confirms that the information that it has received from Tereon server B matches the information it received from the merchant's system and the directory system.

M4 The merchant's payment portal now sends the details of the amount that the consumer must pay for his goods to Tereon server A.

S3 Tereon server A now passes the payment currency and amount to Tereon server B, and informs the server that payment for the entire transaction should be immediate. Tereon server B confirms receipt and Tereon server A waits for the consumer's response.

C3 Tereon server B checks to see if the consumer is paying in the same currency as the merchant has requested. If so, then the server simply sends the payment amount and the currency code to the customer's application. If not, then the server first contacts

bank B for a quote for the payment amount in the consumer’s currency, and then passes that amount and the currency code to the consumer’s application.

C4 The consumer’s application displays the merchant’s name or some other identification string that the merchant has registered (never the merchant’s Tereon ID), the amount to pay in the consumer’s currency, and, if his currency is different to that of the merchant’s, the amount in the merchant’s currency, the exchange rate and any transaction fee.

The consumer reviews the amount and presses “*Buy*” to make the payment. The application now asks the consumer to enter his payment authorization credential, such as a PIN. This is to prevent an unauthorized payment from the consumer’s account.

The consumer enters the PIN and presses “*OK*”. The application now sends the customer’s PIN to Tereon server B, which confirms it against its one-way record of that consumer’s PIN. (If the provider was bank B, then the Tereon server could communicate with that bank’s core systems and ask the bank to verify the PIN against its one-way record of the consumer’s PIN. The Tereon server would not have a record of the PIN in that case.)

The payer has now authorized the payment.

B1 Tereon server B confirms that the consumer has sufficient funds in his account or an approved credit facility to cover the payment. It now communicates with the bank to confirm that the bank will be transferring funds from the control account that the bank holds on the provider’s behalf, and the bank confirms that the account holds sufficient funds, or has sufficient credit from an approved credit facility to transfer funds to the merchant’s provider.

S4 Tereon server B communicates with Tereon server A to inform it that the consumer has authorized the payment.

B2 Tereon server B instructs the bank to make the transfer or payment to the merchant, and provides the transaction number for the transaction, and the merchant’s bank details (these are not the merchant’s bank account but the bank at which the merchant holds his account), and to debit the consumer’s account.

Tereon server B updates the ledger entry for the consumer to show that his account has been debited, and credits its internal control ledger for payments that will leave the control account

S5 Tereon server B informs Tereon server A that it has cleared the transfer or payment.

S6 Tereon server B informs Tereon server A to settle the payment.

B3 Tereon server B instructs the bank to update its settlement accounts in favor of bank A with the transaction number as the reference.

B4 Tereon server A instructs the bank to update its settlement accounts to account for the payment from bank B with the transaction number as the reference, and to credit the account of the merchant with the sum, less any transaction charges.

Tereon instructs the bank to credit the transaction account with the transaction charges (if any) levied on the merchant.

M5 Tereon server A informs the merchant's system that he has received the funds into his account, and the payments portal displays a message that it has received payment and the goods (eBooks and MPS downloads) will be available for download to the consumer immediately.

C5 Tereon server B informs the consumer that he has completed the payment.

During the transaction, the two Tereon servers exchange audit and contextual information.

A_A Tereon server A feeds the audit information to bank A's core systems in real-time.

A_B Tereon server B feeds the audit information to bank B's core systems in real-time.

CD Tereon server A and B exchange contextual data.

If the merchant cannot dispatch the goods until later, then the payment will become a deferred payment. Tereon will hypothecate the consumer's payment and confirm to the merchant that it will complete the payment and credit the funds to the merchant when the merchant confirms that the goods will be dispatched. In this case the flow is very slightly different. The process is as above, except for the following steps:

S3 Tereon server A now passes the payment currency and amount to Tereon server B, and informs the server that payment for $45.00 should be immediate, with $44.50 deferred until dispatch. Tereon server B confirms receipt and Tereon server A waits for the consumer's response.

C3 Tereon server B checks to see if the consumer is paying in the same currency as the merchant has requested. If so, then the server simply sends the payment amount and the currency code to the customer's application. If not, then the server first contacts bank B for a quote for the payment amount in the consumer's currency, and then passes that amount and the currency code to the consumer's application.

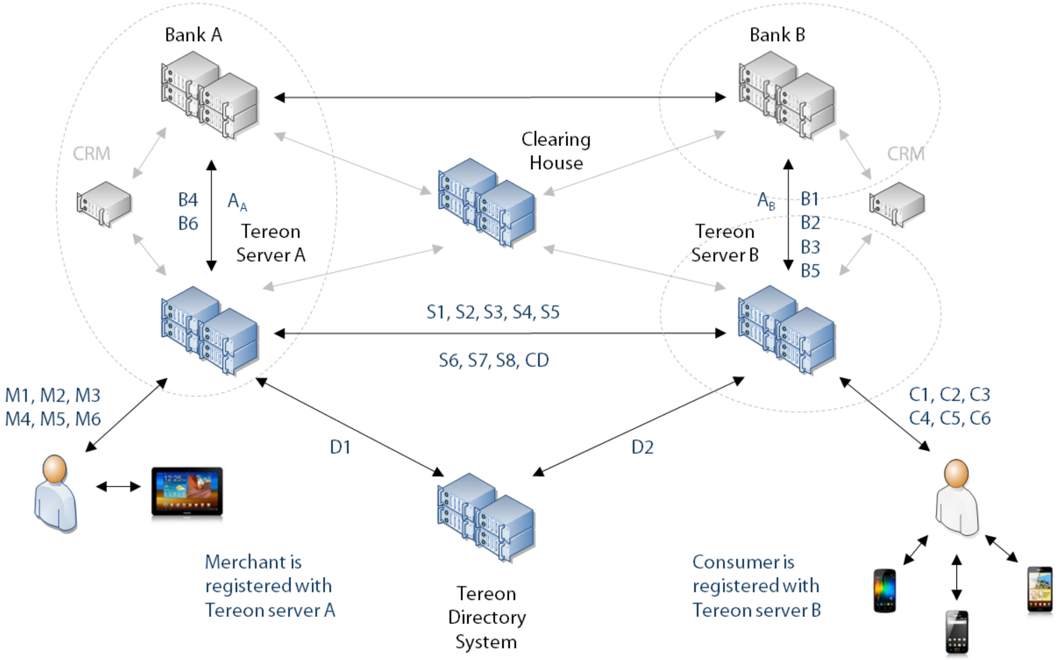


Figure 30 - P2B E-commerce payment with deferred component

Figure 30 above sets out the flow for a typical e-commerce payment. Here part of the payment is deferred as the consumer purchases goods or services that are available immediately on payment, and a good that is not yet in stock.

C4 The consumer's application displays the merchant's name or some other identification string that the merchant has registered (never the merchant's Tereon ID), the amount to pay in the consumer's currency, and, if his currency is different to that of the merchant's, the amount in the merchant's currency, the exchange rate and any transaction fee.

The consumer reviews the amount and presses "*Buy*" to make the payment. The application now asks the consumer to enter his payment authorization credential, such as a PIN. This is to prevent an unauthorized payment from the consumer's account.

The consumer enters the PIN and presses "*OK*". The application now sends the customer's PIN to Tereon server B, which confirms it against its one-way record of that consumer's PIN. (If the provider was bank B, then the Tereon server could communicate with that bank's core systems and ask the bank to verify the PIN against

its one-way record on the consumer's PIN. The Tereon server would not have a record of the PIN in that case.)

The payer has now authorized the payment.

B1 Tereon server B confirms that the consumer has sufficient funds in his account or an approved credit facility to cover the payment. It now communicates with the bank to confirm that the bank will be transferring funds from the control account that the bank holds on the provider's behalf, and the bank confirms that the account holds sufficient funds, or has sufficient credit from an approved credit facility to transfer funds to the merchant's provider.

S4 Tereon server B communicates with Tereon server A to inform it that the consumer has authorized the payment.

B2 Tereon server B instructs the bank to make the transfer or payment to the merchant, and provides the transaction number for the transaction, and the merchant's bank details (these are not the merchant's bank account but the bank at which the merchant holds his account), and to debit the consumer's account.

Tereon server B updates the ledger entry for the consumer to show that his account has been debited, and credits its internal control ledger for payments that will leave the control account

S5 Tereon server B informs Tereon server A that it has cleared the transfer or payment.

S6 Tereon server B informs Tereon server A to settle $45 of the payment.

B3 Tereon server B instructs the bank to update its settlement accounts to the amount of $45 in favor of bank A with the transaction number as the reference.

B4 Tereon server A instructs the bank to update its settlement accounts to account for the payment from bank B with the transaction number as the reference, and to credit the account of the merchant with the sum, less any transaction charges.

Tereon instructs the bank to credit the transaction account with the transaction charges (if any) levied on the merchant.

M5 Tereon server A informs the merchant's system that he has received the funds into his account, and the payments portal displays a message that it has received payment and the goods (eBooks and MPS downloads) will be available for download to the consumer immediately. It also informs the consumer that it will dispatch the remaining goods (a frying pan) in the next few days when it is back in stock.

C5 Tereon server B informs the consumer that he has completed the payment. He can, of course, cancel the remaining part of his order at any time.

M5 When the frying pan is back in stock, the merchant’s website informs Tereon server A to request the final part of the payment, identified by the transaction number.

S7 Tereon server A contacts Tereon server B to request the final part of the payment.

S8 Tereon server B contacts Tereon server A to inform it that it has cleared the final part of the payment.

S9 Tereon server B informs Tereon server A to settle the final $44.50 of the payment.

B5 Tereon server B instructs the bank to update its settlement accounts to the amount of $44.50 in favor of bank A with the transaction number as the reference.

B6 Tereon server A instructs the bank to update its settlement accounts to account for the payment from bank B with the transaction number as the reference, and to credit the account of the merchant with the sum, less any transaction charges.

Tereon instructs the bank to credit the transaction account with the transaction charges (if any) levied on the merchant.

M6 Tereon server A informs the merchant’s system that he has received the funds into his account, and the payments portal sends a message to the consumer to inform him that his frying pan is being dispatched to him.

C6 Tereon server B informs the consumer via an in-application notification that his transaction has now completed in full.

7. P2B – Consumer to merchant card payment

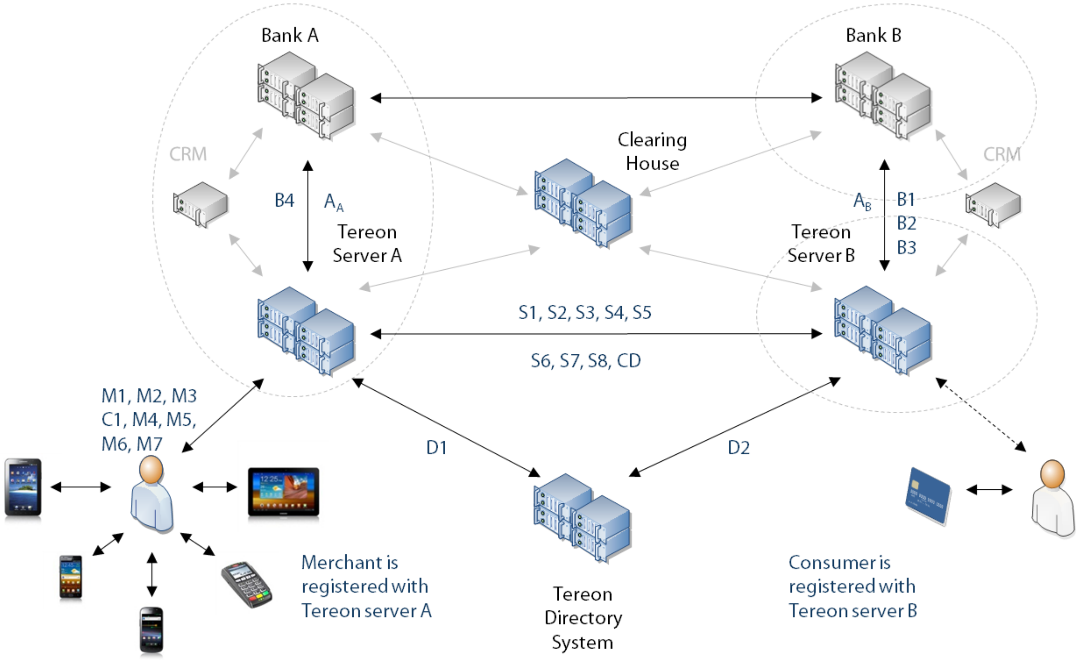


Figure 31 - P2B Card payment

Figure 31 above sets out the flow for a card payment system where both users have NFC-capable devices. In the case of the consumer, she may have several devices, but she is using her NFC-capable card for this payment. If a user has more than one facility registered to a card, for example a debit and a credit facility, then she can select which facility to use for a particular payment. It is important to note that the merchant's device does not check the PIN locally, unlike EMV transactions, and so avoids the risk of attacks via the merchant's device and other well-known EMV attacks.

M1 The merchant starts up her device. It communicates with its respective Tereon Server, which confirms that the device is correctly registered and that the merchant has not blocked it.

M2 The application now asks the merchant to enter her password to access the application. The merchant enters her password, which the device now confirms is correct with its respective Tereon Server.

M3 The merchant and consumer want to conclude a transaction, where the consumer wants to pay for goods. The merchant presses the "*Receive payment*" button, and confirms that the consumer is present.

C1 The merchant asks the user to tap her card against the merchant's device, and she does so. The card and device identify themselves to each other.

M4 The merchant application now contacts Tereon server A and passes the consumer's ID and the fact that the consumer is present to the server.

The server checks to see if it has transacted with the consumer ID before. It has not. It does this by checking its own records and then its local directory server that operates as a cache.

D1 Tereon server A's internal directory server contacts the external directory system and asks it for the server that the customer is registered with. The directory system verifies that the consumer ID exists and responds with the server ID and its address.

S1 Tereon server A caches the information it has received in its internal directory server and then contacts Tereon server B directly to verify that it manages the consumer's Tereon ID, and passes the merchant's Tereon ID to Tereon server.

D2 Tereon server B contacts the external directory system and establishes that Tereon server A manages the merchant's Tereon ID, and that the server and the merchant's device are correctly licensed and authorized to operate.

S2 Tereon server B caches the information that it has received from the directory system in its internal directory server and then contacts Tereon server A directly to confirm that the consumer's ID is registered with it. Tereon server A confirms that the information that it has received from Tereon server B matches the information it received from the merchant's device and the directory system.

M5 The merchant's application now asks for the amount that the consumer must pay. The merchant enters $129.68 and presses "*Sell*". The application now asks the merchant to enter her PIN (the provider can remove the need to enter a PIN, though it does enable the merchant to track exactly which of her sales assistants took a particular payment).

If the transaction incurs any fees over those that the merchant has accepted in her contract with her provider, then her application will display the fee. She can always cancel the transaction if she refuses to pay the fee.

The application now sends these details to Tereon server A. If the merchant has entered a PIN, then the server first checks the PIN against its one-way record of the merchant's or her sales assistant's PIN.

S3 Tereon server A now passes the payment currency and amount to Tereon server B. Tereon server B confirms receipt and Tereon server A waits for the consumer’s response.

C4 Tereon server B checks to see if the consumer is paying in the same currency as the merchant has requested. If not, then the server first contacts bank B for a quote for the payment amount in the consumer’s currency.

S4,M6 The server now contacts the merchant’s device via Tereon server A and displays the amount that the consumer must pay in her own currency. If the consumer uses a different currency to that of the merchant then the terminal will also display the exchange rate, the transaction charges if any, and the total amount in the merchant’s currency that she must pay (the exact mode in which Tereon server B communicates with the merchant’s device here is subject to a patent application).

(If the consumer can make debit and credit payments with the same device, in this case her card, then the terminal will give her the option to choose whether to pay by debit or credit. The merchant can also set her terminal to prefer debit or credit payments if the user has that choice. This flow does not show these options for the sake of clarity.)

The consumer reviews the amount and presses “*Buy*” to make the payment. The application now asks the consumer to enter her payment authorization credential, such as a PIN. This is to prevent an unauthorized payment from the consumer’s account.

The consumer enters the PIN and presses “*OK*”. The application now sends the customer’s PIN to Tereon server B, which confirms it against its one-way record of that consumer’s PIN. (If the provider was bank B, then the Tereon server could communicate with that bank’s core systems and ask the bank to verify the PIN against its one-way record of the consumer’s PIN. The Tereon server would not have a record of the PIN in that case.)

The payer has now authorized the payment.

S5,B1 Tereon server B confirms that the consumer has sufficient funds in her account or an approved credit facility to cover the payment. It now communicates with the bank to confirm that the bank will be transferring funds from the control account that the bank holds on the provider’s behalf, and the bank confirms that the account holds sufficient funds, or has sufficient credit from an approved credit facility to transfer funds to the merchant’s provider.

S6 Tereon server B communicates with Tereon server A to inform it that the consumer has authorized the payment.

B2 Tereon server B instructs the bank to make the transfer or payment to the merchant, and provides the transaction number for the transaction, and the merchant’s bank details (these are not the merchant’s bank account but the bank at which the merchant holds her account), and to debit the consumer’s account.

Tereon server B updates the ledger entry for the consumer to show that her account has been debited, and credits its internal control ledger for payments that will leave the control account

S7 Tereon server B informs Tereon server A that it has cleared the transfer or payment.

S8 Tereon server B informs Tereon server A to settle the payment.

B3 Tereon server B instructs the bank to update its settlement accounts in favor of bank A with the transaction number as the reference.

B4 Tereon server A instructs the bank to update its settlement accounts to account for the payment from bank B with the transaction number as the reference, and to credit the account of the merchant with the sum, less any transaction charges.

Tereon instructs the bank to credit the transaction account with the transaction charges (if any) levied on the merchant.

M7 Tereon server A informs the user that the transaction is complete, and the merchant that she has received the funds into her account.

During the transaction, the two Tereon servers exchange audit and contextual information.

A_A Tereon server A feeds the audit information to bank A’s core systems in real-time.

A_B Tereon server B feeds the audit information to bank B’s core systems in real-time.

CD Tereon server A and B exchange contextual data.

8. P2B – Check payment

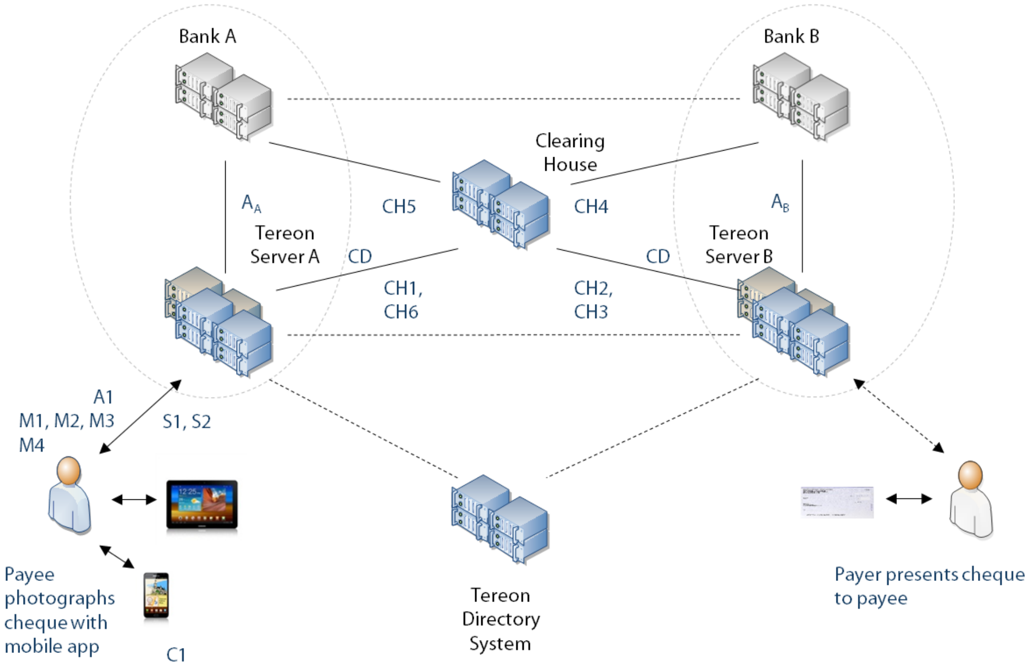


Figure 32 - P2B Check payment

Figure 32 above sets out the flow for a check payment system where the providers use a central clearing house at which they also settle their inter-provider check payments. This is the only example in this document where the providers use a central clearing house. This process is modeled on the initial Tereon implementation in Central America. The objective there is to deliver straight-through and real-time check processing.

M1 The merchant starts up his device. It communicates with its respective Tereon Server, which confirms that the device is correctly registered and that the merchant has not blocked it.

M2 The application now asks the merchant to enter his password to access the application. The merchant enters his password, which the device now confirms is correct with its respective Tereon Server.

The consumer writes out a check and hands that to the merchant.

M3 The merchant selects "*Process check*" and uses his application to take a photograph of the front of the check. The merchant does not need to photograph the rear of the check and so selects "*Done*".

The merchant now enters the date of the check and amount on the check, and selects "*Submit*". The application transmits the image or images that it has captured, together with the date of the check and the amount on the check, to the Tereon server, which identifies the merchant as the payer via that merchant's Tereon ID.

CH2 The clearing house's Tereon server now communicates with the Tereon server of the bank on which the consumer drew the check to inform it of the check's status.

If the check has been presented before then the server will flag this to the administrator, who can take investigative action.

If the check is validly presented, then the server will process the image and compare –

- the amount detected with the amount entered by the merchant
- the date detected with the date entered by the merchant; and
- the signature on the check against the sample signatures held against the account on which the check is drawn (if the consumer's bank verifies signatures, as not all banks do so).

CH3 If the server processes the check successfully and verifies the date then it informs the clearing house that it has processed and approved the check.

CH4 The clearing house now settles the check between bank A and bank B through its existing settlement network with its member banks. Its connection with bank B instructs the bank to debit the payer's account and to credit the settlement account in favor of bank A. The clearing house updates the settlement accounts that it holds for bank B to show that the bank has "transferred funds" to the clearing house's settlement accounts.

CH5 The clearing house now instructs bank A via its connection that it has received an amount from bank B. The clearing house updates bank A's settlement accounts to credit it with the funds, and instructs bank A to credit the merchant's account with the funds.

CH6 The clearing house informs the merchant's Tereon server that it has cleared the check. The clearing house also informs the server that it has settled the check.

M4 The merchant's server informs the merchant's device that the check has cleared, and the device notifies the merchant that the check has been cleared and, that he is now in funds.

During the transaction, the two Tereon servers exchange audit and contextual information.

A_A Tereon server A feeds the audit information to bank A's core systems in real-time.

A_B Tereon server B feeds the audit information to bank B's core systems in real-time.

CD The Tereon servers exchange contextual data via the clearing house.

If two or more clearing houses serve separate providers for the purposes of clearing checks, then Tereon can scale to connect these clearing houses and so enable any provider to accept and present checks from any other provider. Figure 33 below illustrates a configuration where Tereon connects multiple clearing houses. This document does not set out the steps for this configuration.

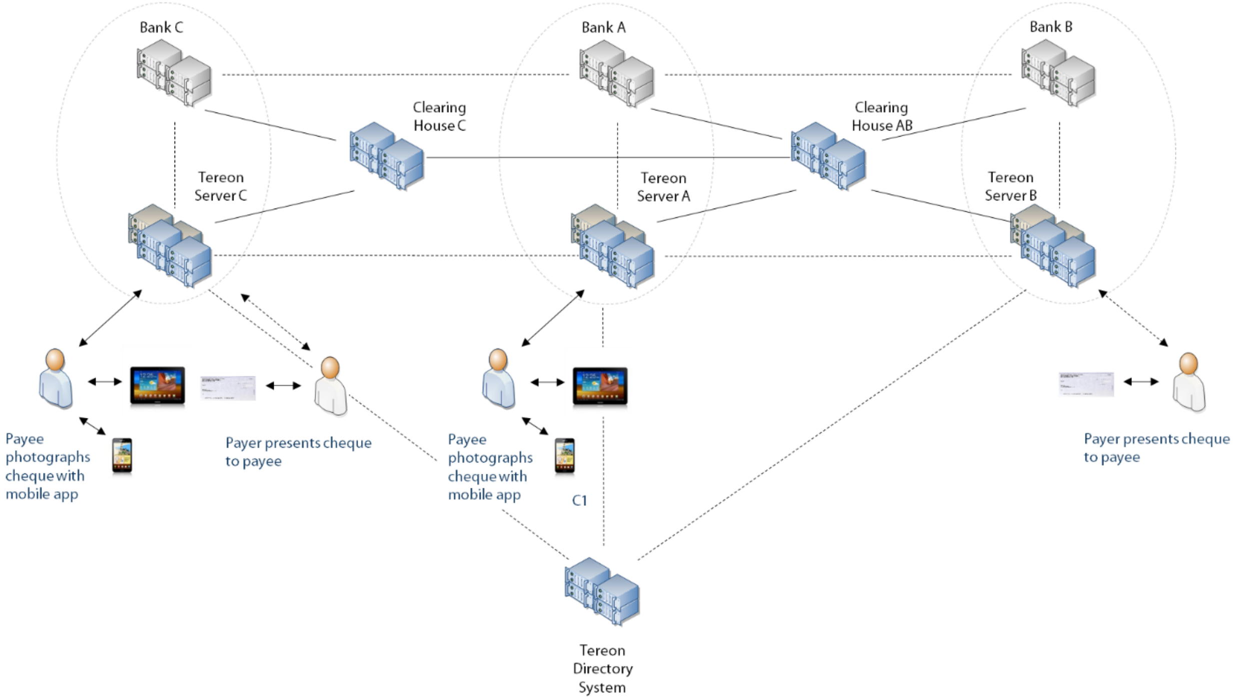

Bank C
Bank A
Bank B
Clearing House C
Clearing House AB
Tereon Server C
Tereon Server A
Tereon Server B
Payee photographs cheque with mobile app
Payer presents cheque to payee
Payee photographs cheque with mobile app
C1
Payer presents cheque to payee
Tereon Directory System

Figure 33 - P2B Check payment with multiple clearing houses

9. P2P – Peer-to-peer transfer

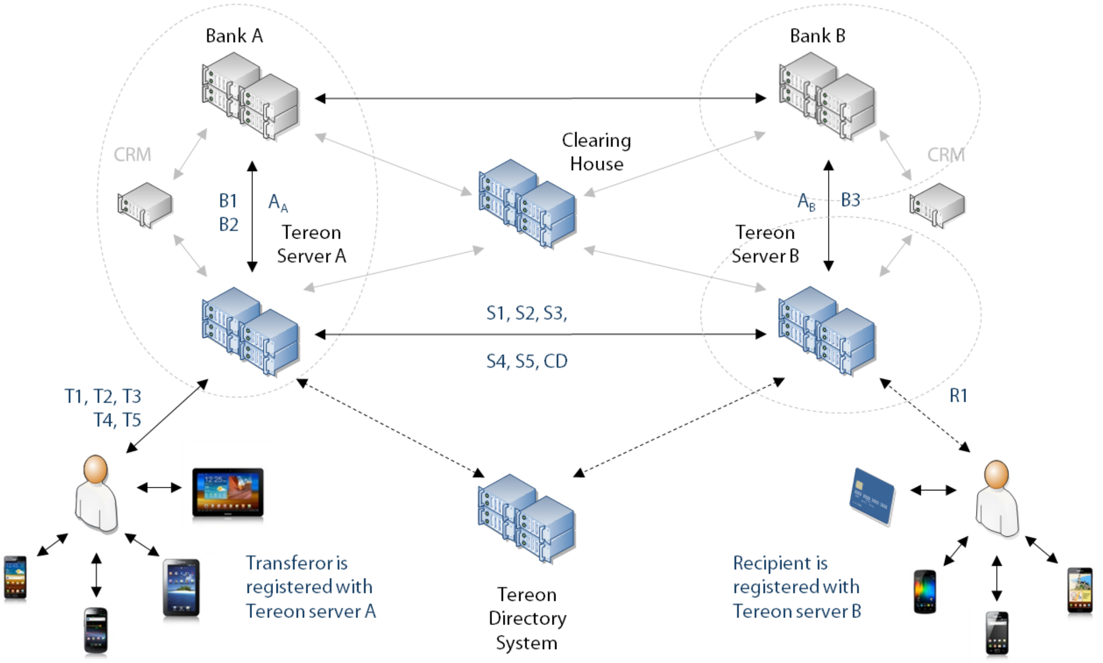


Figure 34 - P2P Transfer

Figure 34 above sets out an example configuration of a peer-to-peer transfer between two registered users of Tereon. A real-world example might be one friend paying another, or a parent transferring a sum of money to her child.

T1 The transferor starts up her device. It communicates with its respective Tereon server, which confirms that the device is correctly registered and that neither the server nor the bank has blocked it.

T2 The transferor's server now communicates with the transferor's application and displays an identification string that the transferor registered with her account. This step (which is optional) allows her to confirm that her application is authenticated to her server. The application asks the transferor to enter her application password to access the application. She enters the password, which the device now confirms is correct with its respective Tereon server.

T3 The transferor wants to transfer $150 to the recipient. She selects "*Make a transfer*" and selects the recipient's details from her list of contacts. Her application contacts Tereon server A and passes the recipient's ID to the server.

The server checks to see if it has transacted with the recipient’s ID before. It has. It does this by checking its own records and then its local directory server that operates as a cache.

S1 Tereon server A contacts Tereon server B directly to verify that it manages the recipient’s Tereon ID, passes the transferor’s Tereon ID to Tereon server, and informs the server that it wishes to make a transfer to the recipient.

S2 Tereon server B contacts Tereon server A directly to confirm that the recipient’s ID is registered with it, and passes details of the recipient’s currency to the Tereon server.

T4 The transferor enters the amount that she wishes to transfer to the recipient, and then selects transfer. Tereon server A now checks to see what currency the recipient can receive. If it is a different currency then the server contacts bank A for a quote for the transfer in the recipient’s currency, and then passes that amount, the currency code, the exchange rate, and any charges for the exchange to the transferor’s application.

Her application now displays the amount that she wants to transfer to the recipient, any transfer charges, and any options as to who should pay the transfer charges. The options may be that the transferor pays the charges, the recipient pays the charges, or they share the charges equally.

If the recipient’s currency is different to that of the transferor, then the application will also display the currency and amount in that currency the recipient will receive, the exchange rate, and any additional charges for the exchange.

The application now asks the transferor to enter her payment authorization credential, such as a PIN. This is to prevent an unauthorized transfer from her account.

The transferor enters the PIN and presses “*OK*”. The application now sends the transferor’s PIN to Tereon server A, which confirms it against its one-way record of that consumer’s PIN. (The provider is a bank, so the Tereon server could communicate with that bank’s core systems and ask the bank to verify the PIN against its one-way record on the consumer’s PIN. The Tereon server would not have a record of the PIN in that case.)

The transferor has now authorized the transfer.

S3 Tereon server A communicates with Tereon server B to inform it that the transferor has authorized a transfer.

B1 Tereon server A instructs the bank to make a transfer to the recipient, and provides the transaction number for the transaction, and the recipient’s providers’ bank details

(these are not the recipient's bank account, as the recipient has an account with a non-bank account provider that retains the funds in a control account in bank B), and to debit the transferor's account.

S4 Tereon server A informs Tereon server B that it has cleared the transfer. It sends the transferor's name and address and the recipient's name and address to Tereon server B, as required by AML regulations.

S5 Tereon server A informs Tereon server B to settle the payment.

B2 Tereon server A instructs the bank to update its settlement accounts in favor of bank B with the transaction number as the reference.

B3 Tereon server B instructs the bank to updates its settlement accounts to account for the transfer from bank A with the transaction number, and to credit the control account with the sum, less any transaction charges that the recipient must pay.

Tereon instructs the bank to credit the transaction account with the transaction charges (if any) levied on the recipient.

T5 Tereon server A informs the transferor that she has successfully transferred the sum to the recipient.

R1 Tereon server B will inform the recipient that she has received a transfer from the transferor when the recipient next accesses Tereon. If the recipient has configured email or text notifications, then Tereon will uses these channels to inform her of the transfer as well.

During the transaction, the two Tereon servers exchange audit and contextual information.

A_A Tereon server A feeds the audit information to bank A's core systems in real-time.

A_B Tereon server B feeds the audit information to bank B's core systems in real-time.

CD The Tereon servers exchange contextual data via the clearing house.

10. P2P – User to unregistered user transfer

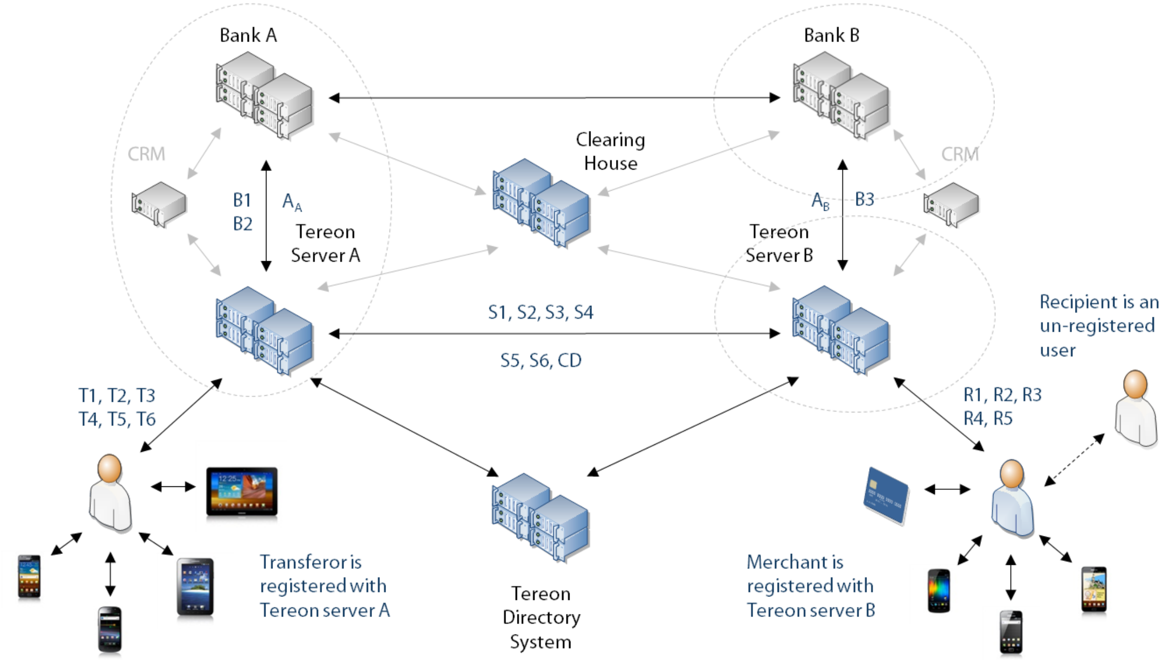


Figure 35 - P2P Transfer to an unregistered user

Figure 35 above sets out an example configuration of a peer-to-peer transfer between a registered user of Tereon and an unregistered user.

T1 The transferor starts up his device. It communicates with its respective Tereon server, which confirms that the device is correctly registered and that neither the server nor the bank has blocked it.

T2 The transferor's server now communicates with the transferor's application and displays an identification string that the transferor registered with his account. This step (which is optional) allows his to confirm that his application is authenticated to his server. The application asks the transferor to enter his application password to access the application. He enters the password, which the device now confirms is correct with its respective Tereon server.

T3 The transferor wants to transfer $110 to the recipient. He selects "*Make a transfer*", selects the recipient's mobile number from his list of contacts, and sets the date by which the recipient must access the funds. (If the recipient fails to access the funds by that date then Tereon will cancel the transfer and return the funds, less any costs, to the transferor's account.)

The recipient is an unregistered user, and the transferor has never transferred sums to him before. The transferor's application asks him to enter the recipient's name and address into a dialog box.

T4 The transferor enters the amount that he wishes to transfer to the recipient, and then selects transfer. Tereon server A now checks to see what currency the recipient can receive from the address that the transferor provided. If it is a different currency then the server contacts bank A for a quote for the transfer in the recipient's currency, and then passes that amount, the currency code, the exchange rate, and any charges for the exchange to the transferor's application.

His application now displays the amount that he wants to transfer to the recipient, any transfer charges, and any options as to who should pay the transfer charges. The options may be that the transferor pays the charges, the recipient pays the charges, or they share the charges equally.

If the recipient's currency is different to that of the transferor, then the application will also display the currency and amount in that currency the recipient will receive, the exchange rate, and any additional charges for the exchange.

The application now asks the transferor to enter his payment authorization credential, such as a PIN. This is to prevent an unauthorized transfer from his account.

The transferor enters the PIN and presses "*OK*". The application now sends the transferor's PIN to Tereon server A, which confirms it against its one-way record of that consumer's PIN. (The provider is a bank, so the Tereon server could communicate with that bank's core systems and ask the bank to verify the PIN against its one-way record on the consumer's PIN. The Tereon server would not have a record of the PIN in that case.)

The transferor has now authorized the transfer.

T5 The transferor's application now displays a transaction number, which it also sends by text to the recipient's mobile number. It also displays a collection PIN that the transferor needs to send to the recipient by another channel. The transferor can always access the mini-statement for the transaction and recover these two credentials up until the point at which the recipient collects the funds.

B1 Tereon server A instructs the bank to credit its transfer account with the sum transferred, less any transfer charges, and to debit the transferor's account.

In order to collect the funds, the recipient must visit a Tereon-enabled merchant within the time period specified by the transferor.

R1 The recipient hands the transaction number to the merchant, who enters the number into his device.

D1 Tereon server B’s internal directory server contacts the external directory system and asks it for the server that registered the transaction number for the transfer. The directory system responds with the server ID and address for Tereon server A.

S1 Tereon server B contacts Tereon server A to request that it confirms that it manages the transaction number and that it wishes to access the funds on behalf of the recipient, and passes the merchant’s Tereon ID to Tereon server.

D2 Tereon server A’s internal directory server contacts the external directory system and asks to confirm and that the server and the merchant’s device are correctly licensed and authorized to operate. The directory system responds with the server ID and address for Tereon server B.

S3, R2 Tereon server A now contacts the merchant’s device via Tereon server B and requests that the recipient enter his collection PIN (the exact mode in which Tereon server A communicates with the merchant’s device here is subject to a patent application).

The recipient enters the PIN and presses “*OK*”. The application now sends the collection PIN to Tereon server A, which confirms it against its one-way record of that collection PIN. (If the provider was bank A, then the Tereon server could communicate with that bank’s core systems and ask the bank to verify the PIN against its one-way record of the transaction’s PIN. The Tereon server would not have a record of the PIN in that case.)

S4 Tereon server A communicates with Tereon server B to inform it that the transferor has authorized a transfer.

B2 Tereon server A instructs the bank to make a transfer to the recipient, and provides the transaction number for the transaction, and the merchant’s providers’ bank details (these are not the merchant’s bank account, nor are they the recipient’s bank details as the recipient is an unregistered user. They are the details for the control account held by bank B on behalf of the merchant’s provider), and to debit the server’s transfer account.

S5 Tereon server A informs Tereon server B that it has cleared the transfer. It sends the transferor’s name and address and the recipient’s name and address to Tereon server B, as required by AML regulations.

S6 Tereon server A informs Tereon server B to settle the payment.

B3 Tereon server A instructs the bank to update its settlement accounts in favor of bank B with the transaction number as the reference.

B4 Tereon server B instructs the bank to updates its settlement accounts to account for the transfer from bank A with the transaction number, and to credit the control account with the sum, less any transaction charges that the recipient must pay. The Tereon server credits its transaction ledger with the amount that the recipient will receive.

Tereon instructs the bank to credit the transaction account with the transaction charges (if any) levied on the recipient.

T6 Tereon server A now informs the transferor that the recipient has accessed his transfer. The transferor cannot revoke the transaction after this point.

R3 The merchant's device displays the amount that the recipient can collect, in the recipient's currency. The merchant confirms to the recipient that he has sufficient cash to satisfy the amount that the recipient wishes to collect, and the recipient enters the amount he wishes to collect, enters his collection PIN again, and presses "*OK*". (If the recipient only collects part of the funds, then Tereon will retain the remaining funds against a ledger entry for the recipient to collect at another time.)

Tereon server B now checks the PIN against the one-way record that it now has of the collection PIN.

R4 The merchant's device displays the amount that the merchant must had to the recipient. The merchant hands the money to the recipient, and enters his PIN (the provider can remove the need to enter a PIN, though it does enable the merchant to track exactly which of his sales assistants took a particular transaction).

R5 The Tereon server credits the merchant's ledger with the amount that the recipient has collected, debits the transfer ledger, and displays a message on the merchant's device that the transaction is complete.

During the transaction, the two Tereon servers exchange audit and contextual information.

A_A Tereon server A feeds the audit information to bank A's core systems in real-time.

A_B Tereon server B feeds the audit information to bank B's core systems in real-time.

CD The Tereon servers exchange contextual data via the clearing house.

11. IoT – Smart refrigerator

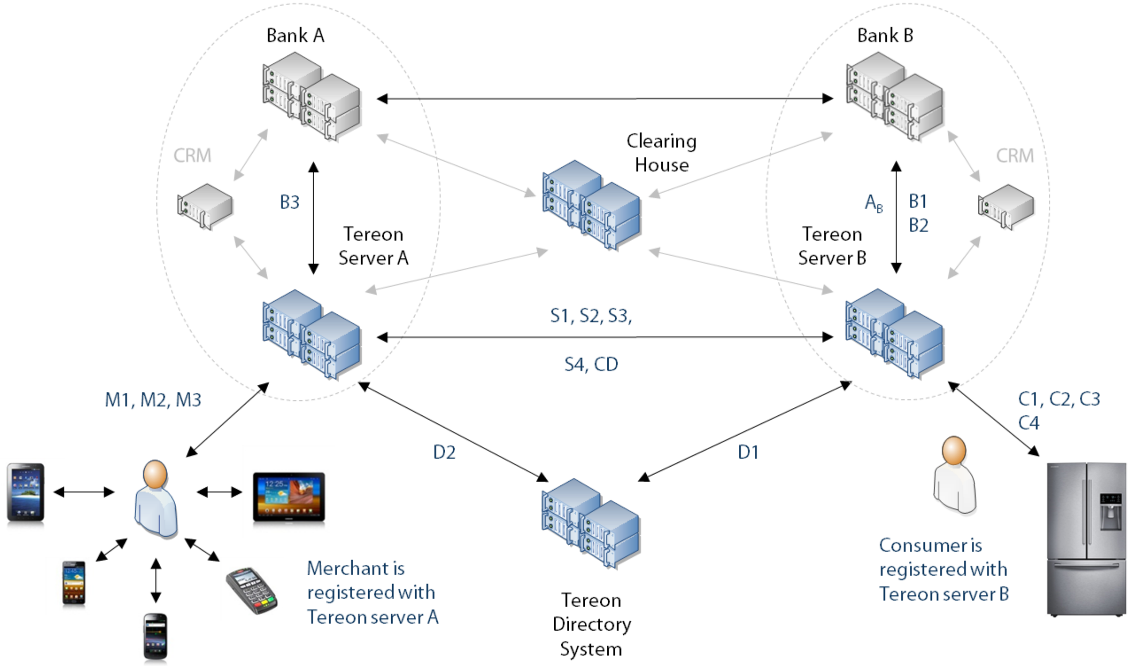


Figure 36 - IoT Smart refrigerator payment

Figure 36 above is an example configuration of a domestic smart appliance placing an order within preset spending limits and parameters. It is an example of an automated pre-authorized payment.

C1 The consumer’s smart refrigerator authenticates itself to Tereon server A and confirms that it is authorized and certified.

M1 The smart refrigerator has detected that the consumer is running low on milk. The consumer has already set the refrigerator to order the weekly shop, ready for the consumer to collect that evening. The consumer’s daughter had, in the meantime used up the milk, and failed to update the shopping list.

The refrigerator’s self-ordering parameters allow it to adjust the weekly shop by up to $20, so it adds two pints of milk to the order.

The refrigerator’s application now contacts the merchant’s e-commerce portal to place the weekly shopping order, together with the additional two pints of milk. The order comes to $92.56, which is within the acceptable parameters of an automatic order.

The refrigerator passes the consumer's Tereon ID, which she created especially for the smart refrigerator with a weekly spending limit of $200, to the e-commerce portal. The merchant's e-commerce site now contacts Tereon server A and passes the consumer's ID to the server.

The server checks to see if it has transacted with the consumer ID before. It has, as she (or rather the refrigerator) is a regular customer. It does this by checking its own records and then its local directory server that operates as a cache.

M2 The merchant's payment portal now sends the details of the amount that the consumer must pay for her goods to Tereon server A.

S1 Tereon server A now passes the payment currency and amount to Tereon server B, and informs the server that payment for the entire transaction should be immediate. Tereon server B confirms receipt and Tereon server A waits for the consumer's response.

B1 As the payment is pre-authorized, as it is made against the Tereon ID created for pre-authorized payments and comes within the weekly spending limit of $200, Tereon server B instructs bank B to make the payment to the merchant, and provides the transaction number for the payment and the merchant's bank's details (these are not the merchant's bank account but and bank at which the merchant holds her account), and to debit the consumer's account.

S3 Tereon server B informs Tereon server A that it has cleared the payment.

S4 Tereon server B informs Tereon server A to settle the payment.

B2 Tereon server B instructs the bank to update its settlement accounts in favor of bank A with the transaction number as the reference.

B3 Tereon server A instructs the bank to update its settlement accounts to account for the payment from bank B with the transaction number as the reference, and to credit the account of the merchant with the sum less any transaction charges.

Tereon instructs the bank to credit the transaction account with the transaction charges levied on the merchant.

C4 Tereon server B informs the refrigerator that it has paid the merchant $92.56 and that the merchant has received the funds, and informs the consumer that she can pick up her groceries that evening.

M3 Tereon server A informs the merchant's systems that it has been paid $92.56 for the order of groceries that the consumer will collect that evening.

During the transaction, the two Tereon servers exchange audit and contextual information.

A_A Tereon server A feeds the audit information to bank A’s core systems in real-time.

A_B Tereon server B feeds the audit information to bank B’s core systems in real-time.

CD Tereon server A and B exchange contextual data.

The refrigerator could just have easily ordered milk, eggs, or any other necessary supplies as a separate order and informed the consumer of that order. Here, because it was due to order a weekly shop, the refrigerator simply appended the extra items to the order. This is an example of automated pre-authorized payments made via Tereon.

Part A, Section 3: Use Case by Effectiveness Criteria

The table below sets out the effectiveness criteria addressed by each of the use cases that Tereon supports (business to business; business to person; person to business and/or person to person, as indicated in the table "Supported use case coverage summary", above). Some of these lifecycle stages occur simultaneously, as indicated in the discussion in part A section 1 of this proposal.

Use case by effectiveness criteria					
Lifecycle stage	**Criteria**	**B2B (Y/N)**	**B2P (Y/N)**	**P2B (Y/N)**	**P2P (Y/N)**
Initiation	U.1	Y	Y	Y	Y
	U.2	Y	Y	Y	Y
	U.3	Y	Y	Y	Y
	U.4	Y	Y	Y	Y
	U.5	Y	Y	Y	Y
	U.6	Y	Y	Y	Y
	E.4	Y	Y	Y	Y
	S.7	Y	Y	Y	Y
	S.9	Y	Y	Y	Y
Authentication	U.2	Y	Y	Y	Y
	U.3	Y	Y	Y	Y
	S.7	Y	Y	Y	Y
	S.9	Y	Y	Y	Y
	S.10	Y	Y	Y	Y
Payer Authorization	U.2	Y	Y	Y	Y
	U.3	Y	Y	Y	Y
	S.2	Y	Y	Y	Y
	S.7	Y	Y	Y	Y
	S.9	Y	Y	Y	Y
Approval by the Payer's Provider	S.3	Y	Y	Y	Y
	S.7	Y	Y	Y	Y
	S.9	Y	Y	Y	Y
	F.1	Y	Y	Y	Y
	F.5	Y	Y	Y	Y

Use case by effectiveness criteria					
Lifecycle stage	**Criteria**	**B2B (Y/N)**	**B2P (Y/N)**	**P2B (Y/N)**	**P2P (Y/N)**
Clearing	E.4	Y	Y	Y	Y
	S.7	Y	Y	Y	Y
	S.9	Y	Y	Y	Y
	F.2	Y	Y	Y	Y
Receipt	U.1	Y	Y	Y	Y
	U.2	Y	Y	Y	Y
	U.3	Y	Y	Y	Y
	U.6	Y	Y	Y	Y
	S.5	Y	Y	Y	Y
	S.7	Y	Y	Y	Y
	S.9	Y	Y	Y	Y
	F.3	Y	Y	Y	Y
	F.5	Y	Y	Y	Y
Settlement	S.4	Y	Y	Y	Y
	S.7	Y	Y	Y	Y
	S.9	Y	Y	Y	Y
	F.4	Y	Y	Y	Y
Reconciliation	U.3	Y	Y	Y	Y
	E.7	Y	Y	Y	Y
	S.5	Y	Y	Y	Y
	S.6	Y	Y	Y	Y
	S.7	Y	Y	Y	Y
	S.9	Y	Y	Y	Y

PART B: BUSINESS CONSIDERATIONS

1. Implementation Timeline

Version 4 of Tereon will be available within the next six months. It will be able to support all of the use cases and baseline functionality set out in this document. The use cases illustrate that, for the most part, the configurations required to support the various use cases are very similar. It is the business logic behind the actual use cases that differs.

Kalypton has designed Tereon to make it possible for third-party systems integrators, consultancies, and even providers themselves to implement Tereon. Tereon's built-in interoperability for both domestic and cross-border transactions would enable the providers to interconnect their systems, irrespective of which systems integrator has implemented a particular provider's solution. This facilitates parallel implementation, whereby multiple systems integrators and others can work with multiple providers to implement Tereon quickly. There is no reason to prevent Tereon from being implemented widely within the Task Force's proposed timescales.

Tereon's modular design means that the Task Force need not specify that all of the baseline use cases be implemented immediately. Tereon's design enables providers to implement a set of baseline functionality at the start of a project, and then add additional functions as the need for those functions arises.

Tereon does not require any third-party software and the issues around hardware and communications are very modest indeed. The requisite skills exist in most, if not all, competent systems integrators. Kalypton intends to help create an ecosystem that will consist of –

- one or more scheme operators who maintain the central facility directory system consisting of directory servers and, perhaps individual Tereon servers on behalf of individual payment service providers. The scheme operators will respond to the governance body;
- a multiplicity of payment service providers that may or may not be banks;
- service providers who may or may not be banks and operate Tereon servers on behalf of those payment service providers (just as the Bankers' Banks provide services to smaller banks);
- IT consultancies and systems integrators who provide implementation capabilities and support resources to the rest of the ecosystem; and

- one or more rules providers led by ECCHO.

Kalypton intends that there be choice at all levels of this ecosystem to all industry participants if practicable.

The technology can be delivered well within the anticipated timescales and will likely not be a critical path item. In Kalypton's judgment, the key issues will include –

- the process for assembling or building a critical mass of users and merchants to achieve the required scale and ubiquity;
- identifying the scheme operator or operators; and
- developing and implementing the scheme rules and the governance framework

2. Value Proposition and Competition

Overall, Kalypton believes that the economic case for a new real-time payment scheme built upon Tereon will be extremely strong for individual stakeholders and for the US economy as a whole and over time. There need be no trade-offs. Payments using Tereon will be faster and more secure and lower cost and easier to use than their current equivalents.

However, there are industry participants that do very well economically from the current situation. A thorough stakeholder analysis will identify directions from which negative reactions might be expected to emerge.

Kalypton fully expects a competitive reaction from legacy payment schemes to the introduction of a full function, end-to-end Tereon-based scheme. The task of fundamentally re-engineering these schemes is larger, costlier, and slower than the task of building and implementing Tereon with a clean sheet of paper. But there will be noisy promises.

The time dimension is also important. Typically, changes in payments have a substantial up-front cost and this acts both as a barrier to entry and, more importantly, a barrier to exit. The conversion to EMV payments is a current and hotly debated example. Tereon is designed to lower these barriers dramatically. It can use securely a simple Android tablet or smartphone as a merchant device, and a provider can service a scheme to support millions of transactions a second on commodity hardware. The upfront cost can be recovered very quickly, and the cost is low enough not to present a barrier to exit to any provider that wishes to halt offering Tereon-based services to its customers.

The cost of current processes is directly borne by merchants, including Government. It is important to note in this context that Tereon is a full transaction-processing engine, not just a payment platform. That means it can be used to distribute welfare and other government benefits cost effectively. These benefits can be spent at the market via Tereon without the stigma of handing over physical food stamps.

Kalypton looks forward to developing an implementation plan that addresses sectors of the market where the presence of existing legacy systems does not present a major impediment to early adoption, and to develop "staircase" plan that grows the scheme and its presence from that point on.

In parallel with the task of establishing a Tereon-based scheme, Kalypton intends to support an open framework for competition and innovation –

- by allowing payment service providers to develop their own services and develop or source their own apps from anywhere

- by providing interoperability with legacy schemes and other new schemes at the device level, at the server level and via provider core systems
- by supporting this intent via the commercial and governance models

Any provider that is willing to abide by the governance rules and the payments rules can offer a service using Tereon. Providers can differentiate themselves from each other by valued-added services, account services, fees, or any other criteria. Tereon does not dictate what a provider can offer; it only dictates that every provider must provide the baseline functions and must abide by the governance and payments rules.

Any third-party can create new value-added services, provided that they too agree to abide by the governance and payments rules.

Tereon also builds in mechanisms to prevent a provider from locking in a user, in order to promote genuine competition amongst providers and so provide users with meaningful choice. Any user can change providers by using the account switching function built in to Tereon. A user can switch at any time, without fear of losing any in-air payments. Tereon's account switching system is designed to enable a user to switch providers in minutes, and to capture and redirect all in-air payments. In-air payments are payments that a party might make to a user after the user has switched accounts or while her account is being transferred from one provider to another. Tereon's directory look-up service facilities this function, the exact details of which are currently subject to a patent application.

The account switching function also allows a regulator or other party to close a provider and transfer its users to another provider if the first provider materially breaches any governance or payment rules or other applicable regulations.

A user can also subscribe to more than one provider without issue. For example, a user may have an account with a bank that acts as one provider, and a non-bank account provider that provides a second service. A user can register separate devices with these providers, or register the same device with these providers. In this latter case, the user will simply choose which account to use in a particular transaction at the point that she decides to make a transaction.

3. Integration Effort

Tereon is designed specifically to require minimal integration effort. Tereon can interface to, or interoperate with, any existing payment format standard, including customized versions of ISO 20022, ISO 8583, and so forth, and it can adapt to any amended or superseding standards as required. Tereon is also very cost effective, both in time and in money, to adopt. Rather than require expensive dedicated lines or customized server hardware, Tereon is designed to use any IP enabled device, any device that can interact with such a device (such as magnetic or microprocessor cards), high-end server hardware, and the Internet. The protocols impose and implement strict security controls, so these are not the responsibility of users or providers. Tereon is designed to scale to millions of transactions a second.

To get started with Tereon –

- Merchants require a Tereon app to accept payments via Tereon. That app can run on any connected device or as an applet in an e-commerce website. This gives them a range of options. They can co-locate Tereon alongside legacy solutions on an existing merchant device e.g., a card terminal. They can have a second cheaper device e.g., an Android tablet. This device would not be subject to PCI-DSS or EMV accreditation costs. Alternatively, they can accept payment on-line and in store.

- Consumers can use a native application on any smart device, or simply use a magnetic stripe card to make payments. The device is simply a source of a unique reference ID. The device or card does not store any representation of value or data of value e.g., a PIN. This, together with Tereon's ability to support multiple currencies and manage currency conversion dynamically, raises the prospect that a loyalty card can be a one swipe credential to accrue or redeem loyalty points and make payment.

Individual providers need to –

- establish an enabling regulatory status

- form a relationship with the Treasury management function of a bank to hold all funds paid or collected, if they themselves are not a bank or authorized to hold accounts as an authorized non-bank account provider.

- decide whether they require Tereon as middleware or as a virtualized service. If middleware, they need to procure an appliance consisting of Tereon software plus entry level hardware

- procure the co-operation of their core system provider to integrate their core system with Tereon.

Kalypton has developed the solution itself using its intellectual property. It is currently applying for a number of patents that cover aspects of its technology and the methods by which Tereon achieves its performance targets. Kalypton is not aware of any third-party claims on its technology.

Kalypton only uses third-party components where those components' licenses allow Kalypton to use those components within its solution without hindrance or any liability to the users of its solution.

Where a provider wishes to incorporate third-party components into its implementation of the solution, for example to use an API that the provider has licensed from a third-party to connect to Tereon, then that provider will be responsible for all licensing issues and costs that arise.

PART C: SELF-ASSESSMENT AGAINST EFFECTIVENESS CRITERIA

1. Ubiquity

Self-assessed rating:

Effectiveness Criteria			Effectiveness Criteria Self-Assessment (Check One)				Reference
Criteria Name	**#**	**Consideration Name**	**VE**	**E**	**SE**	**NE**	**Proposal Page Number**
Ubiquity	U.1	Accessibility	X				15, 53, 59, 102, 104, 106
Ubiquity	U.2	Usability	X				15, 30, 36, 53, 59, 102
Ubiquity	U.3	Predictability	X				15, 30, 36, 53, 56, 59, 102, 104, 106
Ubiquity	U.4	Contextual data capability	X				15, 56, 59, 106
Ubiquity	U.5	Cross-border functionality	X				15, 36, 49, 59
Ubiquity	U.6	Applicability to multiple use cases	X				15, 30, 53, 59, 104, 106

Justification for U.1:

U.1.1 Tereon was designed from the ground up to facilitate payments to and from any account type, be that an account held by a bank, or by a non-bank account provider. Tereon does not distinguish between the two types of account so far as the user service is concerned. The only difference to the back-end or "rails" is where the non-bank account provider needs to hold funds in a control account in a bank or other depository institution, where Tereon manages all of the user accounting processes on a ledger. Funds will transfer in and out of the control account only when users at the non-banked account provider transact with users at other account providers.

The design enables banks or other depository institutions that hold the user accounts and the control accounts, and non-banks account providers that are authorized to hold accounts to ensure that all AML and KYC processes are followed strictly. Thus, banks, other depository institutions, and non-bank account providers (irrespective of whether they can hold funds or not) can operate the solution to provide all the baseline services to their users.

U.1.2 Each provider can connect to any other provider via the directory look-up service, where the initiating provider will find the recipient provider using the recipient's Tereon ID. This ensures that any user can reach any other user. The peer-to-peer bilateral authentication and negotiation between the two transaction providers ensures that a transferor is informed that the funds have reached the transferee, or in limited cases such as a remittance to a non-registered user will reach the transferee, once the transaction ends. Tereon makes no distinction here between banked and unbanked users unless required to do so by regulation.

U.1.3 Tereon was designed from the ground up to support both mono-and multi-currency payments. The transferor's provider is responsible for obtaining the quote to exchange and transfer the transferor's funds in one currency to the recipient in another currency, so long as the recipient, the recipient's currency, or provider, is not embargoed.

U.1.4 See answers to U.1.1, U.1.2, and U.1.3. By leveraging the Internet and high-end commodity hardware, by simplifying the settlement process, and by removing the time lags between initiation and settlement that affect existing systems, Tereon allows providers to offer services at costs far below those of existing or competing solutions. Tereon removes the risk associated with transferring to or from an unbanked customer. It also enables that unbanked customer to build her financial profile to the extent that she can chose at a later date to become a banked customer should she wish to do so.

U.1.5 Tereon is extremely easy to implement. It reduces dramatically the costs associated with existing solutions, and only requires IP enabled devices at the service level, and high-end commodity servers at the "rails" level. Tereon publishes a set of APIs to integrate to core systems within account providers, and at a level that the account providers can choose.

Tereon manages most of the security issues automatically, and so mitigates dramatically the costs of conforming to PCI-DSS, for example. Tereon not only provides a set of very efficient payments "rails"; it also provides a set of protocols that any provider can use to build new, value added services to the standard baseline services across multiple channels and for any number of use cases.

By providing real-time settlement and receipt, Tereon dramatically improves merchant cash-flow, and removes settlement risks for the providers. The low costs that result from the minimal, if any, settlement risk result in lower operating costs and thus higher margins for both merchants and account providers.

U.1.6 Tereon is designed so that multiple providers, or networks can provide the solution. Tereon enforces interoperability across these providers and networks by using a standardized messaging protocol and by way of the directory look-up service that allows one provider to transact with another provider. The look-up service enables the providers to trust each other as both must be authorized in order to operate the service and interconnect. An unauthorized provider quite simply cannot connect to an authorized provider. Thus a user on one provider or network can transfer funds to and receive funds from a user on another provider or network.

The fast clearing, settlement, and receipt that Tereon facilitates means that both transferors and recipients will know that their accounts have been debited or credited within a second of the transferor initiating a payment. The exceptions are for check clearing, and for remittances to an unregistered user where there will be a time delay between the moment the payer hands over the check or the transferor transfers funds, and the time that the recipient receives the funds. (see pages 47, 49, 55, and 87 for the reasons for the delay).

Justification for U.2:

U.2.1 Tereon supports virtually any payment channel or device, and virtually any use case. Page 23 lists the baseline use cases, though Kalypton can reduce this number if required to do so in order to allow third-parties to provide some of the services. The example use cases on page 59 illustrate some of the variety of services that Tereon supports.

U.2.2 Tereon normally only requires the user initiating a transaction to enter the other user's Tereon ID. Neither party to a transaction needs to know the other's account details, even for an international payment or transfer. Where the users have NFC-enabled devices, such as smart phones, a PoS card terminal, or a smart card, then the initiator does not need to know the other user's Tereon ID, as the devices will identify themselves to each other via NFC.

Where required, such as when a user remits funds to an unregistered user, Tereon will require the transferor to supply the recipient's name and address before the transferor can initiate the transfer. If a user remits funds to another user in a third country then Tereon will, if that transfer is to a registered user, automatically identify the recipient's relevant details to the transferor's provider – the recipient's provider will exchange those details with the transferor's provider as part of the contextual data exchange. If paying by a paper check, then a payer will necessarily expose some information about her bank, as that information is printed on the check.

U.2.3 Tereon is designed to be available on a 24×7×365 basis. Its design builds in n+2 redundancy by default. The dependency is that the account providers' systems operate on a 24×7×365 basis.

U.2.4 Tereon's flexibility allows providers to allow any user authentication credential and user authorization credential that satisfies the provider's risk models and which is suited to the user in question. These can range from biometric through to the standard PIN. Providers can develop applications for Tereon that can provide for varying degrees of complexity or simplicity, depending on the requirements of the users. The baseline services are designed to require minimal user interaction.

Justification for U.3:

U.3.1 Page 23 sets out the baseline transactions that each Tereon server, and thus each provider, can provide. Third-parties and providers can add additional valued-added services to their users without affecting the baseline functions. Consequently, a user with one provider will be able to carry out a baseline transaction with a user with any other provider.

U.3.2 The default position is that baseline features are consistent across all providers. If, for regulatory reasons in a particular jurisdiction the baseline service differs, or imposes fees on the transferor then Tereon will communicate these clearly to the transferor before the transferor initiates the transfer or payment.

Tereon operates with fiat money, as opposed to private tokens that present a contingent liability on an issuer or provider. Tereon is designed to comply with existing financial service regulation, rather than require special exemptions to operate, unlike mobile-money or token-based solutions.

Tereon supports UTF-8 and can thus present an interface and all communications and messages to its users in the language of their choice.

U.3.3 Tereon uses a standard communications and messaging protocol to deliver all baseline services. Third-parties and providers can add to the protocol to add new value-added services. However, the protocols will retain full compatibility with all baseline services.

U.3.4 Tereon is designed to be device and channel agnostic in order to ensure that any user can access any of the baseline services via any channel or device. In some cases, a user may use one device, such as a smart card to access those services via a second device, such as a merchant's terminal. The baseline functions are predefined to ensure that they are consistent across all providers, channels, and devices.

U.3.5 Tereon is designed to remove the settlement risks that occur due to the time lag that can occur between clearing, settlement, and receipt. It is designed to audit and account all transactions in real time and to ensure that a transferor or payer can guarantee that the funds are or have been received by the recipient. It is designed to protect all users' and providers' personal and financial data. As such, Tereon is designed to require only simple rules that describe the protections, rights, and liabilities of the payer, the payee, and the providers. The rules will be expressed in plain, simple language, in order to ensure that anyone can understand them, and so mirror the simplicity of using Tereon

U.3.6 Tereon can support any branding, language, and terms and conditions of service. It is designed to fit in with the cultural and legal frameworks of any culture or jurisdiction.

Justification for U.4:

U.4.1 Tereon has a built-in messaging protocol, which supports UTF-8 and allows it to pass contextual data, where the transaction requires that data, contemporaneously with the payments data. In addition to data that is required for transactions, merchants, providers, and other third-parties can use the same facility to offer value-added services, such as targeted offers to customers, invoices with tax information, reasons for discounts or refunds, and so on. Tereon can even provide a messaging service for users to add messages to transfers or remittances.

Tereon's multi-currency capability allows it to treat loyalty points as if they were simply another set of currencies. Tereon can account for these in the same way that it

accounts for any other currency, and thus merchants, providers, or other third-parties can build loyalty schemes on top of Tereon, without affecting the underlying protocols or their interoperability between servers and devices.

U.4.2 Tereon can provide data feeds to any number of third-party applications that can receive data inputs from external sources. It can translate its internal format to any format of character set required using schemas and other translation frameworks. In the same way, Tereon can accept data feeds from any external source, provided that it can implement a scheme to translate that data to its internal format. Tereon will also remove executable code from such data feeds before it ingests that data.

Tereon can thus integrate contextual data with interfacing businesses, personal finance systems, or banking information systems where required. It uses the same mechanism to interface to bank and other account providers' core systems to facilitate AML, fraud, and other monitoring requirements.

U.4.3 Tereon can adapt and add to its internal schemes to enable it to translate into internal format to any information standard as required (see the answer to U.4.2).

Justification for U.5:

U.5.1 Tereon is built to manage payments in any currency and to handle multi-currency payments. If a transferor or payer wishes to transfer or pay sums to a recipient who uses a currency that differs from the transferor's or payer's currency, then Tereon's default configuration is for the transferor's or payer's provider to request one or more quotes from its foreign exchange service to exchange the sum to the recipient's currency. If the provider does not have a service, then Tereon can request those quotes from a settlement bank that provides the cross-border settlement.

If Tereon provides the exchange facility internally, then it will use decimal floating point arithmetic, coupled with bankers' rounding, or any other rounding method mandated by applicable regulation, to ensure that the sums involved in any exchange are fixed at the point of exchange.

By using quotes, or decimal arithmetic with defined rounding, Tereon does not risk incurring exchange rate rounding errors that can build over time. If the cost for a user in the United States to pay a merchant in the United Kingdom is £69.90, and this comes to $102.56 including fees, then the payer will pay $102.56, and not $102.558,

or $102.561, and Tereon will use the figure of $102.56 for all its records and accounts.

U.5.2 Tereon can interconnect to other payments systems, provided that providers accept the settlement risks that these systems may impose. It can translate its internal communication to meet the requirements of other payment systems using the same mechanisms that it uses to translate its internal format to those of connected information management systems (see answer to U.4.2).

U.5.3 Tereon must, by default, inform the transferor or payer of the exchange rates, and any fees or costs that the user will incur in any transaction before that user initiates the transfer or payment (Tereon does this for any transaction that incurs fees for the transferor or payer).

U.5.4 Tereon automatically includes the ability to convert payments and transfers from one currency to another (see answer to U.5.1).

U.5.5 This does not apply as Tereon supports cross border functionality.

Justification for U.6:

Page 23 sets out Tereon's baseline services. Page 59 sets out some of these use cases, including the targeted use cases. Tereon provides the flexibility to support any use case that can be built using its internal business logic engine, any combination of supported devices, and any credentials accepted by a provider.

2. Efficiency

Self-assessed rating:

Effectiveness Criteria			Effectiveness Criteria Self-Assessment (Check One)				Reference
Criteria Name	**#**	**Consideration Name**	**VE**	**E**	**SE**	**NE**	**Proposal Page Number**
Efficiency	E.1	Enables competition	X				15, 30, 102, 104, 106
Efficiency	E.2	Capability to enable value-added services	X				15, 30, 102, 104
Efficiency	E.3	Implementation timeline	X				102
Efficiency	E.4	Payment format standards	X				15, 36, 45, 63, 66, 97, 104, 106
Efficiency	E.5	Comprehensiveness	X				15, 30, 36, 41, 45, 49, 53, 56, 59, 102, 104
Efficiency	E.6	Scalability and adaptability	X				15, 56, 87, 106
Efficiency	E.7	Exceptions and investigations process	X				15, 36, 41, 56, 59

Justification for E.1:

E.1.1 Any provider that is willing to abide by the governance rules and the payments rules can offer a service using Tereon. Providers can differentiate themselves from each other by valued-added services, account services, fees, or any other criteria. Tereon does not dictate what a provider can offer; it only dictates that every provider must provide the baseline functions and must abide by the governance and payments rules.

E.1.2 Any user can change providers by using the account switching function built in to Tereon. A user can switch at any time, without fear of losing any in-air payments. Tereon's account switching system is designed to enable a user to switch providers in

minutes, and to capture and redirect all in-air payments. In-air payments are payments that a party might make to a user after the user has switched accounts or while her account is being transferred from one provider to another. Tereon's directory look-up service facilities this function, the exact details of which are currently subject to a patent application.

The account switching function also allows a regulator or other party to close a provider and transfer its users to another provider if the first provider materially breaches any governance or payment rules or other applicable regulations.

A user can subscribe to more than one provider without issue. For example, a user may have an account with a bank that acts as one provider, and a non-bank account provider that provides a second service. A user can register separate devices with these providers, or register the same device with these providers. In this latter case, the user will simply choose which account to use in a particular transaction at the point that she decides to make a transaction.

E.1.3 Tereon's enrollment procedure will require providers to disclose their costs to users when those users enroll with the provider. If a provider amends its fees, then Tereon's internal messaging system will inform users of those changes. A user can, of course, switch provider if she does not agree to the changes (see answer to E.1.2).

E.1.4 Tereon is specifically designed to enable providers of any size to offer the baseline services. Tereon can thus be used by the smallest credit union to the largest bank. Size, or lack thereof, is not an impediment. Kalypton does not mandate any size of operation for an organization to be a provider.

Justification for E.2:

E.2.1 Kalypton will publish its protocols and standards to enable providers to integrate with Tereon and provide value-added services to any user.

E.2.2 Any provider, regardless of its size, can create and offer additional value-added services on Tereon. All it needs to do is conform to Tereon's protocol specifications, which Kalypton will make available (see answer to E.1.4).

E.2.3 Every provider must provide the baseline services to its users. Tereon will clearly disclose value-added services as optional extras. Tereon puts the user in full control of which additional services, if any, she wishes to use. The user can always remove any value-added service that she no longer wishes to use.

Justification for E.3:

E.3.1 The technical and operational challenges to implement Tereon are well known. Tereon can be implemented within the timescales established by the Task Force; Kalypton is already implementing Tereon within another territory and will have completed that work by Q4 of 2016. The key issues are not the technology, but the will of major banks and providers of banking core systems to co-operate with the Task Force to implement a genuine real-time payments solution.

Major retailers would be enthusiastic adopters, as Tereon will dramatically reduce their security and transaction costs, and so increase their margins significantly. It may prove necessary to create one or more specialist payments banks to compete with the existing banks to provide a service. Major retailers may wish to become non-bank service providers themselves. Until these questions are answered it would be premature to devise a detailed plan. However, Tereon is designed to be implemented technically in a matter of months; it is not the technology that defines implementation timescales.

Justification for E.4:

E.4.1 Tereon can interface to, or interoperate with, any existing payment format standard, including customized versions of ISO 20022, ISO 8583, and so forth, and it can adapt to any amended or superseding standards as required (see the answers to U.4). The issue here will be whether the providers will accept the settlement risks, and the increase in costs associated with those risks, that third-party payments services will pose. Tereon can protect the information that it has control of. It cannot vouch for any of that information once that information has passed beyond its control to third-party systems.

It is possible to encapsulate third-party systems within Tereon, as its technology and protocols allow it to overlay a security layer on those systems. Tereon will still secure the transport of the information, but it cannot secure the end-points servers of those

systems. If required, it could be a condition for a third-party to accept such an overlay if it wished to connect to Tereon.

E.4.2 Tereon is designed to facilitate full cross-border interoperability.

E.4.3 Tereon is very cost effective to adopt. Rather than require expensive dedicated lines or customized server hardware, Tereon is designed to use any IP enabled device, any device that can interact with such a device (such as magnetic or microprocessor cards), high-end server hardware, and the Internet. The protocols impose and implement strict security controls, so these are not the responsibility of users. Providers can use applications supplied by Kalypton for those devices, or they can create their own applications for those devices by adhering to the protocols that Kalypton will publish. Kalypton, quite simply, sees no reason whatsoever to tie providers to its own services or applications.

Tereon is also designed to provide a clear path to interface to existing core banking and account management facilities. The real issue is not one of cost, but one of the will on the part of the banks and core systems providers to wish to do so.

E.4.4 Tereon uses protocols that Kalypton will publish that will allow any third-party to develop and implement new services and use cases. It will also provide a clear path to upgrade and maintain its underlying technology. Tereon's internal design is highly modular with defined internal APIs. This allows Kalypton to update or change any of the internal components in order to improve performance, or add additional functionality, without compromising on the integrity or portability of the system.

E.4.5 Kalypton will publish the protocols necessary to allow any third-party to develop new applications or use cases. If required, then Kalypton would be willing to pass these to ISO or some other standards body to manage and publish.

Justification for E.5:

E.5.1 Tereon is designed to operate as a stand-alone system, with the ability to integrate into the existing financial services infrastructure where required. As the user cases and description make clear, Tereon manages all of the relevant aspects of the end-to-end payments process. Where Tereon needs to integrate to existing settlement systems and accounts, or to core banking and other account management systems, then it can do so.

E.5.2 Tereon's design supports all its features; its features and the need to support them dictated its design. One of its design goals was to support competition and innovation, and enable any provider, no matter how large or small, to offer the baseline services to its end users.

Justification for E.6:

E.6.1 Tereon is designed to support all of the baseline services set out on page 23, including the use cases outlined on page 59. The use cases set out in section 2 of part A, on pages 59 to 100, are simply some illustrated examples of some of those use cases.

E.6.2 Tereon is designed to process millions of transactions per second per provider. Its peer-to-peer design means that it is not restricted by the need to pass all transactions through a central hub, and the throughput of transactions between two peers will not limit the throughput of transactions between other peers.

Tereon is also designed to scale automatically. If a provider's system exceeds a predetermined load, then Tereon will scale itself horizontally to manage that load, scaling back as and when that load drops below a pre-determined threshold. Tereon's internal architecture is based on a number of functional levels, each of which is itself modular. Tereon will scale these levels independently, depending on the needs of the system at the time. If a provider determines that its choice of hardware cannot meet the throughput of its service, then Tereon will allow it to migrate the system to new hardware, moving the accounts and data to that new system in a way that does not compromise the integrity of that data of the service. The move will be completely transparent to users.

E.6.3 Tereon's design is flexible and extensible in order to adapt to any ongoing developments. It is as suited to emergency disaster relief as it is to operating as a full-scale payments infrastructure and service set. Its internal business logic can be adapted at any time to modify existing services, or to add new services, without needing to reissue or re-implement existing devices.

Justification for E.7:

E.7.1 Tereon is designed to minimize the risk of exceptions. It is designed to clear, settle and receipt transactions within a second, and records all transactions in a manner that guarantees ACID consistency. If a transaction fails for whatever reason, then Tereon rolls it back completely and users can begin again if they so wish.

Tereon still provides all of the messaging and audit capabilities to manage exceptions in the event that one does occur. Tereon records every transaction, regardless of whether that transaction fails, and provides the full access and management tools to enable users and administrators to manage and repair exceptions, in the unlikely event that they occur. The tools and methods used are flexible and can be configured to meet all applicable laws and regulations.

E.7.2 Tereon records a full audit trail of every transaction, internal or external, that occurs. It does so in real-time, which means that the system begins recording a transaction as soon as it starts, and completes the record as soon as it has completed. Each record is fully time and date stamped, and created in such a way that it evidences the transaction, even if an attacker was able to access the system and amend the record of the transaction itself (that attack would, itself, be recorded in any event). Tereon does not use the blockchain for this; that technology is too slow and cannot meet the legal and regulatory requirements for data protection, auditability, forensic investigation, or mandated repair and amendment of false or erroneous records.

Kalypton has developed a new audit technology that is currently subject to a patent application. Tereon’s audit system is fully integrated to its internal and external communications protocols and cannot be circumvented. It is designed to provide a completely contemporaneous audit of the system in real-time. That technology provides all of the real-time audit and validation support that Tereon requires, while protecting the privacy of data and the audit itself. It provides full forensic capabilities, and allows administrators to amend records when required to do so by a court of law, without compromising the audit or any of the preceding or subsequent records. The audit trail and the transaction are contemporaneous to each other. Whenever a stage of a transaction is recorded, the audit record is created as well. If a transaction fails and rolls back, then the audit captures that failure and roll back as well. Every user is made fully aware of the audit trail, as each user can access the information setting out her transactions and actions at any time.

The audit system can capture every action, except the key strokes for a user's password or PIN. If a provider enables geo-location functionality on end-devices, then it will capture that data as well, so that the audit will have a full list of the locations of the end-points in any transaction. Though the audit trail captures all of the contextual data surrounding every transaction, the administration system can anonymize that data until the provider or regulator launches a formal investigation. On presentation of a warrant from a competent court, the provider can provide authorities with a full transaction record for the suspect users or transactions. Only authorized administrators or investigators may access the audit trail in detail.

One of Tereon's design aims was to enable providers to combat money laundering and fraud. Its audit system is just one of the many systems that it provides to help providers combat financial crime. The data store for the audit trail is fully searchable via the administration portal. However, Tereon can also feed the data in real-time to the provider's report generating system or data analysis system if required.

E.7.3 Tereon can provide a full data feed into any exception investigation system (see the answers to U.4).

3. Safety and Security

Self-assessed rating:

Effectiveness Criteria			Effectiveness Criteria Self-Assessment (Check One)				Reference
Criteria Name	**#**	**Consideration Name**	**VE**	**E**	**SE**	**NE**	**Proposal Page Number**
Safety and Security	S.1	Risk management	X				15, 30, 36, 41, 45, 49, 56, 59
Safety and Security	S.2	Payer authorization	X				15, 36, 97
Safety and Security	S.3	Payment finality	X				41
Safety and Security	S.4	Settlement approach	X				49, 59
Safety and Security	S.5	Handling disputed payments	X				15, 53, 56
Safety and Security	S.6	Fraud information sharing	X				15, 30, 41, 45, 56
Safety and Security	S.7	Security controls	X				15, 30, 36, 41, 45, 49, 53, 56
Safety and Security	S.8	Resiliency	X				15, 45, 49, 56
Safety and Security	S.9	End-user data protection	X				15, 30, 36, 41, 49, 53, 56, 59
Safety and Security	S.10	End-user /provider authentication	X				15, 30, 59
Safety and Security	S.11	Participation requirements	X				15, 30, 41, 49, 53, 56, 59, 102, 104

Justification for S.1:

S.1.1 Tereon's internal business logic and structure allows it to support any use case. That flexibility also enables a provider to amend any service should a law or regulation suddenly require that amendment. For example, a regulation might come into force that for 30 days requires all payments above a low threshold, say $30 for the sake of argument, to be reported. The system can patch existing providers' solutions to meet that requirement as an upgrade, removing that upgrade once the regulation expires.

The flexibility can even be granular to a particular provider, or even a user. Irrespective of how the legal and regulatory landscape develops, Tereon is designed to accommodate those developments.

S.1.2 Tereon's settlement approach is to remove the time lag between receipt and settlement where possible. Tereon's default approach is to reorder the payments lifecycle stages so that receipt comes immediately after settlement. There are a few cases, such as remittances to unregistered users, and check presentation, where a lag may, unavoidably, come into the process. In these cases, the transferor's funds to cover the transaction are debited once the transaction is cleared, and hypothecated to the settlement accounts. The transferor can cancel the transaction up to the point at which the transfer or payment is settled, but, until that happens, the funds are hypothecated for settlement to ensure that there is no settlement liquidity risk to the recipient's provider.

Providers may also wish to continue to use their batched settlement mechanisms. In these cases, the settlement will occur after the recipient has been credited with funds. Here, however, Tereon will also hypothecate the settlement funds debited from the transferor's account and hold those for settlement. Again, this is to ensure that there is no settlement liquidity risk to the recipient's provider.

Tereon will prevent a user from making a transaction unless she has sufficient funds in her account, or an approved credit line, to cover a transaction. Thus, not only can a user not go overdrawn, but Tereon also ensures that the funds will always exist to settle a transaction. This is built in to Tereon's internal controls.

S.1.3 Tereon automates as much of a payments system as it can to minimize the risks of human error. It does not require after-the-event batch processing. Every transaction is individual and transacted and recorded in full. Its resilient design with built in redundancy and automatic scaling allow it to withstand infrastructure and usage shocks. Its account switching technology allows it to migrate users quickly from one server cluster to another should that prove necessary.

Tereon's internal controls prevent an administrator from acting as a user and so transacting payments as if she was a user. Though a user can ask an administrator to initiate a payment, the administrator will not be able to do so until the user reveals a random set of characters from a security password created specifically for this type of event. If a user forgets or loses her password or PIN, then an administrator cannot retrieve those credentials. The administrator can only set the system to generate new, random passwords or PINs that it sends to the user via a secure channel, unseen by the administrator. Every action by a user or administrator while accessing the system through its management or user portals is audited.

Tereon only allows access to the system via signed and encrypted communications. It can also enforce this policy to prevent administrators from accessing the system from unknown networks. For example, an administrator may be able to access the system in the provider's own secure network on site using a laptop or tablet. However, that same administrator, using that same laptop or tablet will not be able to access the system from any other network or location. The exact method for doing this is currently subject to a patent application.

S.1.4 Tereon uses multiple credentials before a user can authorize a payment. Without these credentials, no-one can authorize a payment from a particular user's account. Systems that rely on PINs are particularly notorious, as adults often provide their PINs to children to enable those children to make a purchase. With Tereon, there is no need to reveal a PIN to anyone. If a user wants to provide another user, such as her daughter, with the ability to make a payment using her mobile or card, then she can set up a PIN for her daughter with a time limit and a spending limit. Her daughter can then only use her own PIN within the allotted time period and up to the spending limit.

If a user makes a Tereon payment via a merchant's device, then the merchant never gets to hold any information that an attacker could use to initiate a payment. That merchant records only the date, time, and amount of a transaction, together with the transaction number and any details of the good or services for which she received payment. Tereon just does not allow the merchant to retain information that she would otherwise need to protect using PCI-DSS.

If a user makes a payment via an online portal, then the merchant will only ever see the Tereon ID used by the user. The user will complete the transfer on her interactive device, and not by entering payment information via the merchant's portal. If the user does not have an interactive device, then the user does not reveal her PIN to the merchant. Instead, she will supply a random set of characters from a password created for this purpose.

Tereon includes a mechanism to detect induced payments made under duress. The user need simply enter her PIN in reverse and this will alert Tereon to the fact that the payment is being made under duress. If using her smart phone, or any other smart device such as an ATM, then Tereon will take a picture (without alerting the user or her attacker) to try to capture the attacker's face. Tereon will alert the administrators who can report the user's location to law enforcement authorities immediately (Tereon can record geo-location data for each end-point in a transaction. Even if the user has disabled geo-location, Tereon can still use HLR lookups, and other data to determine the user's location. The provider may ultimately make it a condition of use to use the geo-location function in the event that the user raises an alarm). Tereon can, if configured to do so by the provider, "fail" the transaction at the first attempt in order to delay the transaction and so provide more time for the authorities to arrive at the user's location.

Tereon does not store authorization or authentication credentials on the device. Consequently, if an attacker were to obtain a device, then he would not be able to retrieve any information that would enable him to initiate a payment.

See also the answer to S.1.3.

S.1.5 Tereon removes the settlement risk that other providers may face. If providers fail to comply with the governance rules and payments rules, then the ultimate sanction is to remove all authorization from their servers. That provider will no longer be able to offer any services on Tereon, and will lose the financial benefits and revenue that come with those services. Tereon will alert the users who can transfer their accounts to another provider.

S.1.6 The governance and payments rules will set the review period within which providers will be audited to confirm that they comply with those rules. In addition, they will set the review period for Tereon's risk management framework. Tereon's risk management model, like its payments services, is defined by the internal rules, all of which can be configured via updates that Kalypton will push to every Tereon server that requires those updates. (These are separate to technical updates that will affect the code of the servers. Those will be updated by Kalypton on a regular basis as required.)

Justification for S.2:

S.2.1 This is how Tereon operates. Kalypton will not allow providers to interfere with this requirement. Any attempt to do so will revoke that provider's authorization.

S.2.2 Again, this is how Tereon operates with pre-authorization. The provider can dictate the maximum value that they will allow a user to pre-authorize for particular payment types. The user can always decline this option or reduce those limits further at any time. A user can also decide to pre-authorize payments after having declined the option. The user is always in ultimate control of which options she chooses to use and when.

S.2.3 See answer to S.2.2 and S.3.2. The user can revoke any payment within seconds. The moment the user submits her instruction to revoke a payment is the moment the payment is revoked.

Justification for S.3:

S.3.1 This is how Tereon operates. Kalypton will not allow a provider to amend this mode of operation. Any attempt to do so will revoke that provider's authorization.

Tereon ensures that users are fully informed at all times of the funds in their accounts, and of transaction and other fees that a transaction will incur. If the user has an approved credit line, then her account will also inform her at all times of the credit available to her. In order to protect the value of funds with the system, Tereon will not allow any provider to extend credit to their users unless that credit is regulated by an appropriate authority.

S.3.2 Tereon's architecture ensures that a payment becomes irrevocable when a recipient receives the funds, whether or not the settlement between providers has occurred (for example, if the providers operate a batched settlement system rather than Tereon's real-time settlement mechanism). In most payments, Tereon will clear, settle, and receipt the payment with a second of the transferor or payer initiating the payment or transfer.

The payment rules will clarify when a transferor of payer can cancel or revoke a pending transfer or payment. Any cancellation or revocation will take effect within a second of the user submitting her decision.

S.3.3 The payment rules will provide a mechanism to compensate payers or payees if a payment is disputed successfully. However, Tereon is architected to prevent disputes over payments. Both parties to a payment or transfer are kept informed at all stages, and except for deferred remittances or check presentations, most payments are completed within a second of the transferor or payer initiating that payment or transfer.

The rules appropriate to the system are similar to those for electronic checks. Tereon's payment model is best described as using electronic bills of exchange that are presented for immediate payment within a second of drawing that bill.

Justification for S.4:

S.4.1 This is how Tereon operates. Kalypton will not allow providers to interfere with this requirement. Any attempt to do so will revoke that provider's authorization.

Tereon automatically hypothecates funds required to settle transactions to the settlement accounts where those transactions are between two users with accounts at different providers. Together with the controls that ensure that a user cannot make a transaction unless she has sufficient funds in her account, or an approved credit facility, to cover a transaction, this ensures that account providers have the funds necessary to settle all transactions.

Where a provider settles on behalf of other providers, then Tereon will operate a similar mechanism, where the providers will hold accounts with the settlement institution. Where these accounts hold sufficient funds to cover the transactions, Tereon will simply settle the transactions between these accounts, and then between the settlement accounts between the provider and the settlement institution that the providers will hold. If an account falls below a preapproved amount, then Tereon will instruct the provider to transfer further funds to its settlement account with the settlement institution.

S.4.2 Tereon monitors transactions and their values in real-time, and so it monitors every provider's settlement exposure in real-time. Tereon hypothecates funds for settlement, regardless of whether providers use a central bank settlement system, a third-party

settlement system, or settle via a commercial bank. Tereon's preferred settlement method is for providers to hold settlement accounts with the central bank and so settle using central bank money. This removes the settlement liquidity risks for the providers for inter-provider settlement (see answer to S.4.3). In cases where Tereon must use a netting and batched settlement service, then it can monitor in real-time the settlement exposures of the various providers using that settlement system. If a provider's exposure exceeds certain parameters within the settlement period, then Tereon can instruct the provider's system to transfer further funds to the settlement institution to cover that exposure. See also the answer to S.8.3.

S.4.3 Tereon's preferred settlement method is for the providers to hold settlement accounts with the central bank and so settle using central bank money. Tereon can manage these accounts and so clear, settle, and deliver transactions within a second of the transferor or payer initiating the payment or transfer. This removes all settlement liquidity risks for the providers

Where providers settle using commercial bank money via a settlement institution, then Tereon includes mechanisms to minimize and strictly control any credit or liquidity risk that could otherwise arise (see answers to S.4.1 and S.4.2).

Justification for S.5:

S.5.1 Tereon can block user, accounts, devices, or providers, depending on the response required due to fraudulent activity. This happens immediately a block is executed.

Tereon feeds the audit of a transaction to the provider's core systems in real time. Though Tereon clears, settles, and receipts transfers or payments within a second of the transferor or payer initiating that transfer or payment, that is not the start of a transaction. As the descriptions on page 13 and the use cases on page 59 show, a transaction may start several seconds before the transferor or payer initiates the transfer or payment. For example, a merchant will enter the amount to pay into his PoS terminal before the user initiates the transaction with her card or phone. If a provider detects a fraudulent transaction taking place, perhaps because the merchant or user is suspected of wrongdoing, then the relevant provider's systems can block the transaction in mid flow, before it authorizes payment under stage 4 of the payments lifecycle, provided that it is lawful to do so in the circumstances.

Tereon's audit system tracks all transactions and actions, and provides the mechanism by which users, administrators, and investigators can investigate and resolve fraudulent or erroneous payments. Tereon itself includes measures to prevent fraudulent transactions in the first place. Providers must identify users, and must limit the value of transactions that a user can enter into depending on the level of knowledge that the provider has of that user.

Providers must identify each merchant that wishes to use Tereon, which will then identify that merchant to the user. If a merchant sells goods or services using Tereon, then both the merchant and the user will have a list of the goods or services purchased by that user, which either can access at any time, as can the administrators or investigators if they are required and authorized to do so.

Every party to a transaction is identified and recorded in the audit trail, whether banked, unbanked, or unregistered (an unregistered user must identify herself if she initiates a transfer, or she must be identified by the transferor if she is the recipient). Every part of a transaction, including relevant contextual information is recorded and searchable. Investigators can thus investigate any aspect of a suspect transaction if they are authorized to do so.

S.5.2 Tereon is designed to enable a provider to conform to consumer protection law. It provides mechanisms for refunds from merchants, data protection for all parties, reversal of erroneous payments, where those payments were erroneous, and minimizes the potential for disputed payments through its real-time clearing, settlement, and receipt process. See answer to L.3.

S.5.3 Tereon provides merchants with a mechanism to refund users via the original transaction number, even if those users have changed providers between making the payment and receiving the refund. Users can use Tereon's messaging system to request the prompt voluntary return of funds, which the recipient can act on. Tereon also provides the mechanism for an administrator at the recipient's provider to return funds to the originator, if required to do so under the payments rules, or if required to do so by law.

Tereon can implement any other mechanism mandated by law.

S.5.4 Tereon delineates administrator roles, responsibilities, and liabilities. No single administrator can have unfettered access to the system, and every administrator's action is captured by the audit system.

S.5.5 See answer to S.5.4.

Justification for S.6:

S.6.1 Tereon can tailor its information feeds to deliver the information that the recipient is entitled to see, and no more. It ensures that information shared between providers and other bodies for fraud management purposes is tailored to that purpose only. No personal data (information that identifies or can be used to identify an individual) will ever be disclosed in any information that is shared between providers for fraud management purposes. Investigators can access personal data only under warrant and under strict controls. The data that Tereon shares will enable providers and other bodies to analyze transaction patterns for fraud. If they detect any potential fraud, then they can take further steps to investigate, provided that they have or obtain the correct legal authorization to do so. Tereon treats fraud management data as a class of contextual data (see answer to U.4).

The only circumstance that one provider will send personal data to another is where it must provide information to identify the recipient of a cross-border remittance as part of the contextual information that accompanies the remittance. The information that the provider will include in the contextual information will be limited to that which meets the requirements for that transfer and no more.

S.6.2 See the answer to S.6.1. One of Tereon's design aims is to protect personal data and only permit access to such data under strictly controlled circumstances where the investigator or administrator has the lawful authority to access that data.

S.6.3 Tereon can provide its data feeds in real-time, contemporaneously to the transactions. The limitation is whether the providers' systems are capable of ingesting and processing the data in real-time. Tereon can also provide the data in batches, should that be necessary. If providers do not have the capability to ingest and process the data feeds in real-time, then Tereon can provide the data store and analytical data layers that providers can use to analyze the transactional data in real-time. It goes without saying that providers will be able to analyze the data ex-post. Tereon does not destroy its historical data unless required to do so by law.

S.6.4 This is part of Tereon's design (see answer to U.4).

S.6.5 This is part of the design of Tereon. Tereon strictly controls access to data based on ownership and roles. A user can access her personal data without any issue, which an administrator may only access that same data with the user's permission. Different administrators will have different levels of access, depending on their roles.

S.6.6 Tereon can feed data to a central authoritative trusted repository if that is required. This would simply be classed as a special purpose provider of a particular service, and

treated accordingly. Such a repository may be useful for aggregating fraud management data, or general data traffic analysis, but it should not detract from the providers' responsibility to manage fraud risks by and amongst themselves.

S.6.7 This is the purpose of Tereon's ability to aggregate and analyze aggregated data. Tereon can feed its transactional data into "big data" analytical systems to analyze all transactions for emerging patterns that will help detect fraud, money laundering, or other illegal activity.

Justification for S.7:

S.7.1 This is part of Tereon's design. No-one can access the system unless she is authorized to do so. Tereon includes a context-based security system (the details of which are subject to a patent application) that prevents access unless several credentials and parameters are met, irrespective of the level of access.

Tereon's security controls are layered, and all access is recorded by Tereon's audit system. Tereon is designed to prevent any access to any of its components unless that access is signed and encrypted.

All data is encrypted using known and tested algorithms and implementations. Encryption is AES256 at a minimum, and Tereon encrypts the data as well as all communication sessions with independent keys. By default, Tereon uses signed TLS 1.2 to identify the end-points and servers. This is related to its authentication mechanism. However, Tereon then uses a second protocol to generate the session keys that it will then use to encrypt the data and separately to encrypt the communications between servers, and between servers and end points. Tereon does not reuse keys for subsequent communications, and generates a new set of keys for each session. Tereon uses a cryptographically secure random number generator.

Tereon only uses algorithms in modes approved by NIST, and provides an algorithm or protocol roll-over facility; it has a mechanism to replace or update algorithms, protocols, and modes without affecting the integrity of the service.

Tereon is designed to provide full ACID consistency for all transactions in order to guarantee the integrity of the data. Tereon retains a minimum of three copies of each record in separate data stores to guard against systems failure, in addition to its n+2 systems redundancy.

S.7.2 This is part of Tereon's design. Tereon retains full control over the retention and disposal of data. The provider must set retention controls for the data that meet its legal and regulatory requirements and the requirements of the payments and governance rules. No administrator can dispose of any data unless permitted to do so by the policy or by law.

The Tereon audit system records every administrative action. It also provides a mechanism to recover records that were deleted when they should not have been deleted.

Tereon provides communications and network security from the end-point to the server, and from server to server. Its design assumption was that it could not rely on any existing security that a provider or entity may have in place, and so it encrypts all data and all communications before it sends data to or from any end-point or server. This security model does bring to light issues of security within bank core systems, but Tereon can use deprecated algorithms such as 3DES to communicate with these systems if necessary. All communications between Tereon servers, and between Tereon end-points and Tereon servers is encrypted with AES 256 as a minimum.

The participation rules will govern the physical and environmental security that a provider must meet in order to offer the service. The same rules will set out the rules governing operations security, monitoring, and incidence response. The participation rules will be a subset of the governance rules.

S.7.3 Tereon governance and payment rules will stipulate the managerial policies and oversight that providers must follow in order to offer a service to entities. The rules will integrate with existing risk management processes, though they will not be onerous, as Tereon's design dramatically reduces the risks that providers would otherwise face if they used other payments solutions. Tereon was designed to minimize the risks to entities and providers.

Tereon's governance and payments rules will, in particular, motivate all parties to maintain and improve the security of all transactions. There is no need for any user or provider to do things that, in other systems, would compromise security. Tereon is secure; it also provides convenience and supports almost any use case. For example, unlike existing systems, Tereon provides the facilities for a user to allow anyone in her family to use her device and account in strictly controlled circumstances without compromising the system's or her security and privacy (see answer to S.1.4). There is simply no need for a user to be tempted to compromise her security for the sake of convenience.

Kalypton will draw up the governance and payments rules with ECCHO once the baseline services that the solution will offer are agreed.

Justification for S.8:

S.8.1 The target availability and metrics will be defined by each provider based on its requirements and hardware capability. Tereon is designed to provide a robust, fully redundant, resilient, and massively concurrent payments service. Each implementation monitors its health and performance continuously. Where necessary, Tereon can scale itself automatically to manage any increase in workload.

S.8.2 This is part of Tereon's design (see answer to S.8.1).

S.8.3 This is part of Tereon's design. Tereon is massively concurrent, where each transaction is processed independently of any other. If one transaction fails, then Tereon will roll-back the transaction so that both end-users are in the same position that they were before the transaction was initiated.

In the same way, each Tereon server is independent of the others. Tereon is designed so that there can be no single point of failure in the system. Tereon servers operate as a mesh with the providers communicating on a peer-to-peer basis. Settlement institutions could theoretically provide a single point of failure, though here too they will have multiple Tereon systems offering n+2 redundancy. In the unlikely event that a settlement institution should suffer a systems failure or attack that takes it off line, then Tereon can do one of two things. It can immediately begin netting off one provider's transactions against another's until the settlement institutions systems come back up again, at which point it will reconcile the settlement records with those held at the institution and resume settling in central bank money. Tereon can also divert all settlement operations to a back-up settlement institution system or site.

S.8.4 This is a central part of Tereon's design. Tereon is designed to be available on a 24×7×365 basis, with full n+2 redundancy, resilience, and replication.

S.8.5 The governance and payments rules will stipulate the requirements and procedures for all providers to carry out regular contingency testing. Tereon is able to detect whether such tests have been carried out, and to flag to the provider and to any other authorized regulatory or control body when such tests are overdue. Tereon enforces contingency testing.

Justification for S.9:

S.9.1 This is part of Tereon’s design.

S.9.2 This is part of Tereon’s design.

S.9.3 This is part of Tereon’s design.

Justification for S.10:

S.10.1 The governance and payments rules will require providers to undertake KYC and anti-money laundering (AML) procedures to identify their account holders. The level of information required will be commensurate with the transaction limits that the provider wishes to allow the user to transact. Providers will be held responsible for ensuring that they have identified their users correctly.

Providers will also need to be identified and agree to undergo periodic auditing if they wish to be authorized to operate Tereon servers and offer services to their users.

At a system level, every end user device, and every server must be licensed (regardless of whether this is free or for a cost) and approved. Each device and server will have a unique signature and set of registration keys issued by Tereon, and these will be linked to the end users’ and servers’ accounts. These keys and signatures will remain valid so long as the end users and servers are authorized to operate Tereon, and will be revoked or suspended should the end users or servers lose that authorization in any way.

Only authorized devices and servers can only communicate with authorized servers.

S.10.2 The Tereon communication protocol is a bi-directional negation and communication. Both the transferor’s or payer’s server and the recipient’s server must identify themselves to each other and confirm that the other is authorized to operate, before they confirm the existence of their users to each other. The servers do not identify the users; they merely confirm that they manage the accounts linked to the Tereon IDs. The transaction will then continue until both sides confirm that the transaction has completed, and that the parties to the transaction have sent and received funds.

S.10.3 This is part of Tereon’s design.

S.10.4 This is part of Tereon's design. Tereon uses the same robust identification and management procedure, irrespective of the value of a transaction. A $1 transaction from someone who is poor is just as valuable to her as a $100, or even a $1000 transaction from someone who is wealthy. Tereon's internal efficiency means that it does not need to make value judgments over authentication models or procedures.

S.10.5 This is part of Tereon's design. Providers are free to re-authenticate their end users, or indeed require their end users to re-authenticate themselves with additional information should those end users wish to increase their transaction limits. This is a similar procedure to that which they will need to follow if a user wishes to remit funds to a recipient in another country, or if a user wishes to transfer funds over AML reporting levels.

S.10.6 This is part of Tereon's design (see answer to S.7.1)

Justification for S.11:

S.11.1 Tereon moves many of the data integrity, data security, and encryption protocols beyond the control of the provider. The provider has no choice but to follow those protocols to ensure that it maintains the integrity and security of all data, including a user's personal data, at all times.

Tereon provides "rails" and a set of protocols to offer services on those rails. Tereon does not allow providers to degrade or circumvent those protocols, which Kalypton designed to support a wide range of use cases while still protecting the end users' data and privacy, and providing full data and communications security. Tereon also supports three off-line modes (these are currently subject to a patent application and so Kalypton cannot discuss these modes at this stage).

The participation rules will set out the duties and obligations of the provider and its administrators that relate to operating and offering services to end users. The rules will also set out the sanctions that a provider and its administrators will face if it or they fail to comply with the rules and requirements that apply to them. These rules will be based on the provider's and its administrators' roles, and will be written in plain, unambiguous language.

End users will face a similar set of rules, albeit it far simpler, to remind them of what they may and may not use the system for, and the sanctions that they will face if they breach those rules.

S.11.2 The participation rules will ensure that the providers will have the operational, financial, and legal capacity to fulfill their obligations. Tereon will monitor their exposures and will flag any providers that appear to be putting their financial capability at risk.

S.11.3 Tereon monitors the providers on a real-time basis in order to protect the financial and operational viability of the system (see answers to S.11.2, S.11.1, S.8.5, S.8.1, and S.4.2).

4. Speed (Fast)

Self-assessed rating:

Effectiveness Criteria			Effectiveness Criteria Self-Assessment (Check One)				Reference
Criteria Name	**#**	**Consideration Name**	**VE**	**E**	**SE**	**NE**	**Proposal Page Number**
Speed (Fast)	F.1	Fast approval	X				41, 59
Speed (Fast)	F.2	Fast clearing	X				45, 59
Speed (Fast)	F.3	Fast availability of good funds to payee	X				49, 53, 59
Speed (Fast)	F.4	Fast settlement among depository institutions and regulated non-bank account providers	X				49, 53, 59
Speed (Fast)	F.5	Prompt visibility of payment status	X				45, 49, 53, 59

Justification for F.1:

This is one of Tereon's design criteria. Tereon is designed to approve or deny a transfer or payment in less than a second from the moment the transferor or payer initiates the transfer or payment.

Justification for F.2:

This is one of Tereon's design criteria. Tereon is designed to clear a transfer or payment in less than a second from the moment the transferor or payer initiates the transfer or payment.

Justification for F.3:

This is one of Tereon's design criteria. Tereon is designed to credit a recipient's account with funds in less than a second from the moment the transferor or payer initiates the transfer or payment.

Justification for F.4:

F.4.1 Tereon is designed to settle a transfer or payment in less than a second from the moment the transferor or payer initiates the transfer or payment. A design criterion was to eliminate as far as possible the settlement liquidity risks posed by other solutions. Tereon's insistence on only permitting a user to make a transaction is she has sufficient funds or approved credit to cover that transaction enables it to reduce or eliminate a credit or liquidity risks exposure that arise from any delay between settlement and receipt of funds.

If Tereon controls settlement, by managing the settlement accounts of the providers, then it can provide settlement services on a 24×7×365 basis. Tereon will, in any case, hypothecate all funds required for settlement in the provider's settlement accounts. Where final settlement occurs periodically, such as where the providers prefer to use existing settlement mechanisms, then Tereon can net transfers to other providers against transfers coming from those providers in order to maintain liquidity levels in each provider. It will be for the regulatory authorities to determine the liquidity levels that providers must maintain. Tereon will simply enforce those levels.

F.4.2 Tereon operates on UTC time internally for all of its actions. It displays both the UTC time and the local time for each transaction or action in its audit logs and in the records for each transaction. As Tereon manages the settlement accounts, including any netting procedures to manage liquidity levels, it is able to manage cross-border and cross-time zone settlement internally. Tereon will implement on a case-by-case basis any special procedures that it needs to implement to manage existing settlement mechanisms, if the providers prefer to use those rather that commercial bank or central bank settlement systems, where Tereon can manage the settlement accounts on a 24×7×365 basis.

F.4.3 Tereon can manage batched or periodic settlement systems if required as it automatically hypothecates funds to cover a transaction once that transaction is cleared for settlement.

Justification for F.5:

F.5.1 Tereon immediately reports the status of a payment to the payer's systems, and thus to the payer, once the payer's system has approved the payment for settlement. In reality, for most payments, the payment will be approved, cleared, settled, and delivered within a second of so of the transferor or payer initiating that transfer or payment. The status reporting function will only be noticeable in payments or transfers where receipt is deferred, such as a pre-autotomized payment to a utility, a remittance to an unregistered user, or a presented check, where there may be a delay between initiating the transfer or payment, and the recipient receiving the funds. In these cases, the transferor or payer will be able to see the status of the transfer or payment in real-time.

Tereon always notifies the transferor or payer when Tereon has debited her account, and when the recipient has received funds in her account, within a second of the event occurring.

F.5.2 Tereon immediately reports the status of a payment to the payee's systems, and thus to the payee, once the payee's system receives notice that the payment has been cleared for settlement by the payer's system. In reality, for most payments, the payment will be approved, cleared, settled, and delivered within a second of so of the transferor or payer initiating that transfer or payment. The status reporting function will only be noticeable in payments or transfers where receipt is deferred, such as a pre-autotomized payment to a utility, or a presented check, where there may be a delay between initiating the transfer or payment, and the recipient receiving the funds. In these cases, the recipient will be able to see the status of the transfer or payment in real-time.

An unregistered user, by default, will not have a device to see any status, but can always see the status of the transfer once she goes to a merchant device to collect some or all the funds.

Tereon always notifies the recipient when a pending transfer or payment to her has been approved and when she has received funds in her account, within a second of the event occurring.

5. Legal Framework

Self-assessed rating:

Effectiveness Criteria			Effectiveness Criteria Self-Assessment (Check One)				Reference
Criteria Name	**#**	**Consideration Name**	**VE**	**E**	**SE**	**NE**	**Proposal Page Number**
Legal Framework	L.1	Legal framework	X				15, 30, 102, 104
Legal Framework	L.2	Payment system rules	X				15, 30, 36, 41, 45, 49, 53, 56, 102, 104
Legal Framework	L.3	Consumer protections	X				15, 30, 36, 41, 49, 53, 56, 104
Legal Framework	L.4	Data privacy	X				15, 30, 36, 41, 49, 53, 56, 104
Legal Framework	L.5	Intellectual property	X				106

Justification for L.1:

L.1.1 The payments rules will supplement the existing payment law and regulations, as these apply to the solution. Tereon is designed to remove the uncertainties, time lags, and risks that occur with existing, legacy payments services, and those services that are built on the legacy infrastructure. Tereon ensures that funds are kept in banks or regulated non-bank account providers to ensure that those funds are fully regulated and safeguarded.

The governance and payments rules will be based on the ECCHO rules created for the Tereon faster payments solution, but simplified to reflect the operational capabilities and minimal risk of the solution.

Page 23 sets out the baseline functionality that Tereon can provide. The exact baseline that the proposed solution will provide may include all of the listed services, or a subset of those functions. Kalypton and ECCHO lead a process that involves the stakeholders to construct the governance and payments rules (the participation rules

are a subset of the governance rules) once the baseline functionality for the solution has been agreed.

ECCHO will identify and analyze the relevant laws and regulations that will form the basis of the legal framework for Faster Payments. During that analysis, any weaknesses will be identified, along with plans to address those gaps. In addition to ECCHO's staff expertise in rules and regulations, ECCHO utilizes counsel from a premier payment systems legal firm and seeks guidance from the Legal Subcommittee comprised of the best payments attorneys in the nation.

Faster Payments rules will be drafted in a collegial setting according to the ECCHO Rules methodology, to incorporate existing law and develop rules to bridge any gaps present in the existing legal environment. Stakeholders will have input into the decision-making process and a voice with the decision-making body/the Board.

It is important to clarify that service provider system rules and legal rules are different. The primary purpose of the legal rules for Faster Payments is to define roles, allocate responsibilities and liabilities, and provide for exception resolution, etc. for all of the parties to the payments transaction. The primary purpose of the service provider system rules is to define how the process works and who will do what and when. Legal rules are specific to each payment system (e.g., Faster Payments, check, ACH, wire) and are layered on top of existing laws, regulation, compliance, and case law to ensure full legal coverage for any payment situation.

L.1.2 Tereon does not need legal exemptions to operate, as it was designed to operate within the existing financial services and payments regulations. It does not create private, contingent debts. Instead, it simply instructs account providers to transfer funds from one account to another. The providers themselves will settle using central bank money or commercial bank money. There are no gaps in the legislative framework that prevent Tereon from operating.

Tereon provides the flexibility to alter any of the baseline services to accommodate legal development in the future, should those developments require changes to any of those services.

In this first step, ECCHO, in conjunction with its legal counsel and the Legal Subcommittee, will identify all relevant legal sources in order to understand and set the basis for the Faster Payments Rules. The following items will be researched and identified:

- Applicable existing law and compliance (e.g., Reg Z, Reg E, Reg GG, OFAC, AML, BSA, various federal and state laws, and potentially case law)

- Any unique conditions in which the same functions are subject to different laws depending upon who performs the functions—whether financial institutions, consumers, processors, corporates, etc.

- Gaps in laws that will need to be filled—this is where the Faster Payments rules come into play—to meet these gaps or to clarify liabilities

- All players, their roles and responsibilities—how the entities and payments will be legally bound

- Flow of faster payments from payer to payee that describes the various components of the legal framework and where/how each part of the process is governed by agreements, rules, law, compliance, warranties, indemnifications, etc.

L.1.3 Providers will be bound to each other and to end users by both agreement and by the applicable legislation and regulation.

End users will be bound to each other and to providers by both contract and by the applicable legislation and regulation.

L.1.4 See answer to L.1.2.

L.1.5 See answer to L.1.2. Providers that offer services to end users must conform to the existing legislation and regulation that govern those services.

Justification for L.2:

L.2.1 The payments rules will describe the rights and obligations of all end users and providers of the system. Those rules will be based on the operational features described in this document, and, in particular, Tereon's ability to provide genuine real-time clearing, settlement, and receipt of transfers and payments. ECCHO will work with Kalypton and the solutions governing organization to define those rules.

ECCHO is uniquely qualified to facilitate the development of Faster Payments rules because it recently developed the rules for another new payment system (image exchange) from the ground up. The check image exchange system is arguably the most complex payment system legally and operationally. ECCHO's experience includes evaluating the best strategy for electronification, creative design that enabled swift industry-wide transition, lobbying and testifying before Congress to change the law, and involving widely disparate stakeholders.

L.2.1.1 The rules will set out and take as their starting point the unique method by which Tereon identifies and authenticates all entities, payments, and messages connected to a transfer or payment.

L.2.1.2 The rules will set out the legal responsibilities and obligations of providers towards their end users, and towards other providers and end users.

L.2.1.3 The rules will address the obligations that arise from when a user initiates a transaction, and when a user initiates a transfer or payment where this occurs separately from initiating a transaction (see page 17).

L.2.1.4 The rules will set out when a user can cancel or revoke a transfer or payment.

L.2.1.5 Tereon uses a fail-stop protocol, in order to minimize the possibility of a failed transfers or payments from occurring. Tereon also uses a bi-directional handshake between providers to manage the transfer or payments process to guard against any delay in a payment once that payment has been authorized and approved. Nevertheless, the rules will set out the liabilities for delayed or failed payments.

L.2.1.6 The rules will set out when a transfer or payment becomes final and irrevocable, and the circumstances when that occurs before or after settlement, depending on the transfer or payment type and the settlement mechanism used by the providers.

L.2.1.7 The rules will set out the principles that govern the timings of real-time and deferred transfers or payments. These will cover the sending and the receipt of a transfer or payment.

L.2.1.8 The rules will set out the records of proof that the transferor or payer will have to evidence her transfer or payment, including where she is an unregistered user making a transfer to another user. The rules will also set out the records of proof of receipt that the recipient will receive, including where she is an unregistered user in receipt of a transfer.

L.2.1.9 Tereon's real-time payments functionality provides mechanisms to minimize the occurrence of a disputed payment. Nevertheless, the rules will establish effective and economic mechanisms for users and providers to resolve any disputed payments.

L.2.2 The process will be similar to that set out in G.1 and G.2.

L.2.3 The process will be similar to that set out in G.1 and G.2. The governance organization will be responsible for enforcing the rules in the first instance, though the ultimate appeal within the framework established by the payments rules may be to the independent oversight body or personality created under G.1.4.

L.2.4 The participation rules will establish the objective criteria that an organization must comply with in order to become a provider. Those same rules, together with the payment rules, will set out the requirements that providers will need to follow to obtain valid authorizations from payers, including what the authorizations credentials must conform to, and how providers may distribute those credentials to their end users.

L.2.5 Tereon is designed to minimize or avoid the errors that occur with existing, legacy systems. Nevertheless, the rules will set out an error resolution process that users will be able to follow to resolve any errors that might occur, including unauthorized payments, disputed in the payments process, failed payments, failed cancellations or revocations, and so forth.

Justification for L.3:

L.3.1 Tereon is designed to limit dramatically the possibilities for disputes over transfers or payments. Nevertheless, the solution requires a legal framework to provide protection and certainty for consumers (natural persons who make transactions for personal, family, or household purposes, and small and medium sized companies that use the solution for their day-to-day trading purposes) if it is to attract consumers as users.

The legal framework, which will bind all users, will define the legal and financial responsibilities of all users and providers for substantiated claims of unauthorized, fraudulent, or erroneous consumer transfers or payments. This framework will supplement and build on existing consumer protection legislation, and may exceed those protections that are otherwise required under applicable law.

The legal framework for consumer protections has the opportunity to go beyond any other non-cash payment system because consumer representatives will be involved at a different level than ever before. It will build on, and may exceed the protections provided by the Consumer Financial Protection Bureau.

L.3.2 The payments rules and procedures will support quick and effective error resolution mechanisms for consumer claims that arise from payments fraud, unauthorized

payments, or errors, and may exceed those protections that are otherwise required under applicable law.

L.3.3 The payments rules will allow providers and end users to establish additional consumer protection rules and processes for payments that exceed those that are otherwise available to users of the system.

Justification for L.4:

L.4.1 Tereon is designed to protect users' and providers' data. Nevertheless, the solution requires a legal data privacy framework to limit what data providers and other end users may collect, and what they may do with that data. The framework may be modelled on parts of the EU General Data Protection Regulations and may exceed those protections that are otherwise required under applicable law.

L.4.2 Tereon provides the mechanism to secure data within the payment systems and at the provider locations. The system does not store any personal data on the end user devices, and does not expose one user's data to another unless that data is required as contextual data within a transaction.

Tereon also secures all communications between end user devices and providers' servers, and between providers' servers to protect all information in transit, and Tereon never reveals the users' accounts or other financial information.

The legal framework will set out the obligations of providers, such as their obligations to secure physical access to their systems, manage and supervise administrator access, and the liabilities and sanctions for their failure to do so. The framework will also set out circumstances that providers will be mandated to work with law enforcement and other investigatory authorities once those third-parties obtain warrants or other lawful authority to access records held by the providers.

L.4.3 End users will need to provide basic information to enroll in the payments system, or to use the system to make or receive transfers as unregistered users. The legal framework will specify what information an end user must provide and the limited use to which that information will be put.

L.4.4 The solution will set out how end users can obtain visibility on the data that providers and others collect on them, the limits to any sharing of that data their ability to access that data, including their ability to require providers and other holders of that data to

correct any errors in that data. The end user's rights will mirror some of those set out in the EU General Data Protection Regulations (see answer to L.4.1).

Tereon puts users in complete control of their transfers or payments. It also puts users in complete control of their data. Consequently, a user can change her privacy settings with regards to what providers and other third-party services providers may do with her data. The user's choice will become effective the moment she submits her choice, and all providers and third-party service providers are obliged to comply with that user's choice immediately. The legal framework will establish the sanctions that the providers or third-party service providers will face if they fail to comply with the framework, including loss of authorization to operate the service or to offer value-added services.

L.4.5 The framework will set out the mechanism for providers to notify end users and the governance organization of any data breaches of their system. End users do not hold any private information by design. The framework will set out the liabilities and responsibilities among providers in the event of a data breach. See answer to L.4.1.

Justification for L.5:

L.5.1 Kalypton has developed the solution itself using its intellectual property. It is currently applying for a number of patents that cover aspects of its technology and the methods by which Tereon achieves its performance targets. Kalypton is not aware of any third-party claims on its technology.

Kalypton only uses third-party components where those components' licenses allow Kalypton to use those components within its solution without hindrance or any liability to the users of its solution.

Where a provider wishes to incorporate third-party components into its implementation of the solution, for example to use an API that the provider has licensed from a third-party to connect to Tereon, then that provider will be responsible for all licensing issues and costs that arise.

Kalypton and ECCHO will continue to conduct due diligence reviews of all applicable intellectual property rights on an on-going basis and define the approach to managing the property rights as may be necessary as a result of any findings from the due diligence process.

(ECCHO has direct experience with intellectual property rights based on the pervasive image technology lawsuit. ECCHO and its members assisted the industry by providing prior art and expert witness testimony. ECCHO was present at some of the trials and is equipped to do the research to prevent this situation from occurring again.)

6. Governance

Self-assessed rating:

Effectiveness Criteria			Effectiveness Criteria Self-Assessment (Check One)				Reference
Criteria Name	**#**	**Consideration Name**	**VE**	**E**	**SE**	**NE**	**Proposal Page Number**
Governance	G.1	Effective governance	X				102, 104
Governance	G.2	Inclusive governance	X				102, 104

Justification for G.1:

G.1.1 The Faster Payments Task Force has been an exemplary illustration of how to bring together representatives of all stakeholders to develop consensus around strategic objectives and coherent and comprehensive criteria for technology selection.

Over the coming months, the Task Force will evolve and form sub-groups to explore a number of issues including governance. Kalypton anticipates that the governance model that emerges will reflect the effective working relationships that have been established since the Task Force was formed and the unique requirements of the USA economy, industry and regulatory framework.

The solution's governance operating structure will be determined by the bylaws of the solution's rules organization. The bylaws of the organization will be developed by interested stakeholders in the creation of a new legal entity associated with the rules organization and would include considerations for proportional representation in the decision making process.

The solution's governance structure would include a Board of Directors comprised of representatives from a wide range of stakeholders, including merchant and consumer groups. The Board size would be anticipated to be sufficiently small to enable effective decision-making. The Board will set policy, objectives and approve the rules and will act in the interests of all stakeholders and pursue long-term objectives.

G.1.2 The governance arrangements, like the payment rules, will be made public.

G.1.3 The appeals process would be determined by and included in the Solution’s organizational bylaws. It is anticipated that the appeals process would begin with a request to the solution’s governing organization. The solution’s governing organization would refer the appeal to the appropriate substructure or advisory group for through vetting and consensus building followed by further vetting and consensus building through the operations committee followed by recommendations, as appropriate, to the Board of Directors.

G.1.4 The governance arrangements will provide for independent validation of the governing organization’s compliance with the solution’s governance and payments rules, and with applicable law. It will also provide for independent validation of the solution’s compliance with those rules, and that the rules achieve both the solution’s objectives and the greater public policy and public interest objectives.

The exact mechanism will be decided upon when the governance rules are created, but can range from an independent board through to an Ombudsman’s Office specifically created to carry out this oversight.

Justification for G.2:

G.2.1 The governance rules will mandate that the Board’s decisions, and those of the substructures and advisory groups, consider the public interest and the wider stakeholder interest when making rules and decisions.

G.2.2 The Board’s decisions will be based on input received from other substructures or advisory groups such as ad hoc or standing subcommittees. The responsibilities of the substructures would be assigned by the Board of Directors. The substructures would be composed of all interested parties as approved by the Board of Directors.

G.2.3 As issues and considerations become apparent that need solutions, those issues and considerations will be presented to the various substructures or advisory groups that will thoroughly review, vet and develop appropriate initial conclusions. Those conclusions will be presented to and further vetted by an operations committee. The size of the operations committee would be sufficiently large to allow participation of representatives from all stakeholder segments. The operations committee would work to achieve consensus recommendations to the Board of Directors. The chair of the operations committee would attend the Board of Directors meetings and present the recommendations of the operations committee to the Board. This process and

participation level would ensure transparency of process. No rules or portions of rules will be created behind closed doors.

G.2.4 See answer to G.2.3.

G.2.5 The bylaws of the solution's rules organization would include provisions for managing conflicts of interest, both actual and perceived.

APPENDIX A – ABOUT KALYPTON

Kalypton’s founder and CEO, Lars Davies, first experienced payments as the son of an international banker, living in India, the Middle East and Africa. He saw payments being processed in minutes, and point to point, via telex.

Whilst on the faculty of the Centre of Commercial Law Studies, Lars studied the first tranche of digital money, such as Flooz, Beanz and Digicash.

Lars formed Kalypton to operate at the cusp of Information Technology and the Law. Among other things, Kalypton consulted to Microsoft, Dell, and Ernst & Young. Kalypton developed Undeniable, a structured consulting process to help any organization review its many obligations in information management and use them to develop and implement, policies and technology to meet those disparate requirements.

In parallel with this, Standard Bank established a skunk works called Beyond Payments to develop and implement disruptive payment technologies that could be implemented in Africa while meeting the strict regulatory requirements of South Africa. They commissioned an external software house to do much of the work and the result was, and remains, implemented in at least three African countries.

The developer repatriated to the UK and sold the code and intellectual property to Kalypton in 2010. Kalypton retrospectively named this code base Tereon 1.0.

Kalypton demonstrated Tereon 3.0 in Chicago and Tereon 4.0 will be available for demonstration within the timescale of the QIAT evaluation process.

The first commercial deployment of Tereon will be for a consortium of banks in Guatemala and the initial deployment of Tereon for straight-through and real-time processing of check images. The consortium’s vision is that subsequent phases will create a “payments hub” reducing costs in established use cases, enabling innovation and facilitating financial inclusion. Kalypton is confident of a second deployment in Africa during the course of 2016.

Kalypton is majority owned by Lars, with the balance held by friends and colleagues. Its agenda is to achieve a robust financial position, secure long-term independence and then measure its success in terms of impact rather than profit maximization. Lars intends that a substantial block of Kalypton stock will be placed into a foundation.

APPENDIX B – ABOUT ECCHO

ECCHO is a not-for-profit clearinghouse that provides rules for private sector, interbank, image exchange that is vendor independent and solution agnostic. ECCHO Rules fully allocate liability among the various parties. The rules are flexible enough to allow ECCHO members to interact with their customers as they wish, as well as use technology to achieve their business objectives as appropriate while ensuring both the consistency and safety of check payments.

ECCHO chaired the Faster Payments Legal Work Group and participated in the Faster Payments Task Force. ECCHO has experience with developing rules from the inception of a payment system. Although check is not a new payment system, image exchange is—requiring rules to fill the gaps in existing law to cover electronic check payments and new technology (e.g., image, RDC, mRDC).

The check system has provided a unique learning opportunity for rules development because it is such a complex and open system. Many of the same issues will be addressed when developing rules for Faster Payments including: identifying gaps and melding new agreements with multiple existing laws, incorporating new technologies, managing multi-operator/many vendor environment, dealing with payment origination from consumers, businesses, government, and financial institutions.

ECCHO played a major role in developing and enhancing laws to validate that electronic check records carry the same legal weight as paper checks. It facilitated sixty organizations to create joint recommendations to Congress in order to pass the Check 21 Act. It also supported the industry in coordinating joint industry comment letters on proposed regulatory changes in Regulation CC, Regulation J, and others. ECCHO was instrumental in the inclusion of checks in the creation of the E-Sign Act and the Uniform Electronic Transactions Act.

ECCHO serves approximately 3,000 members as well as the industry at large. ECCHO's principals constantly monitor the payments landscape for opportunities for improvement. ECCHO stays abreast of the hot topics, court cases, and regulatory agencies' plans, taking action as necessary in its role as rules developer, educator and advocate. ECCHO excels at fostering a collegial environment that encourages membership input.

ECCHO is unique in the quality of facilitation it offers its members and Faster Payments. It brings in all the stakeholders—including competing organizations and large and small players, to discuss the issues and come to consensus—even when there are diverse viewpoints. While some associations and clearinghouses focus on a particular segment of the market, ECCHO is purposefully inclusive with representation from large and small banks, processors, credit unions, corporate credit unions, bankers' banks, payments associations, solutions providers, consultants, the Federal Reserve, The Clearing House, consumers, consumer groups, corporates, and other

industry players. The rules that go to the Board are developed from vast and diverse input. ECCHO facilitates the conversations that lead to the rules—rather than driving rules to a pre-determined conclusion.

Need for Rules

Faster Payments system rules serve the important role of reducing the uncertainty of dispute resolution among parties by establishing the legal rights and obligations of stakeholders in a consistent and uniform manner. These rules outline the legal responsibilities, in the form of warranties and indemnifications, and how exceptions are resolved. Payment system rules are vital because they address the ambiguities and gaps in the law and provide a uniform application regardless of any providers' specific solution. While there are existing laws that cover many aspects of payments, there is currently no law that covers all aspects of payments in an online real-time payment system. A common, uniform set of rules can best address this need.

Objective Development

Faster Payments rules development should be led by an independent and impartial party not associated with any specific service provider—one that is dedicated to finding the best solution for the industry and all versions of faster payments. Rules development should include fair representation to all participants through a transparent process. This is not an easy task as issues affect organizations and parties to the payment transaction differently. Only through facilitated conversation can disparate parties gain the understanding of other perspectives and find the best long term approach/solution—often one that was not previously conceived.

ECCHO Focus

ECCHO's not-for-profit status ensures that its focus is on the needs of the stakeholders. ECCHO is unique in its stakeholder-centric approach. While most organizations develop the system or product, then seek to acquire users, ECCHO begins with an understanding of the stakeholders' objectives and then develops the rules to best address those objectives. ECCHO believes this focus ultimately drives usage by creating a level playing field for large and small participants, within a transparent, inclusive setting—finding solutions that everyone can embrace. ECCHO, in conjunctions with broad industry participation, found ways around every obstacle in the ramp-up of the check image payment system—resulting in the fastest usage transition in payment system history.

ECCHO Methodology

ECCHO's Rules development methodology is preferred across the industry because it involves the active participation of stakeholders—listening to their issues and jointly creating a solution. ECCHOs explore issues regardless of who brings them to the table—implementing if there is

consensus about the value. ECCHO Rules enable an open environment suitable for all vendors and solutions.

The ECCHO Rules methodology is –

- Bottom-up – members bring us real-life problems and opportunities to discuss and resolve;
- Inclusive – involve widest group to pursue most equitable way forward; and
- Continuous – always improving and making additions to the rules and operational procedures including large banks, bankers' banks, credit unions, small banks, processors, corporate credit unions, Federal Reserve, The Clearing House, regional payments associations, consultants, solutions providers and will add consumer representation and corporates for Faster Payments.

Attorneys create an initial draft of the Rules followed by broad stakeholder discussion, review and modification. Once the initial set of rules has been implemented the next phase of continual maintenance and enhancement begins. The process begins with issues brought by members, ECCHO staff and other industry players and continues to discussions amongst the membership. Discussions begin in subcommittees or at an informal brainstorming roundtable session. Members discuss whether others are experiencing the same challenges and how best to address the issues. Subcommittee meetings are teleconferences for the widest participation, ad hoc, and exist on an as-needed basis. ECCHO currently hosts hundreds of participants on conference calls and facilitates input from all who wish to voice opinions and offer ideas. Rules drafts are created and refined in subcommittee. Subcommittees typically are formed for: rules development, exception processing management, legal & compliance issues, special projects, etc. Following discussion in subcommittee, rules language is reviewed by the Legal Subcommittee which is comprised of the most experienced payment system lawyers in the U.S. Ultimately, rules are finalized in the in-person operations committee meetings and sent to the Board for approval. The rules language recommended in the operations committee is the exact rule that proceeds to the Board for approval.

Faster Payments Education

With any new system, education is a vital component. ECCHO will provide Faster Payments education to the industry in conjunction with the Regional Payments Associations (RPAs). ECCHO has a strong, long-time partnership with the RPAs—speaking at their conferences and engaging them to provide training for the National Check Professional certification program. At the request of the industry, ECCHO and the RPAs can create a certification program for Faster Payments to ensure expertise is developed by users across the industry.

Faster Payments QIAT

Proposer: Kalypton Group Limited and the Electronic Check Clearing House Organization (referred to in this document as Kalypton and ECCHO)

APPENDIX A: QUESTIONS FOR PROPOSER

Ubiquity

U.1 Accessibility

Additional information

The proposal mentions blockchain-like capabilities without being able to provide details as those abilities are currently the subject of a major patent application.

The patents have now been filed, and Kalypton is now able to reveal more details of Tereon's capabilities.

Tereon does not provide a distributed ledger. It provides distributed authentication of private ledgers. This delivers the "internet of trust" heralded by the IMF without the concomitant shortcomings of a distributed ledger. (Of course Tereon can support public ledgers if that is a requirement.)

As the Bank of England has identified in its proof-of-concept trials of blockchain-based technologies, distributed ledgers present major impediments to adoption as the basis of the functioning payments system. These are issues to do with a distributed ledger's scalability, security, privacy, interoperability, and sustainability. To quote from the bank's report:

"Our view is that it is important to gain further experience in this area. In particular, we would like to explore the following areas:

- Scalability - we would need assurance that a system could be scaled in such a way that it operates with total data integrity, and reliably at the high speeds and volumes required by central bank infrastructure;
- Security – we will need certainty that the privacy of the data in distributed ledgers cannot be compromised by cyberattack, now and in the future;
- Privacy - current protocols require a trade-off between privacy and resilience – for DLT to be used in any central bank application, a high standard of both would be required;
- Interoperability - we would like to understand how existing data standards and infrastructure might interact with distributed ledgers; and
- Sustainability – DLT systems typically use more energy and require more data storage than traditional ledgers for equivalent transaction flows. An important consideration therefore is how these can be minimized as systems increase in scale."

Tereon is designed from the outset to address these issues.

Scalability

It is designed to scale both vertically (adding resources to existing servers) and horizontally (adding additional servers to a cluster) while preserving its ability to provide a high throughput of ACID consistent transactions. Tereon currently processes in excess of 1,000,000 ACID consistent transactions per server on mid-range carrier-grade server hardware. It can do this because its design mitigates the effect and likelihood of partitioning (the exact method is currently the subject of a patent application). Tereon's design means that its transaction throughput is simply dictated by the vertical and horizontal hardware resources available to it. This approach means that Tereon can deliver game changing throughput within the constraints of the CAP theorem (which are sometimes misinterpreted).

Tereon also scales its services, and does so in two ways. Tereon uses APIs to connect to services and systems. In doing so, it can connect to any number of third-party systems and services via these APIs, and it can separate the services to individual servers or clusters of servers if required to do so. Tereon's directory service system allows services to discover and authenticate themselves to other services or systems on an ad hoc basis. Tereon's license and directory services ensure that only authorized services can interconnect. Tereon can also scale its services through its extensible, modular architecture.

Tereon implements each component as a self-contained module, and each module can provide one or more services to other modules by communicating via a set of internal APIs. This has several benefits. It means that any module can be replaced or upgraded at any time without detrimentally affecting Tereon's operations. It means that new modules can be added at any time to add functionality to Tereon. Examples could be to add new interfaces to third-party solutions or systems, or to add new protocols that update or supersede existing protocols. The modular design also means that Tereon can segment services to separate servers or clusters of servers, as mentioned above.

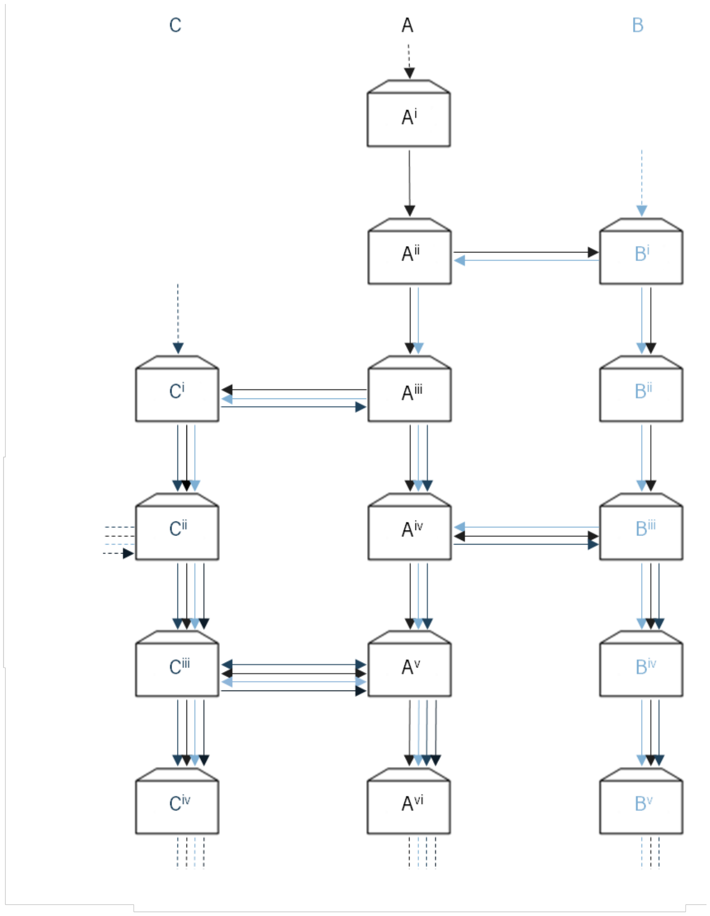
Security

Tereon's security model is not just about preserving the confidentiality of data and transactions; its model ensures that data is secured, authenticated, and verifiable without compromising any user's privacy.

Tereon preserves the confidentiality and privacy of all transactions by using protocols that are designed to authenticate every device and systems, and to prevent man-in-the middle attacks. Its security model means that only authenticated and authorized devices and systems can interact with the system; providers and operators authenticate the devices that their users register with the system. Tereon's modular design means that Tereon can upgrade security protocols without affecting the system's security.

Tereon secures access to the system by ensuring that all access is based on the roles of the party or system accessing the data, the device or system being used to access the data, and the network over which that device or system is requesting access to the data. Tereon audits and monitors all access in real-time, and ensures than no one role can access all of the data on any system.

Tereon's audit and monitoring system audits every action in real time. Its use of zero-knowledge proofs ensures that each transaction or action is contemporaneous with its audit. It constructs a series of dendritic authentication chains that enables any party or system to authenticate any transaction that occurs in its chain. This forms a distributed authentication chain, as opposed to a distributed ledger, and achieves the distributed authentication promised by the blockchain without needing to distribute the underlying transactional data. It is this need to distribute the underlying transactional data in blockchain that leads to compromises of privacy and confidentiality, and its incompatibility with financial services regulations. In Tereon, all transactional data remains private to the parties to the transaction, and to authorized aggregators of that data, such as fraud monitors, regulators, and the like.



The diagram opposite illustrates a simple dendritic nature of the authentication chain that involves three separate systems, A, B, and C. At A^{v}, A can authenticate all its transactions, all of B's transactions up to A^{iv}, and all of C's transactions us to C^{iii}, as can C at C^{iii}.

Tereon records all transactions in real-time in order to preserve causality (Tereon does not rely on date and time stamps for this, as these cannot be relied upon to preserve causality, an issue that is often overlooked. Instead, Tereon uses monotonic counters to preserve causality, with time and date stamps to show the time of each stage in a transaction within the error margins of the synchronized clock system).

The use of the zero-knowledge proofs, and in particular the manner in which Tereon uses those proofs, enables the records to exist separately from the independent audit chain and yet be authenticated and verified by that chain. The structure of the authentication chain means that, unlike the distributed ledger or blockchain, parties can revoke, reverse, or amend transactional records if required, without affecting the audit or the authentication chain. Each revocation, reversal, or amendment is itself audited and recorded and refers to the action in the authentication chain. (The exact method used to achieve this is subject to a patent application, as is the method by which Tereon creates the authentication chain.)

Privacy

Tereon does not expose any account details for a user to anyone other than the user's bank or payment service operator. This reduces dramatically the susceptibility of users to criminals. They simply do not hold any data that is of any use. Only a user's provider can identify to a third-party, such as an investigator, the parties to a transaction if legally authorized and required to do so.

Interoperability

Tereon provides a number of APIs to enable third parties to develop their own solutions to operate across Tereon (see prior discussion and answer to question E.2 below).

Sustainability

Tereon creates its authentication chain in the course of creating the transaction and with minimal computing overhead. There is no need for iterative proof of work exercises involving billions of billions of hash calculations at miners based next to hydroelectric dams (as with blockchain).

Tereon is designed to operate on standard carrier-grade servers (these provide additional hardware reliability), as set out above and in the answer to question E.6 below. This provides a cost-effective platform on which to operate Tereon.

Questions and answers

U.1.2: Please describe the process for a non-registered user to receive a payment. How will the Solution confirm payee identity? What entity is accountable for payee authentication?

Use-case 10, on page 93 of the original proposal document sets out the steps required for a registered user to transfer funds to an unregistered or non-registered user and for the unregistered user to receive that payment. Tereon can also support a transfer from an unregistered user to an unregistered user, though Kalypton felt that adding this and the remaining 31 use-cases would overload the document and exceed its recommended length.

To precis the steps set out in the use-case, when a user selects the option to transfer funds to an unregistered user, the transferor must enter the recipient’s name and address in order to identify the recipient. This can include the recipient’s mobile telephone number and email address, if the recipient has either of those. This identifies the recipient to Tereon (step T3). If the transferor has transferred to the unregistered recipient before, then the Tereon system will bring up the recipient’s details for the Transferor to confirm or amend (the system stores a record of each unregistered recipient’s details with the transferor’s account).

Once the transferor has identified the recipient, entered the amount to transfer, and entered his or her PIN, the Tereon system will provide the transferor with two credentials. The first is the transaction number (which Tereon can also email to the recipient, if the recipient has an email address, or send by SMS text to the recipient’s mobile number, if the recipient has a mobile phone (step T5). If the recipient has neither a mobile nor an email address, then the transferor has to send the transaction number to the recipient by another way. The second credential is the collection PIN, which the transferor must provide the recipient (Tereon does not transmit this number for security reasons).

In the above steps, the transferor has identified the recipient and Tereon has generated the two credentials that the recipient can use to identify him or herself and to authenticate the collection.

In order to identify him or herself, the recipient must go to a merchant or another party who provides a Tereon-based withdrawal service, and present that merchant with the transaction number to enter (step R1) (if a service provider wishes to do so then it could allow a recipient to use a bank ATM connected to Tereon for exactly the same function, whereby the recipient can enter the transaction number and then the collection PIN at the ATM in order to receive the funds transferred. The amounts withdrawn in this way would be limited to the sums that the ATM can dispense. A recipient would most likely use an ATM for a partial collection (step R3), and collect the remaining sums another day at a merchant or at a bank clerk’s desk).

If the recipient goes to a merchant, and hands the transaction number to the merchant to enter, then the merchant’s device can display the information entered by the transferor, and the merchant can ask the recipient to provide additional ID to verify those details (the step to transmit the recipient’s details, which is step S5 in the use-case, would simply be requested after step D2 if the merchant’s provider requires the merchant to ask the recipient for additional ID). Once the merchant is satisfied that the recipient is who he or she says, then the recipient enters the collection PIN (step S3, R2). Tereon now uses that PIN to authenticate the collection. Tereon confirms the recipient’s credentials. Because those credentials are linked to the recipient’s identity, Tereon confirms the credentials against the identity provided by the transferor.

At all times, it is the transferor who is ultimately accountable for providing the recipient’s ID and to communicate the transaction number and collection PIN to that recipient. Tereon may send the transaction number to the recipient by SMS or by email, but it is the transferor’s responsibility to provide the correct details, and those actions are recorded against the transferor’s account. It is therefore the transferor who is ultimately accountable for the identification of, and the authentication of, the recipient. In this way, Tereon conforms to international best practice in enforcing AML regulations and controls.

As in the descriptions of all Tereon use cases, these process flows should be taken as templates to be adjusted to suit factors like legislation and availability of national identity documents. It is trivial, and part of a Tereon deployment process, to agree modifications and elimination of options to create services that are simple and precisely tailored to the environment.

U.1.4: How will the Solution ensure that there is a reasonable network of service Providers (merchants) to support the withdrawal of funds by unregistered users and/or the unbanked who don’t wish to create a Tereon account?

Any merchant or agent who provides withdrawal services can provide a service that enables an unregistered user to receive funds. Tereon does not require an unregistered user to open an account in order to withdraw funds, as once an unregistered user creates an account they become, by definition, a registered user. If an unregistered user makes a partial withdrawal (see step R3), then Tereon will retain the remaining funds against the same transaction number (with the option to retain the original collection PIN or issue a new collection PIN), but that is not the same as opening an account for the unregistered user. All that Tereon is doing is retaining the remaining funds in the transferor’s system’s control account until the recipient has withdrawn all of the funds.

The same network of providers who will provide services to registered users can provide those same services to unregistered users.

The qualifications required to become a merchant supporting withdrawal of funds are a) a smart phone and b) a cash till. The business case for performing the role will be a transaction fee, increased footfall to the premises and the opportunity to use the same infrastructure to accept merchant payments with low fees, reducing cash and the attendant security issues. The recipient can also go to an ATM that is connected to Tereon to access the funds.

U.2 Usability

No questions

U.3 Predictability

Additional information

The original proposal did not define system rules or a dispute management process as Kalypton does not yet know what form the system will take, what the components will be, or the services offered across the system. Kalypton understood that the original intention was to deliver a final proposal that brought together aspects of various individual proposals. As such, the original proposal for Tereon could not impose a framework as that would be suited to Tereon, and not necessarily to the other components or services that the final proposal would comprise. The proposal therefore set out aspirations or suggestions that should be taken into account when drawing up the system rules and dispute resolution framework. Kalypton now understands that, with hindsight, this was a mistake.

The legal framework for the system rules and dispute resolution mechanisms for Tereon will be based on the existing ECCHO Operating Rules, but with the necessary amendments to provide for the operational nature of Tereon, the base-line services that it will support, and its settlement processes and the finality of those processes.

The system rules and the dispute resolution mechanism will borrow heavily from the rules drafted by ECCHO in order to ensure that the rules can benefit from the affordance provided by a well-understood and well-regarded set of rules governing electronic check payments. The structure of the system rules will also benefit from being based on the system rules and dispute mechanisms that will part of the design for the planned implementation in Central America (see question E.3 below).

The system rules will mandate that all providers must describe and set out the base-line services, their functions, operation, rights, obligations, and costs, in clear language (English, Spanish, etc.). The system rules will, with ECCHO's assistance, ensure that the rules comply with existing consumer protection law and commercial law. As the original proposal states, Tereon is designed to operate within existing rules and regulations and so does not need or seek special regulatory treatment. It is designed to comply with the law, and to ensure that its users benefit from all rights conferred on them by law. The system rules will be written to make this crystal clear, and providers may not exclude such protection or rights from their users. If the providers seek to do so, then they will lose the right to offer Tereon-based services.

Questions and answers

U.3.6: Is "Tereon" the Solution's branded name?

Tereon is the name of Kalypton's transaction processing software platform. Tereon does not need to be the user-facing brand for a service or scheme built on Tereon, although Kalypton would appreciate an "Intel Inside" style secondary branding for industry insiders. Kalypton appreciates that the new service needs to resonate in the US market and Kalypton puts forward for consideration "Franklin" because it is the face on the $100 bill and because of Mr. Franklin's notable contributions to both London life and the United States of America. However, Kalypton suspects that this is just one option that the FPTF might wish to consider. Of course, the FPTF may wish to retain the name of "Tereon" as that word itself is derived from the Greek verb that is the root of the word "treasure" (page 6 of the proposal).

U.4 Contextual data capability

Additional information

Although ISO 20022 is a standard, it is still very much a work in progress as parties work to add message types to that standard. This does not detract from its attractiveness:

> “From an industry perspective, this is a meaningful collaborative initiative that can benefit all market infrastructures and their members,” says Gina Russo, Federal Reserve Bank of New York. “By encouraging a standardized global approach to ISO 20022 implementation for high value payments systems, the industry as a whole can be in a position to reduce costs, ensure efficient implementation, and realize the true benefits of using a common global standard.”

Tereon will implement ISO 20022, and it will do so in a way that does not limit or constrain Tereon’s functionality. Tereon can capture a varied array of information that exceeds that reflected within the ISO 20022 standard. For example, Tereon can capture the geolocation of a user when that user makes a payment. Though Tereon captures this data, the ISO 20022 contains no defined field in the ISO 20022 CustomerCreditTransferInitiationV07 message schema for that data. Tereon can also, for example, capture the clock offset and the confidence interval for each device or system’s clock. Again, though Tereon records this data, the ISO 20022 message schema again does not have defined fields for that data.

Tereon’s design is to retain all of the contextual data that it records around a transaction, even if the end schema or message format that it delivers that data in cannot represent that data. Standards, such as ISO 20022 that are extensible are not too problematic. Tereon can make use of supplementary data fields, or Kalypton can work with the FPTF to define and submit additions to the existing schemas to cover the data types that Tereon captures and that are not yet represented by the standard. However, there are some payment format standards, such as ISO 8583 where this approach can cause issues. These are usually fixed formats that cannot be extended without rendering them incompatible with the systems that use them. In these cases, where the provider’s system can only use a date format that is fixed, or where extensible standards do not yet cover the data types that Tereon collects, then Tereon will provide what information it can in the standard format, and retain all of the information that it has recorded for access by the provider via another system, such as a Big Data analytical system.

Tereon does not use fixed data formats to transmit data between its devices and servers, or between the servers themselves. Transmitting data in fixed data formats presents several security risks (see Anderson. *Security Engineering* 2^{ed}. John Wiley & Sons, 2008). The format is known and so the data structure in any encrypted message is known. Tereon transmits its data, including any contextual data, in an obfuscated, serialized, and encrypted form. Tereon translates data from a sender system’s data format into its own internal data format, obfuscates, serializes and encrypts that data, and then transmits that data to the recipient system Tereon server. That Tereon server then decrypts, de-serializes, and de-obfuscates the data, and then translates that data into the recipient’s data format, regardless of whether that format is ISO 20022 or some other format, proprietary to the recipient or otherwise.

Questions and answers

U.4.2: How will the solution ensure that contextual data is accurately translated from/to ISO20022?

Tereon captures data that exceeds that defined by ISO 20022. For example, in the case of a registered Tereon user transferring funds to an unregistered (non-registered) user, Tereon not only captures the data required by AML regulations, such as the transferor's identity and details, and amount and currency of the transfer, the reasons for the transfer (if required) and the recipient's details. It also captures the date and time of the transfer and the confidence interval of that date and time, and for regulatory reasons the geolocation of the transferor when he or she initiated that transfer.

The ISO 20022 message schema defines fields for most, but not all, of that data. For example, the ISO 20022 CustomerCreditTransferInitiationV07 message schema defines fields for structured remittance information as:

```
</xs:complexType>
<xs:complexType name="StructuredRemittanceInformation13">
<xs:sequence>
<xs:element maxOccurs="unbounded" minOccurs="0" name="RfrdDocInf"
type="ReferredDocumentInformation7"/>
<xs:element maxOccurs="1" minOccurs="0" name="RfrdDocAmt"
type="RemittanceAmount2"/>
<xs:element maxOccurs="1" minOccurs="0" name="CdtrRefInf"
type="CreditorReferenceInformation2"/>
<xs:element maxOccurs="1" minOccurs="0" name="Invcr"
type="PartyIdentification43"/>
<xs:element maxOccurs="1" minOccurs="0" name="Invcee"
type="PartyIdentification43"/>
<xs:element maxOccurs="1" minOccurs="0" name="TaxRmt" type="TaxInformation4"/>
<xs:element maxOccurs="1" minOccurs="0" name="GrnshmtRmt" type="Garnishment1"/>
<xs:element maxOccurs="3" minOccurs="0" name="AddtlRmtInf" type="Max140Text"/>
</xs:sequence>
</xs:complexType>
```

The schema goes further to identify further fields within the above definition, such as PartyIdentification43, which identifies the parties:

```
<xs:complexType name="PartyIdentification43">
<xs:sequence>
<xs:element maxOccurs="1" minOccurs="0" name="Nm" type="Max140Text"/>
<xs:element maxOccurs="1" minOccurs="0" name="PstlAdr" type="PostalAddress6"/>
<xs:element maxOccurs="1" minOccurs="0" name="Id" type="Party11Choice"/>
<xs:element maxOccurs="1" minOccurs="0" name="CtryOfRes" type="CountryCode"/>
<xs:element maxOccurs="1" minOccurs="0" name="CtctDtls" type="ContactDetails2"/>
</xs:sequence>
</xs:complexType>
```

and PostalAddress6, which as its name suggests, sets out the address fields for both parties:

```
<xs:complexType name="PostalAddress6">
<xs:sequence>
<xs:element maxOccurs="1" minOccurs="0" name="AdrTp" type="AddressType2Code"/>
<xs:element maxOccurs="1" minOccurs="0" name="Dept" type="Max70Text"/>
<xs:element maxOccurs="1" minOccurs="0" name="SubDept" type="Max70Text"/>
<xs:element maxOccurs="1" minOccurs="0" name="StrtNm" type="Max70Text"/>
```

```
<xs:element maxOccurs="1" minOccurs="0" name="BldgNb" type="Max16Text"/>
<xs:element maxOccurs="1" minOccurs="0" name="PstCd" type="Max16Text"/>
<xs:element maxOccurs="1" minOccurs="0" name="TwnNm" type="Max35Text"/>
<xs:element maxOccurs="1" minOccurs="0" name="CtrySubDvsn" type="Max35Text"/>
<xs:element maxOccurs="1" minOccurs="0" name="Ctry" type="CountryCode"/>
<xs:element maxOccurs="7" minOccurs="0" name="AdrLine" type="Max70Text"/>
</xs:sequence>
</xs:complexType>
```

Tereon includes all of these fields, but with slightly different naming tags. It has a one-to-one relationship to these fields and so can translate easily between its internal data source, and the ISO 20022 data format.

Difficulties occur where Tereon retains more information that that defined in the ISO standard. An example is the definition of ISODateTime:

```
<xs:simpleType name="ISODateTime">
<xs:restriction base="xs:dateTime"/>
</xs:simpleType>
```

The ISO 8601 standard does not define a representation for confidence intervals in a time and data stamp. Nor does it provide the granularity required by certain securities regulations, under which times need to be expressed to within 100ms. ISO 8601 does, however, allow for leap seconds. A provider’s standard system may not be able to process confidence intervals, geolocation data, or other data that is not included within ISO 20022. However, Tereon will still retain this data in its own internal audit logs, and the provider can use other Big Data systems to access and process this data, alongside the same data that was translated in the ISO 20022 for its internal processing systems. Kalypton can, of course, include some of this data in the defined supplementary data field.

```
<xs:complexType name="SupplementaryData1">
<xs:sequence>
<xs:element maxOccurs="1" minOccurs="0" name="PlcAndNm" type="Max350Text"/>
<xs:element name="Envlp" type="SupplementaryDataEnvelope1"/>
</xs:sequence>
</xs:complexType>
```

Kalypton can work with FPTF to define the format for any data that Tereon includes in a supplementary data field, or Tereon can simply provide a definition that fits with the existing definitions in the defined ISO 20022 payments messaging schema.

Just as Tereon will translate from its internal data formats to ISO 20022 on a one-to-one correspondence with its internal fields, so it will translate data from the provider’s ISO 20022 feed into its own data format on that same one-to-one basis. This will ensure that Tereon captures and transmits all relevant ISO 20022 formatted information, contextual or otherwise,

U.4.3: When will ISO 20022 contextual data requirements be prepared and available to Providers?

The ISO 20022 contextual data requirements are already defined in the current payments messaging schemas, which are available today from the ISO 20022 Registration Authority. The exact contextual data requirements will be dictated by, and depend on, the services that the providers wish to offer. Kalypton would define those requirements to the providers at the start of the implementation phase of the solution. Kalypton will also make available any extensions, such as definitions of additional or supplementary data, to the providers at the same time.

U.5 Cross-border functionality

Additional information

The answers to the following two questions will set out the additional information requested for this requirement.

Questions and answers

U.5.2: How will Providers document, quantify, and agree to manage settlement risk?

If Tereon is used to manage or action the settlement, then it removes the settlement risks that are normally associated with end-of-day or DNS systems.

Tereon's default mode of operation is to act as an RTGS (Real-Time Gross Settlement) system, and authenticate, authorize, approve, clear, and settle transactions in real-time. If it is used as a DNS (designated-time net settlement), or an RTGS-DNS hybrid (such as authenticate, authorize, approve, and clear a payment in real-time, with a defined time settlement for the funds), then it acts as a secured-DNS or Lamfalussy-plus system, as it secures and hypothecates the funds that a party requires to settle its transactions on an on-going basis (the answers to E.5 and S.1 will describe this in more detail).

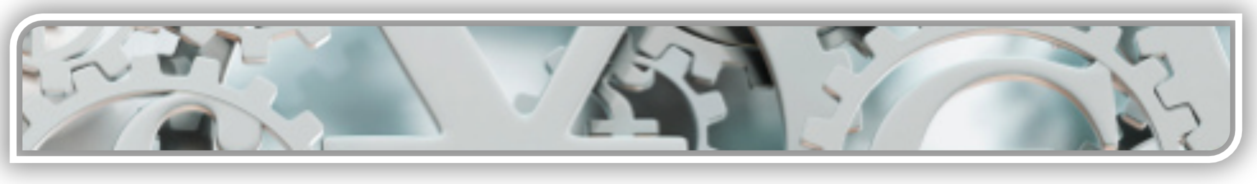
The system rules will detail the provider's obligations over settlement, including the requirements to ensure that funds are hypothecated and secured for the settlement, where that settlement occurs at a designated time. A user cannot make a payment or transfer unless the user has sufficient credit or funds, and the provider cannot approve the payment or transfer unless it has the funds to settle that payment or transfer (page 41 of the proposal).

U.5.2: Please provide details on how contextual data will travel in cross-border transactions.

Tereon makes no distinction between domestic or cross border transactions in respect of the contextual data that it transfers. It was designed to support both domestic and cross-border transactions. The contextual data itself is defined and predicated on the transaction type, and ISO 20022 is designed to operate internationally for both domestic and cross-border transactions.

Tereon does not depend on ISO 20022. It transmits the required contextual data within its own data format that supports more information than is currently defined the ISO 20022 (see answer to U.5.1 and additional information above), which it captures, regardless of whether the sender systems or the recipient system support or use ISO 20022. Tereon is designed to be agnostic with regards to any particular data format. It supports any format that can capture some of the data that it can carry, and it will always retain the data and make in available to the providers, irrespective of those providers' data formats. Tereon thus supports both ISO 20022-enabled end users (providers) and non-ISO 20022-enabled end users. Providers (and other end users) will thus benefit fully from the availability of contextual data in cross-border transactions, irrespective of whether they support ISO 20022 or not.

ISO 20022 is simply one of any number of formats that Tereon can support and translate between.



U.6 Applicability to multiple use cases

No questions

Efficiency

E.1 Enables competition

Additional information

The answers to the following two questions will set out the additional information requested for this requirement.

Questions and answers

E.1.2: Whom does the user need to contact in order to switch Providers? How does the switching process work? Does the end user's account history travel with the account to the new provider? What are the protections against account takeover and switching? Is a separate Tereon ID required to support accounts with multiple providers?

In order to switch providers, the default position is that the user needs to inform that user's new provider. The user need only do this because Tereon's directory look-up service manages the account switching process. (The detailed method is subject to a patent application, but Kalypton can reveal how this works at a high level.)

To transfer accounts from the user's old provider to the user's new provider, the user first opens an account with the new provider's Tereon system and registers his or her mobile, card, or another device. This will necessarily register the user's existing Tereon ID with the new provider (the user can also register non-device specific IDs such as an email address). The new provider's systems will detect that the user is already registered with the old provider via the directory look-up system and so will ask the user if the user wants to transfer his account from the old provider to the new provider.

Once the user has confirmed to the new provider that he wishes to transfer his account, the new provider begins the process of transferring accounts from the old provider. In order to protect against someone taking over his account, the user needs to confirm with both the new provider and with the old provider, using one-time authentication codes, that these providers will send to him via a separate communication channel, that he wishes to transfer his account. The providers may also require the user to provide some additional form of ID when switching accounts. The system rules will set out the options and controls that the providers must, at a minimum, follow before they switch accounts for a user.

Once the user has confirmed to both the old and the new provider that he wishes to transfer his account, the old provider's Tereon system informs the new provider's Tereon system of the user's account registrations, balances, configurations, payment instructions and so forth. The new provider's system sets these accounts up in exactly the same manner as those on the old provider, or as close as it can do to provide the services that it is authorized to provide. If there are any differences to the services that the new provider can offer, or if the user must make a choice of which services he wishes to have, then the new provider will contact the user at this stage and require the user to make his choice.

After it has set up the accounts, the new provider informs the directory look-up service that it now has registered the user's devices, and instructs the old provider's Tereon system to transfer the user's balances to it, together with the user's account history The old provider will now confirm with the directory look-up service that it no longer manages the user's IDs, and transfer the user's balances and account history to the new provider. Once complete, the new provider informs the old provider that it has received the balances and the account history, and informs the user that the account has been transferred.

The old provider now informs the user that his account has been transferred to the new provider, and closes the user's account.

If the user was overdrawn before transferring his account, and the new provider had agreed to accept the account, then the new provider could transfer funds to the old provider to clear the user's overdraft, and the user would now have an overdraft with the new provider. This could, to a user, appear to be similar to transferring a balance from one credit card to another.

If the user has multiple accounts with one provider, then that user can choose which of those accounts to transfer to a new provider. There is no reason that a user need transfer all of his accounts.

A user can register multiple IDs with a provider. It can also register the same ID and device with multiple providers. A user does not need separate IDs to support accounts with multiple providers. Just as the directory look-up service manages account switching, so it can differentiate between separate providers by the services that they provide to a user, irrespective of whether that user registers the same Tereon ID with those providers, or whether the user decides to register separate IDs with each provider.

Taking the example of an account switch again, suppose that the user is registered for both credit and debit transactions with one provider, and decides to register with a new provider for a better credit facility. Though the user can use the same ID, the directory look-up service will direct all debit-type transactions to the old provider, and all credit transactions to the new provider. A user can also register with two or more providers for identical services. The user can then elect which provider to use at any time simply by selecting which account to transact with.

E.1.4: Will the Solution explicitly require participating Providers to meet all applicable regulations and to be in compliance with all applicable payment scheme rules?

Yes, Tereon explicitly requires participating providers to meet all applicable regulations and to comply with all applicable payment scheme rules. The system rules and participation rules will state this explicitly.

E.2 Capability to enable value-added services

Additional information

The answers to the following two questions will set out the additional information requested for this requirement.

Questions and answers

E.2: How will the solution support the integration of value added services that are developed by a third party?

To integrate a service with Tereon, or to create an application that provides a service on Tereon, a third party needs only to conform to the APIs, protocols, and standards that Tereon uses. The APIs and protocols are language agnostic so that third parties are free to use a programming language of their choice to create new applications and services. A third party need only link to one provider's Tereon server in order to offer its services to any user who is allowed to use that service. The directory look-up service will enable users to access and make use of that third party's services.

Kalypton will publish the APIs, protocols, and standards necessary to enable providers to integrate with Tereon and provide value-added services to any user (page 116 of the proposal) or to connect their devices and provide services or application on those devices. These will enable any third party to develop, integrate, and support solutions and devices on Tereon. Where third parties require new APIs, or APIs that have not yet been published, then Kalypton will publish those on request.

Kalypton has already published APIs and protocols for earlier versions of Tereon. For example, the published APIs and protocols for Tereon version 3 for the mobile communications services define five discrete functional areas and over 110 pairs of calls and responses.

The APIs and protocols have been used for a variety of use cases, from connecting to an EMV gateway to enable transactions with existing schemes, to creating the mobile applications that are used to demonstrate Tereon, all the way to creating a plug-in to allow mobile payments via an e-commerce portal. The APIs and protocols have been used to add card-based payments to Tereon and to enable existing card terminals to interoperate with Tereon to support both card-based transactions, and mobile phone to card terminal transactions. The APIs and protocols have been used to integrate a touch screen information panel and convert it into a touch screen point of sale terminal.

As Tereon adds new services and functions, so Kalypton will publish APIs and protocols to enable third parties to make use of those functions and services. Kalypton created two sets of protocols on demand to support two projects. One was to enable a major vendor of a parking application to integrate its application to Tereon for a potential project in East Africa. The second project was to enable a third party to integrate its Tereon servers with a number of commercial ERPs to create a utility bill payment service. To write and comprehensively test a new Tereon API takes anywhere from a few days to approximately three man weeks.

E.2.3: Does the solution require the disclosure to customers that value-added services are optional?

Yes (page 116 of the proposal). Tereon will clearly disclose value-added services as optional extras. It will not allow providers to hide that fact.

E.3 Implementation timeline

Additional information

Kalypton agrees that there are substantial implementation challenges in respect of large financial institutions. In the event that a prospective user of a Tereon-based service banked with such an institution, they have the option to change their bank. Alternatively, they could open an account at a payment bank as part of the service registration process. This account would never hold funds. It would be used to pull funds from the user's main account at the reluctant financial institution and then on to the counterparty to the transaction. As this would be a transaction between licensed banks over existing rails, the reluctant financial institution would have no basis to block it.

Questions and answers

E.3: Please provide more details about the anticipated implementation timeline, including key activities and the dates for key deliverables. How similar is the implementation in Central America to the proposed solution for the U.S.? Will it be possible to leverage this implementation for the U.S. market?

It is difficult to provide an exact implementation plan and timeline, as Kalypton does not yet know who will participate in the eventual solution, or what base-line services the solution will support (Kalypton will base its estimate on the four use cases that the call for the proposal discussed). Kalypton can, however, provide an example timeline based on its experiences in other jurisdictions, and in the planned implementation in Central America in particular. Based on Kalypton's previous and current experience, it is entirely feasible that the solution could be implemented widely in the USA by the end of 2018, and achieve ubiquity within 18 months of implementation. It will follow on from and integrate learning from the Central America project.

Table 1 below summarizes the key components of that assumption, with the estimated times for the various stages of an example implementation project. Each of these stages is explained in more detail below. The times in the brackets refer to the estimated time take to implement the solution where the tasks are carried out sequentially. The times outside of the brackets refer to the estimated times with certain tasks are carried out in parallel.

Task Name	Duration
Tereon Implementation High Level Plan	
Service Scope Definition (Kalypton with FPTF)	**30 days**
Technical Architecture Definition	**20 days**
System development	**70 (100) days**
Service Development	**90 (150) days**
System Testing	**70 (120) days**
Service Launch Preparation	**20 days**
Training	**30 days**
Commissioning	**60 days**
Service Launch and Hand-over to Service Management	**90 (110) days**
	480 (640) days

Table 1 - Example of implementation time lines

The design for the planned implementation in Central America is very similar to that envisaged in the proposal, in that a number of banks will implement Tereon and offer a set of base-line services using the solution. The main difference is that the envisaged implementation in Central America will also offer a merchant payments solution. Kalypton fully intends to leverage this implementation for the

U.S. market, as the underlying implementation will be very similar to that in the U.S. The one exception is the implementation that is planned for the real-time, straight-through, check processing service, which is based on the regulatory requirements peculiar to jurisdictions outside of the U.S. Nevertheless, Kalypton can leverage the basic implementation for that as well, though with changes to meet the U.S. requirements if necessary.

In order to create the example implementation timeline, Kalypton will make some basic assumptions. Kalypton will define the base-line services and architecture in advance, and these will be the same for all providers. This will ensure a consistent user expectation across the industry but with scope for individual service providers to customize services subsequently. As with the planned Central American implementation, in order to speed the timelines, Kalypton envisages that the work to integrate Tereon with the providers' core systems will be carried out by the providers themselves. Kalypton will provide a full set of documented APIs, and the providers will use these APIs to integrate to their Tereon instances.

Kalypton plans to partner with one or more systems integrators, who will work with the providers to help carry out the implementation. The example implementation timelines below will reflect these assumptions.

The days given are rough estimates based on Kalypton's previous experience, and the implementation timelines below are based on an actual project timeline drawn up for both Central America and a project in East Africa. They were drawn up by an experienced project director in Kalypton who has over 25 years of experience in implementing banking infrastructure in challenging environments. The days outside of brackets show the estimated time when some of the tasks run in parallel. The days in brackets show the timelines is all tasks run consecutively.

Service definition

Kalypton assumes that the FPTF will wish to define the scope of the implementation, borrowing from the work carried out for the Central American implementation. The following table sets out the estimated timelines for this stage of the proposed project.

Task Name	Duration
Tereon Implementation High Level Plan	
Service Scope Definition (Kalypton with FPTF)	**30 days**
Define and document requirements (FPTF process)	
Agree critical success factors	2 days
Agree Key Performance Indicators	3 days
Create high level milestone plan	1 week
Agree high level base-line service design (FPTF process)	
Create Service design	4 weeks

Technical architecture

The technical architecture will be based on the architecture drawn up for the Central American implementation. Kalypton will work with the providers to define two separate test environments that the providers will create. This applies regardless of whether a provider wishes to provide the service itself, or whether it wishes to provide the service on a SaaS basis to separate financial institutions.

Task Name	Duration
Technical Architecture Definition	**20 days**
Create user acceptance testing environment	2 weeks
Create operational acceptance testing environment	2 weeks

System and service development

The system and service architecture will again be based on the architecture drawn up for the Central American implementation. However, it is here that the services may diverge from the designs for the Central American implementation as the base-line use cases will differ if they are based solely on those drawn up in U.6 of the faster Payments Effectiveness Criteria. This will also be the stage when the provider begins to develop its own versions of the applications (not shown, as that will be for the provider to schedule).

Task Name	Duration
System development	**70 (100) days**
Agree high level data architecture (if Kalypton is to replace internal messaging set)	4 weeks
Agree system security architecture	4 weeks
Document system interfaces (in parallel with *)	6 weeks*
Document system operation specification (in parallel with *)	6 weeks*

The service development stage differs from the system development stage in that Kalypton and the providers will be examining how the services will integrate with their existing systems. Again this will very much depend on how they wish to operate. The following table is therefore a rough estimate. If the provider must hold its funds in a control account, such as when it cannot provide or manage accounts in its own right as a bank or a non-bank account provider, then it will need to involve the bank that will hold the control account on its behalf.

Task Name	Duration
Service Development	**90 (150) days**
Agree high level service architecture	4 weeks
Agree detailed service design	4 weeks
Define service interfaces (in parallel with *)	6 weeks*
Define non-functional specification (in parallel with *)	6 weeks*

Define system operation specification (in parallel with *)	6 weeks*
Create high level service design	2 weeks
Define service support model	2 weeks

During the service development stage, the software and hardware will be installed at a location specified by the provider. This will happen in parallel with the stages listed in the table above.

System testing

The system testing stage will put in place within the provider the structures, procedures, and processes to maintain and support the solution.

Task Name	Duration
System Testing	**70 (120) days**
Agree testing strategy	2 weeks
System testing	**30 days**
Write testing artefacts (in parallel with *)	2 weeks*
Perform testing (in parallel with **)	4 weeks**
Quality Assurance testing	**30 days**
Write testing artefacts (in parallel with *)	2 weeks*
Perform testing (in parallel with **)	4 weeks**
User Acceptance testing	**30 days**
)	
)	
Operational Acceptance testing	**20 days**
)	
)	

Preparation to launch services and initial training

The preparations to launch the services will include a period of testing with a select group of users to ensure that the services perform as designed and to prepare for the wider pilot. Kalypton will also work with the provider during this stage to help the provider train its service support and operational management teams. Some of the training can run in parallel, though the times are displayed sequentially below for the sake of simplicity.

Task Name	Duration
Service Launch Preparation	**20 days**
Test & Launch Preparation (variable)	4 weeks
Complete Test & Launch Preparation	0 day
Training	**30 days**
Pilot	2 weeks
User training	2 weeks
Operational training	2 weeks
Service support training	2 weeks
Service management training	2 weeks

Pilot and commissioning

If the provider intends to provide the services to end users, then the pilot and commission stage will be the final stage. The pilot and commissioning stage will take into account any teachings from the initial testing stage in order to specify and provision the final; hardware and networking configuration to meet the provider's requirements. In some cases, where the provider has already analyzed their requirements during the system, and service development stages, the commissioning phase will be far shorter than set out in the following table.

Task Name	Duration
Commissioning	**60 days**
Assign data center capacity (variable)	2 weeks
Implement core architecture (variable)	4 weeks
Implement network connectivity (variable)	6 weeks
Service Launch and Hand-over to Service Management	**90 (110) days**
Pilot Service	**60 (80) days**
Launch and hand-over to service management (variable) (in parallel with *)	4 weeks*
Complete launch and hand-over to service management (in parallel with *)	0 days*
Perform pilot (in parallel with *)	12 weeks*
Production Service	**20 days**
Launch and hand-over to service management (variable)	4 weeks
Complete launch and hand-over to service management	0 days
Service Management service quality review	**10 days**

Service review	2 weeks
Complete service review	0 days

If the provider intends to provide Tereon as a SaaS to financial institutions and other secondary providers, then there will be an additional stage in the production service section to link the service to those secondary providers. In addition, the provider will need to repeat some of the earlier development, testing, and launching stages with those secondary providers; it can begin these in parallel with the preparation to launch stage and the subsequent stages.

The implementation of the rules and agreements that will govern the solution, together with the governance structure for the solution, will occur along similar lines, and will run in parallel to the above implementation project.

Task Name	Duration
Rules and Agreements Implementation High Level Plan	
Create working group and appoint governing board	30 days
Drafting preliminary rules and agreements	60 days
Vetting by subcommittees and legal subcommittee, and redrafting based on inputs	60 days
Approval by operations committees and approval by governing board, including any revisions and subsequent approvals	180 days
Rules Launch Preparation	
Publication and training	30 days
Complete launch and implementation	0 days
	360 days

Table 2 - Implementation of rules, agreements, and governance structure

The above timelines do not take into account any additional time that the stages may require if other statutory and regulatory bodies become involved in the process to agree the rules, implementation, and governance structure. The time lines do, however, provide an indication of an example plan to implement those tasks.

The example implementation plan sets out a generous timeline that, nevertheless, will complete within 2018. The widespread adoption of the solution amongst the industry will provide most of the main drivers that are required to achieve ubiquity quickly, namely the widespread adoption of an interoperable solution amongst numerous providers, all of who will provide a common set of base-line services to their end users. This represents a similar scenario to that which allowed M-Pesa to grow quickly, a wide spread adoption of a service, albeit from one provider with market dominance and a permissive regulatory regime. Tereon is designed to operate within the existing financial services regulations and so does not require any regulatory exemptions. There is no need for Tereon to be offered by a provider with market dominance; the solutions' interoperability, together with a proposed common set of base-line services, means that users will have a common set of services that they can use to interact with other users, irrespective of the providers that the users are registered with.

The implementation timelines do not include any marketing or public relations tasks. Those are for the individual providers to undertake according to their own commercial drivers. However, the providers can begin to market their proposed solutions at any time during the implementation timeline.

Kalypton cannot estimate the internal costs of a payment service provider in delivering the project plan outlined above as it is not privy to the provider's internal costings or indeed those of a systems integrator, without defining their scope. Kalypton can however state that its cost element of delivering the project plan is several orders of magnitude less than other major projects of this nature. Kalypton charges a daily rate during the scoping exercise and then upfront payment to cover the software implementation and customization phase based on the identified scope, followed by monthly time and materials invoicing as its team assists in the implementation and testing phases of the project within agreed parameters and milestones. Kalypton's team is highly skilled. Due to the almost plug and play nature of Tereon, Kalypton's team is small in number and this means that its costs remain low.

E.4 Payment format standards

Additional information

Tereon is designed to retain all information that it captures and generates when processing a transaction, irrespective of whether the format that it translates that information into can accept that data. The approach with Tereon has been to enable support to all standards as required and as they evolve.

Kalypton appreciates the importance of standards. Standards are important to achieve ubiquity where the solutions using them do not have extensibility. However, as in the case of ISO 8583, they can also impose considerable migration or conversion costs. If Tereon simply implemented ISO 20022 as currently published, it might have challenges in future proofing, dealing with historic implementations, or dealing with transactions with solutions implementing other standards.

This is not the case with Tereon's design. Tereon can implement ISO 20022 as it is now, both historically and as it will evolve, and it can implement all other standards contemporaneously. Tereon is designed to support multiple message formats, and to translate between formats and between differing versions of those formats without data loss.

Questions and answers

E.4.4: How will the Tereon message format foster innovation with a proprietary message set? What steps have been taken to ensure that Tereon's proprietary messaging will not be limiting?

The entire purpose of Tereon's internal messaging design is to ensure that it is not limiting in any way. It can interoperate with existing standards, such as ISO 20022 (including the various versions of the message definitions within that standard), and it is designed to adapt to future needs and standards as these arise.

Tereon does not have a "*proprietary*" messaging set and nowhere in the text of the proposal does Kalypton make that claim. Kalypton states that Tereon uses an internal messaging protocol that is designed to enable it to capture accurately any information necessary to process and audit a transaction of any type. Its design enables us or a third party to extend the messaging definitions to cover any required information type. Tereon's messaging set is extensible, rather than fixed and proprietary.

Without this extensible nature, Tereon simply could not add new APIs or services to extend its capabilities into the future. Tereon is extensible, and its messaging set supports that feature.

As the answer to E.4.1 in the proposal (page 117 of the proposal) states, Tereon can interface to, or interoperate with, any existing payment format standard, including customized versions of ISO 20022, ISO 8583, and so forth, and it can adapt to any amended or superseding standards as required. The answer to U.4 above explains some of the limitations of the ISO standard when compared to the information that Tereon captures. For example, the definition of ISODateTime tag:

```
<xs:simpleType name="ISODateTime">
<xs:restriction base="xs:dateTime"/>
</xs:simpleType>
```

does not define a representation for confidence intervals in a time and data stamp. Nor does it provide the granularity required by certain securities regulations, under which times need to be expressed to within 100ms. Tereon will capture the confidence intervals and the granularity required. Tereon stores the date and time stamp in a field called <datetime>, which has a direct one-to-one relationship with the ISO 20022 field ISODateTime. Tereon stores the confidence interval for the date and time stamp in a separate field <datetime_error>, which sets out the value of the interval for that particular date and time. These will change slightly during a day, and Tereon will simply record the confidence intervals alongside the date and time recorded for each transaction. In order to capture the information, Tereon uses the Precision Time Protocol and GPS synchronized clocks to keep the time confidence interval to a minimum.

Tereon does not just support extending a particular format, it can also support different versions of the same format. Tereon can also support multiple versions of the same format, translating from one to the other, if necessary.

E.4.4: How will the Solution ensure that contextual data will be accurately translated from the internal protocol to another messaging format and vice versa?

Tereon is designed to translate from one format to another. Tereon uses schemas that associate the fields in a particular format (or version of that format) to the fields that it uses internally. Tereon does not lose any information but retains its own records, as well as the records of the information that it supplies to a provider or received from a provider, in the format that it supplies or receives that information. Tereon is designed to conform to the strictest interpretation of evidential requirements.

Where Tereon translates the data that it captures to a messaging format such as ISO 8583 or ISO 20022, Tereon is designed to retain the data in its original form as well as to present the data in the format required by a provider. Tereon does not delete its records once it has translated data into a particular format. ISO 8583, for example, is far more restrictive than ISO 20022. It is a set bitmap format that was originally designed to support card transactions, and three versions exist, ISO 8583:1987, ISO 8583:1993, and ISO 8583:2003. They are not interchangeable. For example, ISO 8583:1993 sets out the transaction amount and currency in two separate fields (field 4 contains the transaction amount, and field 49 contains the currency code). In ISO 8583:2003, the currency code is contained as a sub element of the transaction amount field. Tereon can easily translate between these variants.

Where translating data into a format would mean that the format contains less information that the original data set, then Tereon will provide the data that it can in the required format and retain the original data in its original format. For example, when translating its record of the time stamp to the ISO 20022 ISODateTime tag, Tereon will enter the date and time in the required ISO 8601 format (or any other format required by the target data format – ISO 8583:1993 does not use the ISO 8601 format), and retain its original record as well in the event that the provider wishes to access the original records at any time during or after the transaction. Tereon retains its data in UTF-8 format to enable the provider to access the original records at any time. The format is well documented and the provider will be able to use any tool that can import data in UTF-8 format.

When Tereon translates from a format into its own messaging system, it will also retain the original data in its original format. For example, if a provider communicates in a format that uses a non-ISO 8601 date and time field, such as a numerical format where the date and time is simply represented by pairs of numerals in the form YYMMDDHHMMSS), then it will translate this into the ISO form. The translation scheme for that provider will include the Y2K date window, which will inform Tereon which century a two-digit date will fall into – this should only be necessary for historical dates. If the provider cannot supply its Y2K date window for Tereon's schema, then Tereon will assume that a transaction falls within the year in which it receives the date and time from the provider. A few well-known, defined payments formats leave out the year entirely, and the translation schema from the provider's format to Tereon's messaging set will specify that Tereon will assume that the year is the year within which Tereon received that date and time information from the provider. Some formats only specify the month and day. Again Tereon will accept the information, and then supply any other information, such as the time, and the time confidence interval based on the time that it receives the information from the provider. Tereon will clearly record where it has had to supply information that was otherwise missing from the original message format, and it will retain that original message in its original format alongside its internal records.

E.4.5: Could the proprietary message format could be replaced with a different message format if required?

Yes, in the sense that Tereon can replace its flexible messaging system with another message format if required, so long as that message format captures the data that Tereon's format currently captures. Tereon could, for example, simply implement the ISO 20022 data tags for defined versions of the various message schemes, and then extend those tags by adding proprietary fields to capture the data that is otherwise missing from the ISO 20022 message definitions. However, if Tereon were simply to use ISO 20022 as the internal messaging format then it would severely limit the capabilities and extensibility of Tereon. ISO 20022 is an ongoing process as message definitions are created, upgraded, and superseded.

Tereon's design allows it to support any number of versions of messaging standards. Thus by using its internal messaging system, Tereon can truly support and continue to support ISO 20022 as that standard evolves.

E.5 Comprehensive

Additional information

Tereon supports the payments process from end to end. It does not have any requirements as to end user accounts as it imposes no requirements. Tereon can provide an end-user account management system, which to an intents and purposes can resemble an on-line bank account. The user can access his or her statements and transaction history, register new devices, deactivate old devices, and so on. Where a provider already provides user account facilities, Tereon can simply integrate to the provider's existing systems via APIs. The provider can simply add Tereon as an additional function or service to its existing user accounts.

Questions and answers

E.5.2: Please provide more details regarding the control account and the settlement account. Who can access each Provider's account? Can Kalypton access all settlement accounts?

In summary, control accounts are there to support the use of Tereon for real-time payments in fiat or commercial money by non-bank service providers with the support of a bank implementing one of two banking strategies identified in McKinsey's "The Fight for the Customer" where banks offer their balance sheet for resale. Settlement accounts are the interface between the authorization and clearing process on one hand and the settlement process on the other. Tereon can use existing settlement mechanisms or support settlement innovation as well as payment innovation. If the latter approach is taken, it will reduce costs of settlement, reduce or eliminate associated liquidity and credit risks, and reduce liquidity requirements enhancing the overall business case for innovation supported by all including major banks. Tereon provides a seamless migration path from current settlement system to a full function and ubiquitous real-time settlement process without restrictive minimum transaction values.

Settlement accounts and control accounts are discrete accounts, each of which serves a separate purpose. A provider will keep funds in a control account, either held by itself or by a bank on its behalf, where it holds funds for users who do not qualify for bank accounts. An example of such as user may be an individual who was previously unbanked and has now opened an account in order to build a financial profile and history before becoming a fully banked user. Another may be a user who has registered for an "account" with a provider that cannot itself provide individual accounts.

In both of the above cases, the provider will hold the funds for all such users in a single control account. The Tereon server will operate ledger entries for each user. To the user, the experience of using Tereon will appear as if the user has an account. The user will only see his or her entries, and the running total for the funds attributed to that user in the ledger entries. The funds, however, will all reside in one account.

If one user with a ledger in a control account transacts with another user who has a ledger and funds in the same account, then no money will leave or enter the control account (other than any fees charged for the transaction). Tereon will simply debit one set of ledger entries and credit another. If the first user wishes to transfer $50 to the second user, and both use the same provider and have funds in the same ledger account, then Tereon will simply reduce the transferor's ledger entry by $50 and increase the recipient's ledger entry by $50. If the provider charges a fee for that transaction, then it will debit that fee from whichever user pays the transaction charge.

Figure 34 on page 90 of the original proposal sets out an example of two providers, one of which offers its users bank accounts while the second cannot do so and instead holds its users' funds in a control account operated by its bank. The case study to which the figure relates sets out a transfer from a registered user with a bank account to a registered user who uses a provider that holds the user's funds in a control account. Here the transferor wishes to transfer $150 to the recipient. Because the funds come from a transferor who holds funds in a separate account (in this use case the funds are in the transferor's bank account), when the transferor transferred the funds, the transferor provider's Tereon system debited the transferor's account $150 and then transferred the funds to the recipient's provider through the settlement system. The recipient provider's Tereon system instructs the bank to allocate the $150 that it receives through the settlement system to the provider's control account, and the provider's Tereon system then increases the recipient's ledger entry by the $150. In other words, the transferor's bank account is debited $150. The recipient's ledger is increased by $150, but that $150 is credited to the provider's control account. The ledger simply shows that the recipient now has an additional $150 of the funds in the control account registered to him. His value of the recipient's share of the funds in the control account has increased by $150.

If the transfer was the other way, that is from a transferor whose funds are held by his provider in a control account to a recipient who has a bank account, then the process is similar. The transferor provider's Tereon system first checks the value in the transferor's ledger to verify that the transferor has sufficient funds registered to him. If the transferor has sufficient funds, then the transferor provider's Tereon system will decrease the transferor's ledger by $150, and instruct the provider's bank to debit $150 from the control account and transfer that sum to the recipient's bank via the settlement system. The recipient provider's Tereon system will credit the recipient's bank account with $150 that it receives via the settlement system.

Conceptually, the control account is similar to a cookie jar into which housemates will put in money to pay for sundries and register their contributions in a ledger or book. Though the money is in a single jar, each will know what he or she has contributed and spent. Unlike Tereon, each housemate will know what the others have contributed (in Tereon, only the provider's administrators and the user will see the ledger entries for that user that will, to all intents and purposes, resemble the statement entries in a bank account). The settlement accounts are different to the control accounts. These are the accounts the register the settlement positions of the providers.

If Tereon is used to provide the settlement system, then it will be able to debit and credit the entries in the settlement accounts directly in order to provide complete end-to-end control of a transaction. If Tereon is not used to provide the settlement system, then the provider can determine whether to use Tereon to debit and credit the settlement accounts of the settlement system that the provider uses, or whether to simply require Tereon to send settlement instructions to the provider's settlement system.

Please provide more details regarding hardware and infrastructure requirements for Providers who wish to implement the Solution.

Tereon does not require specialist hardware or networking. The actual requirements for each provider will depend entirely on the number of users that a provider wishes to service, and the number of services that the provider will offer to its users. The answer to E.6 below goes into more detail.

Please describe the settlement process in more detail. How will the process will change if a real time settlement capability is used rather than a batch capability?

Tereon's default mode of operation is to act as an RTGS (real-time gross settlement) system, and authenticate, authorize, approve, clear, and settle transactions in real-time. It removes the risk of settlement lags and asynchronous settlements, which are a major cause of credit and liquidity risks. The details of how it does so are subject to a patent application. If Tereon is used as a DNS (designated-time net settlement), or an RTGS-DNS hybrid (such as authenticate, authorize, approve, and clear a payment in real-time, with a defined time settlement for the funds), then it acts as a secured-DNS or Lamfalussy-plus system, as it secures and hypothecates the funds that a party requires to settle its transactions on an on-going basis.

The report *Real-Time Gross Settlement Systems* from the Bank for International Settlements (1997), identifies RTGS systems as being the only settlement system compatible with genuinely continuous real-time settlement. Table 3 below is quoted from the BIS report and encapsulates the differences between RTGS and DNS systems. The table does not capture well the point that existing RTGS solutions, e.g. the UK CHAPS solution, are really only used for very large value transactions and are unsuitable for use at scale with small value transactions.

Settlement characteristics	Gross	Net
Designated-time (deferred)	Designated-time Gross Settlement	Designated-time Net Settlement (DNS)
Continuous (real-time)	Real-time Gross Settlement (RTGS)	(not applicable)

Table 3 - Types of large-vale fuds transfer system

Figure 1 below illustrates the three settlement modes that Tereon can support. As mentioned above, Tereon can provide or support either an RTGS system, an RTGS-DNS hybrid system, or a secured-DNS system.

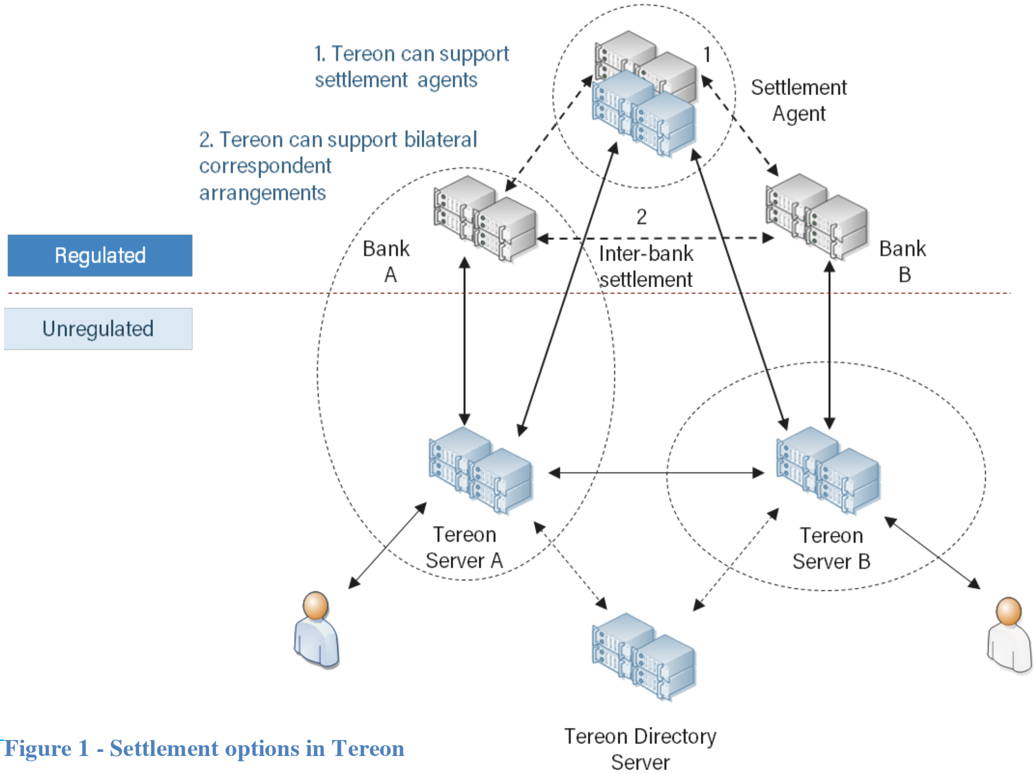


Figure 1 - Settlement options in Tereon

There is a fourth mode that Tereon can support, namely a bilateral correspondent arrangement where Tereon simply manages the providers' correspondent nostro/vostro accounts in bilateral settlement relationship, though this is becoming rare as providers opt to settle via a settlement agent.

Figure 1 also illustrates two other features of Tereon. The first is that provider B holds its funds in a control account with bank B, whereas provider A can provide accounts to its users directly (it is a bank). The second point is that Tereon can be provided as a SaaS service, where the messaging is managed at one level, whereas all transfer or settlement instructions are managed between the banks (or account providers) themselves in a highly regulated environment.

When used as a settlement system, Tereon is designed to eliminate where possible the two basic risks associates with batching or netting settlement systems. The report *Real-Time Gross Settlement Systems* from the Bank for International Settlements (1997), identifies these two basic risks as credit risk and liquidity risk.

The report makes clear that settlement risk "comprises both credit and liquidity risks" (italics are as in the original text):

> "*Credit risk*, which is often associated with the default of a counterparty, is the risk that a counterparty will not meet an obligation for full value, either when due or at any time thereafter. It generally includes both the risk of loss of unrealized gains on unsettled contracts with the defaulting counterparty (*replacement cost risk*) and, more importantly, the risk of loss of the whole value of the transaction (*principal risk*). *Liquidity risk* refers to the risk that a counterparty will not settle an obligation for full value when due but at some unspecified time thereafter. This could adversely affect the expected liquidity position of the payee. … *Settlement risk* may be used to refer to the risk that the completion or settlement of individual transactions or, more typically, settlement of the interbank funds transfer system as a whole will not take place as expected."

The report goes on to explain that the major sources of credit and liquidity risks are a settlement lag, which occurs when there is a time-lag between "the execution of a transaction and its completion" and an asynchronous settlement, which occurs when there is a time-lag "between the completion of the two legs of the transaction", namely between payment and delivery. As the report states:

> "Settlement lags can result in *credit risk* if the two functions of an interbank funds transfer system … (namely the transmission of information about the payment and the settlement of the payment) do not occur simultaneously, so that settlement takes place after the information has been provided. As long as final settlement has not occurred, any payment activity undertaken on the basis of "unsettled" payment messages remains conditional and results in risk. … Settlement lags may also result in *liquidity risk*. Until settlement is completed, a bank may not be certain what funds it will receive through the payment system and thus it may not be sure whether or not its liquidity is adequate."

Asynchronous settlements also pose risks as the settlement lag means that "there is a risk that the seller of an asset could deliver but not receive payment or that the buyer of an asset could make payment but not receive delivery." An RTGS system, which settles only when the buyer pays and the seller delivers removes those risks entirely.

It is to prevent such risks that Tereon's default position is to settle every transaction simultaneously (as part of the overall transaction) with the payment instructions. As the report confirms:

> "RTGS systems can contribute substantially to limiting payment system risks. With their continuous intraday final transfer capability, RTGS systems are able to minimize or even eliminate the basic interbank risks in the settlement process.
>
> More specifically, RTGS can substantially reduce the duration of credit and liquidity exposures. To the extent that sufficient covering funds are available at the time of processing, settlement lags will approach zero and so the primary source of risks in intrabank funds transfers can be eliminated. Once settlement is effected, the receiving bank can credit the funds to its customers, use them for its own settlement purposes in other settlement systems or used them in exchange for assets immediately without facing the risk of the funds being revoked."

The core of Tereon's settlement system is to ensure that the provider has sufficient funds, or has ample warning in advance to provide sufficient funds, to settle each and every payment. If Tereon is used to provide a batch settlement capability, then it will do so either as an RTGS-DNS hybrid system or a secured-DNS system in order to ensure that the settlement system has sufficient funds to settle a payment. DNS systems present settlement risks as they incur a settlement lag or asynchronous settlement due to the very nature of the fact that they defer settlement to sometime after the initial payment message. The Lamfalussy Report, referred to in the BIS report, analyzed the nature of DNS systems and recommended a minimum set of standards for netting systems which were set out in the six minimum standards or principles (sometimes referred to as the Lamfalussy principles) that netting systems should meet. These are (quoted from the Lamfalussy Report):

I. Netting schemes should have a well-founded legal basis under all relevant jurisdictions.

II. Netting scheme participants should have a clear understanding of the impact of the particular scheme on each of the financial risks affected by the netting process.

III. Multilateral netting systems should have clearing-defined procedures for the management of credit risks and liquidity risks which specify the respective responsibilities of the netting provider and participants. These procedures should also ensure that all parties have both the incentives and the capabilities to manage and contain each of the risks they bear and that limits are placed on the maximum level of credit exposure that can be produced by each participant.

IV. Multilateral netting systems should, at a minimum, be capable of ensuring the timely completion of daily settlements in the event of an inability to settle by the participant with the largest single net-debit position.

V. Multilateral netting systems should have objective and publicly-disclosed criteria for admission, which permit fair and open access.

VI. All netting schemes should ensure the operational reliability of technical systems and the availability of back-up facilities capable of completing daily processing requirements.

These principles are interesting in that they do not seek to remove the settlement risks presented by a DNS system, but to ensure that the system has procedures available to manage them as and when they occur. Tereon's core design goal is to remove settlement risks from a payments system.

When used as the basis of an RTGS-DNS hybrid system or a secured-DNS system (sometimes referred to as a Lamfalussy-plus system), Tereon will hypothecate (or secure) the funds necessary for a settlement account to settle each payment as it processes that payment. Each provider will see, on a continuous basis, its net exposure, and can ensure that it has sufficient funds to enable Tereon to hypothecate the required funds. The funds are retained in separate accounts and held on behalf and to the order of the recipient until actual settlement for funds takes place, and the recipient can be assured of receiving those funds, even if the sender bank fails before the actual settlement takes place; the necessary funds have already been safeguarded. Where Tereon is used to provide the basis of a full RTGS system, then there is no need for any hypothecation as it settles the transaction in real-time as it processes the payment instruction.

The use cases set out on pages 60 to 99 of the original proposal could use any of the settlement modes supported by Tereon (with the exception of the transfer to an unregistered user, where the settlement will use either an RTGS-DNS hybrid or the secured-DNS mode as the funds cannot be transferred to the final recipient until that recipient accesses the funds). Tereon considers the transaction settled as soon as it updates the settlement accounts with the transactional information. The settlement mode used by Tereon will determine how settlement proceeds thereafter.

If Tereon uses the RTGS-DNS hybrid system or a secured-DNS system, then once Tereon has the payment details, it will calculate the net debit position of the sending provider and the net credit position of the receiving provider and hypothecate funds to cover the transaction where necessary:

- If the transaction will increase the net debit position of the sending provider and that debit position remains within the limit set for that provider, then Tereon will –
    - instruct the sending provider’s system to debit the payer or transferor’s account
    - instruct the sending provider’s system to debit its settlement account in relation to the receiving provider
    - instruct the sending provider’s system to hypothecate the funds for settlement account to be held in favor of and to the order of the receiving provider; and
    - instruct the receiving provider’s system to credit its settlement account in relation to the sending provider. The receiving provider can credit the recipient as it now knows that it will receive the funds when the funds settle.
- If the transaction will decrease the net credit position of the sending provider (such as where the sending provider is due to receive more funds, but not so that the sending provider’s position becomes a net debit, then Tereon will –
    - instruct the sending provider’s system to debit the payer or transferor’s account
    - instruct the sending provider’s system to debit its settlement account in relation to the receiving provider; and
    - instruct the receiving provider’s system to credit its settlement account in relation to the sending provider. The receiving provider can credit the recipient as it now knows that it will receive the funds when the funds settle.
- If the transaction will increase the net debit position of the sending provider and that debit position will exceed the limit set for that provider, then Tereon will –

- instruct the sending provider’s system to debit the payer or transferor’s account
- instruct the sending provider’s system to hypothecate the funds for settlement account to be held in favor of and to the order of the receiving provider
- instruct the sending provider’s system to transfer the previously hypothecated funds to its account at the settlement agent to cover the net debit position, or to obtain a temporary credit facility to cover the additional exposure (depending on the final rules of the scheme, which will be decided by the FPTF)
- instruct the sending provider’s system to debit its settlement account in relation to the receiving provider; and
- instruct the receiving provider’s system to credit its settlement account in relation to the sending provider. The receiving provider can credit the recipient as it now knows that it will receive the funds when the funds settle.

In the last example, the actual mechanism used to cover the additional net debit position will depend on whether the settlement system is an RTGS-DNS hybrid system or a secured-DNS hybrid system. In an RTGS-DNS hybrid system, the RTGS is usually operated by the central bank, and whether or not the central bank will extend credit to the participants to cover any temporary liquidity shortfall is a matter for the central bank and the structure of the market. Any transfers to the settlement system, or any liquidity provided to cover the temporary liquidity shortfall will be transferred via the RTGS to the DNS used by the payments system. If the settlement system is a secured-DNS system, then this will usually be operated by a commercial entity using commercial bank money. In this case, the sending provider will either need to transfer additional funds to its account with the settlement agent to cover its position, or it will need to obtain a short-term commercial loan to cover its position until it transfers its funds at the time of actual settlement. Any credit in either the RTGS-DNS hybrid system or the secured-DNS system will be covered by collateral from the sending provider, and the recipient provider will know that it will receive the funds on settlement. Though there is a settlement lag, the funds are secured and the receiving provider can rely on receiving them at the designated settlement time set out in the system rules.

As has been mentioned above, Tereon’s default position is to act as an RTGS system. In this case there is no need for the sending provider to hypothecate any funds, as the funds are settled between the sending provider and the receiving provider via the settlement agent at the time that the payment instruction is processed. This removes any settlement lag and thus the credit and liquidity risk that a settlement lag could pose to the receiving provider.

The settlement message flow in Tereon resembles the “V” or “Y” shape as set out in the report from the BIS. Figure 1 above shows the message flow between the providers and the settlement agent, albeit that the shape is inverted.

Figure 2 below shows the message flow in the correct orientation. The shape becomes apparent when the Tereon server is separated from the bank server. This settlement server can be operated by a third party or by a central bank. The account, and the funds, however, will almost always be in the central bank and the settlement will occur using central bank money. The reason is that the central bank is the only institution capable of providing the necessary credit facility at short notice, on an automatic basis if necessary, should a sending provider require a credit facility to settle a sudden, large payment obligation. Any credit would be provided based on collateral offered by the provider to cover such an event.

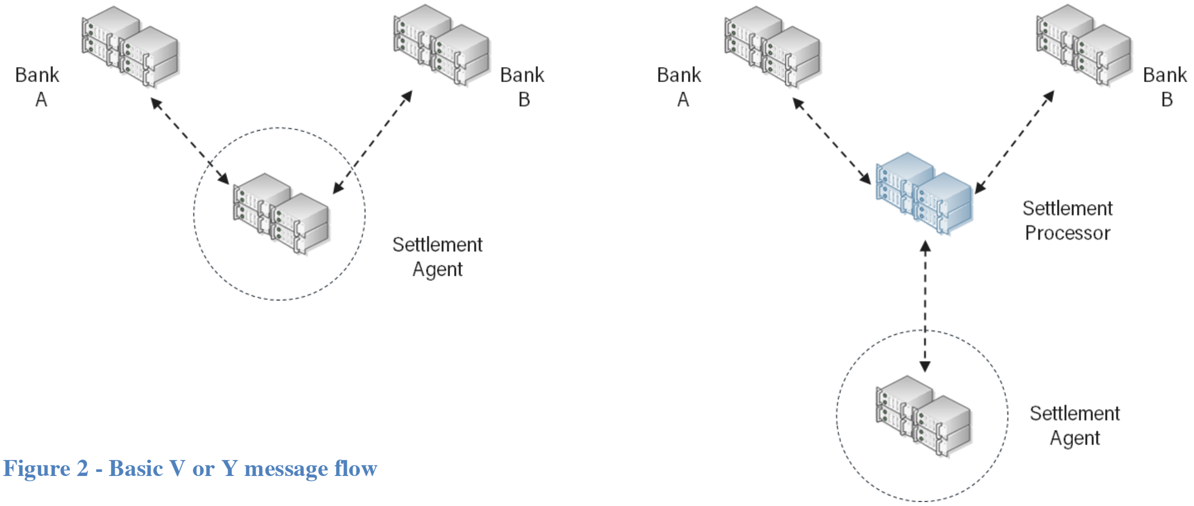


Figure 2 - Basic V or Y message flow

If a standard RTGS system uses the V-shape message flow, then the sending provider (a bank) will send the payment message directly to the settlement agent. The settlement agent (usually a central bank) will process the payment message, confirm that the sending bank has sufficient funds in its account to settle the payment, and then send the payment message to the receiving provider (a bank) with confirmation that the payments has been settled. If the RTGS system uses the Y-shape message flow, then the sending provider sends its payment message to a settlement processor that will process the payment message. That settlement processor may be operated by the settlement agent or it may be an independent entity operating on behalf of the settlement agent. That settlement processor processes the payment message, generates a settlement request from that payment message, and sends the settlement request to the settlement agent. This simply instructs the settlement agent to settle the amount between the sending provider and the receiving provider. The settlement agent will confirm that the sending bank has sufficient funds in its account to settle the transaction, and will then settle the transaction and inform the settlement processor that it has settled the transaction, and the settlement processor will send the payment message to the receiving provider with confirmation that the transaction has been processed.

Unlike traditional message flows in RTGS system, which are not designed for real-time payments, Tereon separates the settlement message from the payment message. Figure 3 below illustrates this flow. As the user cases in the original proposal discuss, the sending provider and the receiving provider will negotiate the payment message between them. Once the transaction has been authorized, approved, and cleared, the sending provider will send a settlement message, not a payment message, to the settlement processor (a Tereon server). That settlement processor will instruct the settlement agent, via the settlement agent's Tereon server, to settle the transaction amount between the sending provider and the receiving provider, which it will do as in the Y-shaped message flow.

Once the settlement agent has informed the settlement processor that the transaction has been settled, the settlement processor will inform both the sending provider's Tereon server and the receiving provider's Tereon server that the settlement has been settled. The providers' Tereon servers will confirm the transaction with their users and complete the payment message, and the settlement provider will record that transaction as complete. This means that neither the sending provider nor the receiving provider can act on any payment message until the transaction has been settled, as the payment message will be incomplete, and the settlement agent does not have the burden of having to process payment messages. This removes all settlement lag, and any chance of an asynchronous settlement, and as such eliminates settlement risk.

When examined in this way, Tereon's payment and settlement messages flow resembles a hybrid between a V-shape or Y-shape flow and a T-shape flow. The settlement messages take a V or Y-shape flow, whilst the payment messages themselves travel across the cross-bar of the T. Whether Tereon's settlement messages take a V or Y-shape flow depends entirely on who operates the settlement processor server. If the settlement agent operates both the settlement accounts and the server then the message flow is V-shaped. If the settlement processor operates as a separate entity, then the message flow is Y-shaped.

Tereon uses its hybrid message flow structure as this structure also works for an RTGS-DNS hybrid system or a secured-DNS system. In either of these two systems, the message that the settlement agent returns to the receiving provider differs slightly from the RTGS system. The settlement agent will confirm that the funds to settle the transaction on behalf of the receiving provider are secure, and the receiving provider can rely on receiving those funds at the designated settlement time. Both providers can then conclude the payment message, and the receiving provider can, if it chooses to do so, credit the recipient's account with the funds that it is not guaranteed to receive. In this way, though the RTGS-DNS hybrid system and secured-DNS system incur a settlement lag for the funds, they too remove the credit and liquidity risks associated with DNS type systems, as the funds to settle the transaction are secured, and the receiving provider will receive the funds, no matter what befalls the sending provider after the two providers complete the payment message.

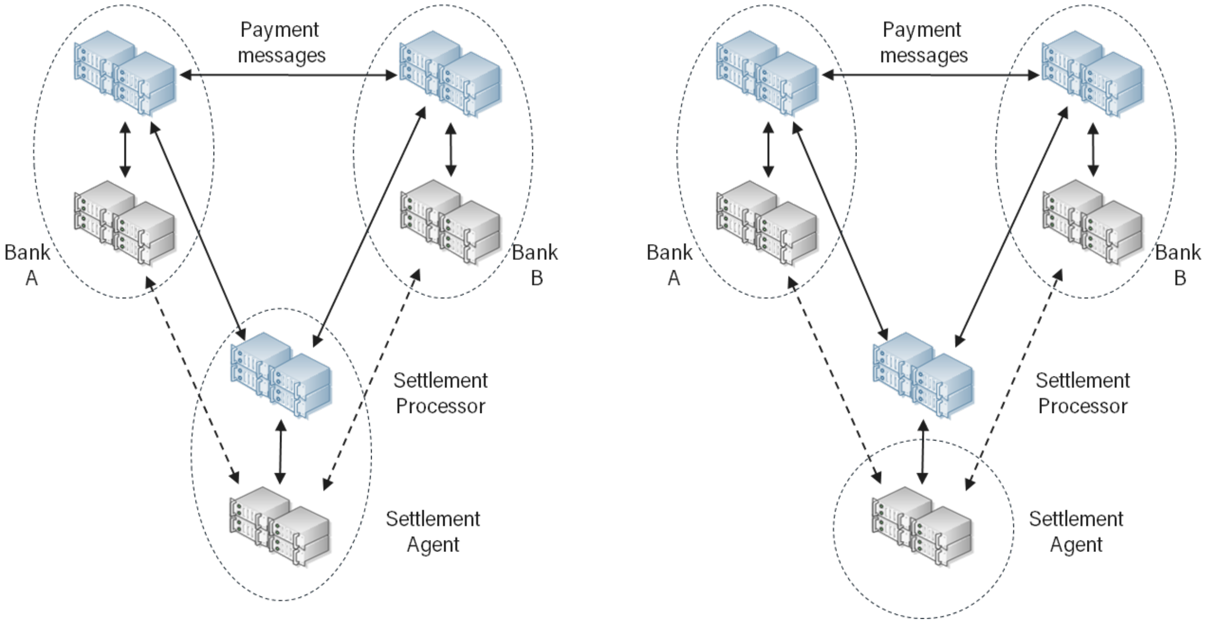


Figure 3 - Tereon's settlement message flow

If the providers operate on a bilateral correspondent basis and so use nostro/vostro correspondent settlement accounts to settle transactions between themselves, then Tereon can still use its message flow structure to control the ultimate settlement of funds between those two providers. Once the providers' correspondent settlement accounts exceed a pre-agreed limit, the providers will simply settle the funds that they hold on behalf of each other via the existing settlement system, or via the Tereon settlement system. Tereon can manage this process automatically.

The hybrid message structure has a further advantage. It allows Tereon to separate the payment message into various components, each of which is sent to the appropriate processors. Thus, just as the settlement element of a payment message is sent to the settlement processor, so information on the payment traffic can be sent to a third party to analyze for fraud or other suspicious patterns in real time.

Tereon message flow means that it can offer another mode of operation, and that is where it overlays its auditing, authorization, approval, clearing, and hypothecating functions over an existing DNS system. Essentially, Tereon would provide the end-to-end authentication service per an existing settlement system to give providers and their users certainty that all funds for eventual settlement have been secured, even though the actual underlying DNS cannot offer such security itself. The system rules will require the sending providers to hold their settlement funds in accounts to the order of and on behalf of the receiving providers, irrespective of whether or not the underlying DNS rules required any such security for those funds prior to actual settlement.

Tereon's message flow means that is can support a genuine RTGS system, it can support an RTGS-DNS hybrid system, it can support a secured-DNS system, it can support bilateral correspondent settlement, and it can overlay an existing DNS system to provide it with secured-DNS functionality. Not only does Tereon support these modes of operation, but it can also provide a migration path from a DNS system to a genuine RTGS system. There would be no need to amend any service running on Tereon as they would all see the same Tereon settlement system. That system could simply migrate over time to provide a genuine RTGS system once all the components, policies, and rules were in place to support that system. This provides a seamless migration path from current settlement system to a full function and ubiquitous real-time settlement without restrictive minimum transaction values.

As mentioned above, there is one use case where Tereon has to operate as a hybrid, and that is where a user (registered or otherwise) transfers finds to an unregistered recipient. The unregistered recipient will not, by definition, have a Tereon account (see answers to the questions in U.1 above), and so Tereon cannot settle the transferred funds to that recipient's account. Instead, Tereon settles the funds to a special remittance account (a class of control account), where the funds will sit until they are either accessed by the recipient or the transfer expires. Tereon will settle the funds into that control account in real-time, but there will be a lag until the recipient accesses those funds. Tereon holds the funds on behalf of the transferor until they are accessed by the recipient, at which point Tereon will hold those funds (if any remain) in the remittance account on behalf of the recipient. The use case on page 93 of the original proposal sets out the workflow of a transfer from a registered transferor to an unregistered recipient.

If the transfer expires and the transferor is a registered user, then the funds are returned to the transferor's account. If the transferor is an unregistered user, then Tereon will notify the transferor that the transfer has expired and ask the transferor to collect the funds from a Tereon-enabled merchant or another agent. The answer to question F.3 below set out the methods that Tereon will use to notify both the recipient and the transferor of the status of the transfer.

Please provide details on the settlement process in an environment where a central bank operates a Tereon server.

The above answer details the Tereon settlement in an environment irrespective of whether the settlement agent is a commercial organization or a central bank. The difference between those scenarios is that a central bank will be able to provide intraday credit liquidity with central bank money and the providers will settle transactions between themselves using central bank money. If a commercial operator acts as a settlement agent then it too may be able to seek liquidity from the central bank, but it will settle between the providers using commercial money, and extend to the relevant provider any intraday credit received from the central bank on a commercial basis as commercial bank money.

Our preferred solution is for the central bank to act as the settlement agent. The central bank will operate the settlement processor as well as the settlement accounts, or it can choose to require a third party to act as the settlement processor. This, ultimately, will be a decision made via consultation between the Federal Reserve and the FPTF.

E.6 Scalability and adaptability

Additional information

The answers to the following two questions will set out the additional information requested for this requirement.

Questions and answers

Please provide details regarding the Provider's hardware investment that is required to support the solution.

A provider's hardware investment will depend entirely on the volume of services that it intends to support and the number of users that it intends to provide the services to. In addition, it will depend on the costs that the provider's chosen hardware supplier charges for that hardware, and whether the hardware is purchase or leased.

From past experience, Kalypton has worked with a major financial services hardware provider to define three hardware configurations, including servers, storage systems, and networking infrastructure. These pre-set configurations ranged in price from $200,000 to $1,000,000 for each set. These configurations would enable each of the target providers to service its customer user-base, which ranged from hundreds of thousands to over 9 million per provider. Kalypton cannot disclose the manufacturer or the details of the actual hardware configurations due to considerations of confidentiality. However, Tereon is designed to operate on standard carrier-grade equipment, and it may prove to be the case that the provider already has the equipment necessary to operate Tereon. This is something that Kalypton and the provider will determine during the initial planning stages of the implementation project.

In the case of the hardware configurations referred to above, the settlement agent was to operate two of the top level configurations in its main location and in its disaster-recovery location, while each of the providers would choose which of the configurations to operates themselves in order to provide the services to their users. The settlement agent's configuration was over-engineered as it could easily cope with the predicted daily traffic. However, its over-specification also meant that it would easily cope with the rare, but massive throughput peaks that would occur at specific times in the year.

How will the volume thresholds that initiate scaling be defined?

Tereon defines four metrics that will determine when it will initiate automatic horizontal scaling (or contraction if it no longer requires the extra instances to process the work load). These four metrics are network load, CPU load, transaction volume, and system temperature.

Each of these metrics, including the transaction volume threshold will be defined based on the capabilities of the hardware that the provider chooses to use for the solution, and the anticipated throughput, both average and peak flows, that the provider expects within a twenty-four-hour period. A typical threshold would be an average CPU load of 50%, with a maximum individual instance core load of 60%, though some hardware configurations may support a higher loading. A typical network threshold would again be an average of 65% with a maximum defined individual network interface load of 70%. Kalypton and the provider will determine the exact loading of each of these metrics for the provider's chosen hardware and networking configuration during the testing phase of the solution implementation project.

Tereon has operated at far higher networking loads in initial tests, though it has yet to reach a CPU load of 60%. The network configuration was geared to high volume, low packet size transactions.

E.7 Exceptions and investigations handling

Additional information

The answers to the following four questions will set out the additional information requested for this requirement.

Questions and answers

When will the system rules be developed and available?

Please see Table 2, Legal Framework Approach/Structure, L.1, L.2, Governance Approach and Structure, G.1, G.2 and Figures 9-11. The time schedule for development and implementation of the Uniform Rules is ultimately dependent on an inclusive, industry wide process that is vender and product neutral and independent.

Will the solution support the use of alerts and notifications to support dispute resolution processes?

Yes. Tereon provides a messaging service that can be used to send alerts and notifications to support all aspects of its service. Supporting the dispute resolution process is simply one example of the use to which the messaging service will be put.

Will an existing framework be leveraged to inform the process to resolve exceptions/disputed transactions?

Yes. Tereon intends to leverage the existing ECCHO rules and procedure to inform the process to resolve exceptions and disputed transactions. Kalypton believes that exceptions or disputes that commonly occur with today's payments system will be extremely rare with Tereon as Tereon is a true real-time payments service, unlike most of the available systems today. Many exceptions that arise today simply cannot occur in Tereon. Nevertheless, the system rules will include effective and economic mechanisms to enable users and providers to resolve any exceptions or disputed payments that may occur, no matter how rarely.

Is there a plan to aggregate transaction data to monitor for suspicious patterns?

Yes. If the providers wish to aggregate transaction data to monitor for suspicious transactions, then they can certainly do so if it is lawful for them to do so. Tereon does not do so by default simply because in many jurisdictions, providers are forbidden from aggregating transaction data. However, Tereon can anonymize that data if required, and it can certainly aggregate that data to a monitoring service or share that data between providers. Tereon can provide the data as a real-time feed, aggregated and suitably anonymized, to enable an aggregator to use big data analytics to monitor the transaction traffic for suspicious patterns.

Tereon retains the flexibility to support whatever monitoring system the FPTF decides to require.

Safety & Security

S.1 Risk management

Additional information

The answers to question E.5 above set out how Tereon is designed to eliminate the settlement risks that can occur with deferred settlement. Tereon builds on the principles enunciated in the Lamfalussy Report and thereafter in the report *Real-Time Gross Settlement Systems* from the Bank for International Settlements (1997) to construct a payment and message flow model that eliminates settlement lag for all transactions. Where it cannot eliminate that lag, such as where Tereon has to operate as a DNS (Designated-time Net Settlement) system, it does so as an RTGS-DNS hybrid system or a secured-DNS system (often referred to as a Lamfalussy-plus system) to ensure that it secures the funds from a sending provider necessary to settle that provider's obligations to all other receiving providers.

Where Tereon has to operate over a standard DNS (Designated-time Net Settlement) system, it can provide the necessary message flow and functions to secure the funds from a sending provider necessary to settle that provider's obligations to all other receiving providers.

Tereon's message flow structure allows it to send details of the payment traffic in real-time to a third party aggregator (if this is legally allowed) to enable that party, and all providers to analyze the payment data traffic for fraud or other suspicions patterns.

Questions and answers

S.1.1: How will the solution address the unexpected application of a law or regulation?

Tereon is designed to accommodate changes to the law or regulation, regardless of whether those changes are expected or not. It addresses such unexpected application in two ways. The first is that the legal and risk management frameworks will be reviewed regularly; every six months is the minimum period that Kalypton would recommend to pass between full reviews of the frameworks. The frameworks themselves will be drafted in a way that allows for regular reviews and updates. This is already something that happens with the ECCHO rules and procedures framework that Kalypton will leverage for this solution (see answer to U.3 above).

The second is that Tereon's solution is extremely flexible and can be configured to apply new legal and regulatory requirements with the minimum of effort. Adding new fields to capture data for a payments process is easy to do, as is adding new contextual information to an existing payments process.

S.1.2: How will the solution identify and address any risks related to batch settlement?

As the answer to E.5 sets out, Tereon is designed to eliminate the settlement risks associated with batch settlement systems. Batch systems are based on a historic design that was limited by the capabilities of the technical systems of the day. The BIS report makes clear that central banks in major jurisdictions are now seeking to move from batched or DNS systems to RTGS systems as these remove both settlement risks and the systemic risks that occur when one provider fails.

Our recommendation is that the solution should move to an RTGS system as only an RTGS can support a real-time payments system required under the Faster Payments Effectiveness Criteria.

S.1.6: How frequently will the solutions risk management framework be reviewed?

Kalypton recommends that the risk management is reviewed at least every six months, with extraordinary reviews held when unexpected changes occur to the legal or regulatory environment within which the solution will operate.

S.2 Payer authorization

Additional information

The answer to the following question will set out the additional information requested for this requirement.

Questions and answers

S.2.3: Please provide more details related to the initiation, modification, and clearing of preauthorized payments.

Tereon allows users to preauthorize payments, as set out on pages 38 to 40 of the original proposal. Either the payer or the payee can initiate a preauthorized payment. The preauthorization either refers to the payer electing to automate authorization for low-value transaction, or to payments at some date in the future that the payer or payee have initiated, and the payer authorizes in advance. The actual approval, clearing, and settlement will take place when the actual payment is made, and not before that point in time. Whether Tereon hypothecates funds to the payer provider's account with the settlement agent will depend on whether the settlement agent provides an RTGS system (in which case no hypothecation occurs) or whether the settlement agents provides an RTGS-DNS hybrid system or a secured-DNS system (in which case the provider's Tereon system will hypothecate funds if necessary to the provider's account with the settlement agent. The answer to E.5 above sets out the settlement process and when Tereon hypothecates funds to a provider's account with a settlement agent.)

The payer can initiate a preauthorized payment in a number or ways, depending on what the payer requires. If the preauthorization is for a payment process, such as a small value transaction using an NFC-enabled device for which the payer does not want to enter a PIN each time he transacts, then so long as the payer's provider supports such a choice, then the payer enters his account settings, and sets the transaction type, and spending limits. For example, PIN-less payments at a metro system gate for $10 or less per transaction, to a daily cumulative total of $20, a weekly cumulative total of $50, and an absolute cumulative total of $250. (These types of transactions will usually be for small values in order to limit the potential risk of someone other than the user obtaining the user's device and using that device to make similar transactions. Of course, that third party would not be able to make any normal transaction that required authorization as part of the transaction process, and the device would only operate until the authorized user cancels or blocks the device.)

Every time the payer uses his device for a preauthorized transaction type (such as at the metro gate), the provider's system will check that the transaction comes within the set parameters:

- If the transaction comes within the set parameters then Tereon will proceed as if the payer had authorized the transaction, and proceed through the remaining approval, clearing and settlement stages. The identification stage will have occurred automatically when the payer used his device at the metro gate.
- If the transaction falls outside the set parameters, such as where the daily cumulative total would exceed $20, then Tereon will require the payer to authorize that transaction before it proceeds through the remaining approval, clearing and settlement stages. Again, the identification stage will have occurred automatically when the payer used his device at the metro gate.

(One example might be the use case on page 72 of the original proposal, if the value of the transaction was small enough and the payer had configured his system to preauthorize that class of transaction for that value or less.)

With this class of preauthorized payments, the preauthorization simply refers to the fact that the user has elected to bypass the need to enter his or her authorization in a small-value transaction. All other aspects of a transaction will proceed as before.

The payer can also preauthorize a merchant payment or a transfer to a recipient. Here the payer will elect to pay a bill or make a transfer at a certain date, and will use a mobile application or the user's account portal to set up the details of the payment. The user will set the time and date of actual payment and will authorize that payment by entering his or her PIN at the time that the payer set up that payment. In some cases, the user may elect to configure his or her account to set aside the funds to cover that payment immediately. This is a form of hypothecation, whereby the payer's account will hold the required funds to one side to ensure that the funds are available to make the payment at the time and date set for that payment.

For example, imagine that a user decides to arrange a transfer of $100 to her friend as a birthday present in 10 days' time. She configures the details in her mobile application, and selected the option to set a date and time for that transfer. She selects 1am on her friend's birthday, and then enters her PIN to confirm. As she has configured her account to set funds aside for preauthorized payments, her account sets the $100 dollars aside. Before setting the transfer, the transferor had $500 in her Tereon account. If she were to examine her account again, she would see that she had $500 in her account, but that she only had $400 available to spend. Tereon has reserved the $100 for the transfer in 10 days' time. Unless the transferor cancels or amends the details of the transfer, for example increasing or decreasing the amount to transfer, or changing the time (not the date in this case) of the transfer, Tereon will process the transfer at 1am on the recipient's birthday. The transferor has already identified the recipient, and had authenticated herself when she configured the transfer. She preauthorized the transfer when she configured it, and so Tereon simply carries out the remaining steps of the transaction in real-time. The user's provider approves the transfer as the user's account reserved the $100, and the provider's Tereon systems clears the settles the transfer.

The user could just as easily configure her account to preauthorize a bill to a commercial recipient, such as a plumber, or whatever, where she sets the payment day as the due date on the bill or invoice that she receives. See, for example, the use case on page 60 of the original proposal where a B2B ad hoc payment is preauthorized in this manner.

A payee can initiate a preauthorized payment. Here the payee would set a date and time for payment when he requests payment from the payer. For example, imagine that a plumber wishes to bill his client, the payer, $125.95 for some work. He enters the amount into his application, and then sets a date and time by which he would like to be paid (14 days from the date of the request). He submits the request to pay to the payer, who approves the request and enters his PIN to authorize the payment (the use case on page 72 of the original proposal sets out an example workflow of a consumer to merchant payment). If the payer accepts the request by entering his PIN, then Tereon will configure the payer's account to make the payment on the due date. If the payer has configured his account to set funds aside for preauthorized payments, then his account will set aside the $125.95 for the payment. If the payer does not have sufficient funds to make the payment, the Tereon will notify him of that fact when he is asked to accept the payment request. He can either decline the payment request, or he can accept the request and then add funds to his account by the due date in order to make the payment. If the user has sufficient funds in his account to make the payment, then on the due date Tereon will approve, clear, and settle the payment. If he does not have the funds then Tereon will not make the payment, and will inform the payee via its internal notification and messaging system that the payer has not made the payment.

S.3 Payment finality

Additional information

Questions and answers

When will payment system rules, including a dispute process, be available?

Please see Table 2, Legal Framework Approach/Structure, L.1, L.2, Governance Approach and Structure, G.1, G.2 and Figures 4-11. The time schedule for development and implementation of the Uniform Rules is ultimately dependent on an inclusive, industry wide process that is vender and product neutral and independent.

S.4 Settlement approach

Additional information

To clarify a point made in the original proposal. the solution requires payers to have sufficient funds or credit to support a transaction.

Tereon is not predicated on accepting the constraints on the current settlement environment. To design a solution that was limited by the constraints on the current settlement environment would go against the drive by central banks to move from a DNS (Designated-time Net Settlement) system, to an RTGS system, as documented in the report *Real-Time Gross Settlement Systems* from the Bank for International Settlements (1997). The Faster Payments Effectiveness Criteria makes it clear that the Federal Reserve and the Faster Payments Task Force envisage a real-time payments system, which by definition will require a genuine RTGS system to manage the settlement of the transactions.

The answer to question E.5 above sets out Tereon's approach to settlement, including the timings for the settlement of funds. As the answer explains, Tereon can overlay across existing DNS (Designated-time Net Settlement) systems to provide them with the functionality of a secured-DNS system. However, that is not the optimal solution, due the potential need to provide intraday credit or liquidity to prevent delays in processing payments – a real-time payments system must not incur delays in processing transaction or else it will fail to be a genuine real-time payments system. If necessary, Tereon can start off by overlaying on an existing DNS system, and provide a migration path to become a true RTGS system. Tereon is certainly not limited by the constraints on the current settlement environment.

Please see previous questions regarding settlement approach.

Please see answer to question E.5 above.

S.5 Handling disputed payments

Please see previous questions related to availability of legal framework, payment system rules and creation of a dispute process.

Please see Legal Framework Approach/Structure, L.1, L.2, Governance Approach and Structure, G.1, G.2 and Figures 4-11. There are potentially three levels of processes to dispute payments; 1) bank to bank disputes under the Uniform Rules, 2) financial institution to customer disputes under the Financial Institution Agreements and 3) financial institution to provider under the Provider Agreements.

S.6 Fraud information sharing

Additional information

To clarify a point Kalypton makes in the original proposal, Tereon does not require the sharing of transaction information to support fraud monitoring and management as that is, legally, the responsibility of each individual provider. However, Tereon is certainly able to share that information, and can do so in real-time, supplying a suitably structured data feed into a big data analytical tool to enable the recipients to analyze that data as required.

Tereon does not prevent sharing of transactional information. It just does not impose that function as it may be unlawful to do so in many jurisdictions.

Questions and answers

Can the solution support the monitoring and sharing of fraud information in real time?

Yes. Tereon supports the monitoring and sharing of fraud information in real-time. The structure of Tereon's payment and settlement message flow, together with its ability to generate a full audit of every transaction in real-time, enables Tereon to monitor and share transaction information.

Tereon can format and shape the transaction information so that its sharing does not contravene and privacy or competition regulations. It can feed that data both to the individual providers and to any number of third parties if necessary. The providers and the third parties can use big data tools and analyze that information.

As an example, Kalypton notes that Early Warning is owned by seven banks representing some 60% of retail bank accounts in the US and offering an important path to ubiquity. Early Warning already offers various fraud alert services including its “Account Threat Detection & Behavioral Biometric solution”.

Building upon the inherent capabilities of Tereon, it would be relatively simple to enhance the scope and value added of these services to Early Warning’s subscribers and shareholders by –

- eliminating at source the risk of late detection of issues
- extending the risks covered by their solution, as Tereon can provide contextual information around a transaction, such as the location of the parties and the clients they are using, as well as the transaction data itself
- enriching the information base for further analysis by additional data tools and solutions; and
- generally reducing the costs of doing business by providing a data feed in real-time that can be analyzed to detect issues as they occur.

No doubt similar value could be added to other fraud management solutions and services in the market place.

Tereon is able to shape the audit and transaction information to any required data format (see answer to U.4 above) and so can feed the date into any number of well-known fraud management tools.

Tereon does not just provide the data required to monitor and manage fraud. It also provides the tools to combat fraud. Administrators, when lawfully authorized to do so, can access the full transaction history of users to investigate those transactions further. They can block transactions or users in real-time, they can suspend and block providers in real-time. The Tereon directory look-up service provides the tools and means to do so as Tereon’s security model provides the tools to control access to the service at a granular level.

Please see previous questions related to fraud information sharing.

Please see the answer above.

S.7 Security controls

Please see previous questions regarding the availability of the legal framework.

Please see Legal Framework Approach/Structure, L.1, L.2, Governance Approach and Structure, G.1, G.2 and Figures 4-11. The time schedule for development and implementation of the Uniform Rules is ultimately dependent on an inclusive, industry wide process that is vender and product neutral and independent.

S.8 Resiliency

Please provide target availability metrics for each Provider and for the solution as a whole.

The target availability for the solution as a whole for each provider is 99.95% for each individual component (such as a server, instance, etc.), with 100% for the service as a whole. Though individual components will fail, multiple redundancy and the ability to start up replacement instances to replace any failures means that the system should provide 100% uptime overall.

One of the hardware vendors that Kalypton can work with has managed to achieve 100% uptime for a public sector network by using similar techniques to those that Kalypton will use. Its development team is well versed in achieving such metrics.

How will the solution ensure a consistent end user experience across providers in terms of uptime and transaction speed?

Please see answer above. Each implementation, and each provider, will have the same availability metrics and the same automated configuration to ensure that it meets those metrics.

How will Provider availability be monitored?

Tereon is self-monitoring, and will provide each provider with all of the tools necessary to monitor the uptime of individual components and the solution as a whole. Though Tereon will automatically start up replacement instances or components to replace any failures, providers are free to do so themselves manually as well.

S.9 End-user data protection

No questions

S.10 End-user provider authentication

No questions

S.11 Participation

When will the participation agreement/participation rules be available for review?

There are three agreements/rules needed to affect participation; The Uniform Rules, the Provider Agreements and the Financial Institution Agreements. For the availability of the Uniform Rules, please see E.7, S.3, S.5, S.7, Legal Framework Approach/Structure, L.1, L.2, Governance Approach and Structure, G.1, G.2 and figures 4 to 11. For the availability of Financial Institutions Agreements, each is dependent on the financial institution that offers the service.

For the availability of the Provider Agreement, Kalypton has a standard user license that needs to be tailored to US law and which can be shared with the FPTF as a straw man for the standard Financial Institution Agreement once the preliminary rules and agreements have been drafted (Table 2 in E.3 above sets out the timelines for this process) in order to ensure that the rules are referenced correctly in

the agreement. Kalypton is acutely aware that any standard agreement must facilitate a choice of technology vendor who can meet the service requirements.

Speed

F.1 Fast approval

No questions

F.2 Fast clearing

No questions

F.3 Fast availability of good funds

Additional information

The 30-day limit mentioned in the original proposal document is simply an example, and illustrates the fact that the transferor can place a limit on the time period that the unregistered recipient has to first access the transferred funds. A transferor can, of course, remove any time limit, but this could leave the funds in limbo if the recipient loses the transaction number and the collection PIN for those funds. By imposing a time limit, the transferor knows that he or she will receive the unclaimed funds if the recipient fails to access them. The transferor can always make a new transfer, which will generate a new transaction number and collection PIN. The transferor can also choose to configure a different time limit, so long as that limit falls within the time periods allowed by the transferor’s provider.

Questions and answers

Please describe how the payer and payee are notified regarding the unclaimed payment.

Tereon will notify the transferor (payer) via its internal notifications and messaging services if the recipient (payee) has failed to claim his funds. Tereon can also use alternative communication channels such as an SMS message or an email message, if the payer has authorized Tereon to use those channels via his account settings. The user can configure Tereon to provide a warning within a time period before the transfer expires (say a week), so that the transferor can try to communicate with the recipient to enquire why the recipient has failed to collect the funds.

In the same way, Tereon can be configured to send the recipient a reminder to collect his funds within a time period before the transfer expires, and daily thereafter, until the transfer expires or the recipient has accessed the funds. When the transferor identifies the unregistered recipient, he can provide either a mobile telephone number or an email address (he can, of course provide both) for the recipient. Tereon will use these to send the recipient an SMS or an email to remind the recipient to collect the funds.

If both the transferor and recipient are unregistered (this is one of the 31 use cases that Tereon supports), then the transferor must provide his mobile number or email address when he identifies himself to Tereon before he can make a transfer to the unregistered recipient (he must, of course, also identify the recipient and provide the recipient's mobile number or email address). Tereon will use these contact details to inform both sides of the transaction that the funds have yet to be collected.

Is there an alternative option for non-Tereon users to access funds without opening a Tereon account?

To clarify a point Kalypton makes in the original proposal, and which it states in its answer to U.1 above, non-Tereon users do not need to open a Tereon account to access their funds. Tereon provided non-Tereon users who have had a transfer made to them an opportunity to open accounts if they wish to do so. However, there is absolutely no obligation to open an account to receive the funds.

F.4 Fast settlement

Additional Information

The answers to the following two questions will set out the additional information requested for this requirement.

Questions and answers

Is there any intention to require real time settlement if this capability is available in the market?

Yes, if the capabilities of any available RTGS do not match the requirements necessary to support a real-time payments system. Many existing RTGS systems can, in some cases, impose delays and queue transactions for processing due to their internal designs and the intraday liquidity issues that they impose on participants when those participants use the RTGS system for sudden, very high-value transactions. Tereon's RTGS system is designed to support payments of any value large or small, and does not impose any queuing requirement. By recommending that the central bank act as the settlement agent (see answers to E.5 above), the RTGS will avoid the need for queuing and the delays in processing a transaction that this may involve. The central bank can provide automated intraday credit using a service modelled on Fedwire that will obviate any queuing and so support fully a set of genuine real-time payments services.

How will the availability of real time settlement impact credit and liquidity risk exposure for Providers?

The question presupposes that Tereon will operate as a standard DNS (Designated-time Net Settlement) system. Tereon does not do this for the reasons set out in the answer to question E.5 above. It operates as an RTGS system, as an RTGS-DNS hybrid system, or as a secured-DNS system. The availability of real-time settlement can eliminate the credit and liquidity risk exposure for providers. The report *Real-Time Gross Settlement Systems* from the Bank for International Settlements (1997) makes it clear that if they are designed correctly –

> "RTGS systems can contribute substantially to limiting payment system risks. With their continuous intraday final transfer capability, RTGS systems are able to minimize or even eliminate the basic interbank risks in the settlement process.

> More specifically, RTGS can substantially reduce the duration of credit and liquidity exposures. To the extent that sufficient covering funds are available at the time of processing, settlement lags will approach zero and so the primary source of risks in intrabank funds transfers can be eliminated. Once settlement is effected, the receiving bank can credit the funds to its customers, use them for its own settlement purposes in other settlement systems or used them in exchange for assets immediately without facing the risk of the funds being revoked."

This is the very reason why Tereon's default settlement mode is to operate as an RTGS system. The same holds true for a correctly designed RTGS-DNS hybrid system or a secured-DNS system, which is why Tereon supports these modes as well.

F.5 Prompt visibility of payment status

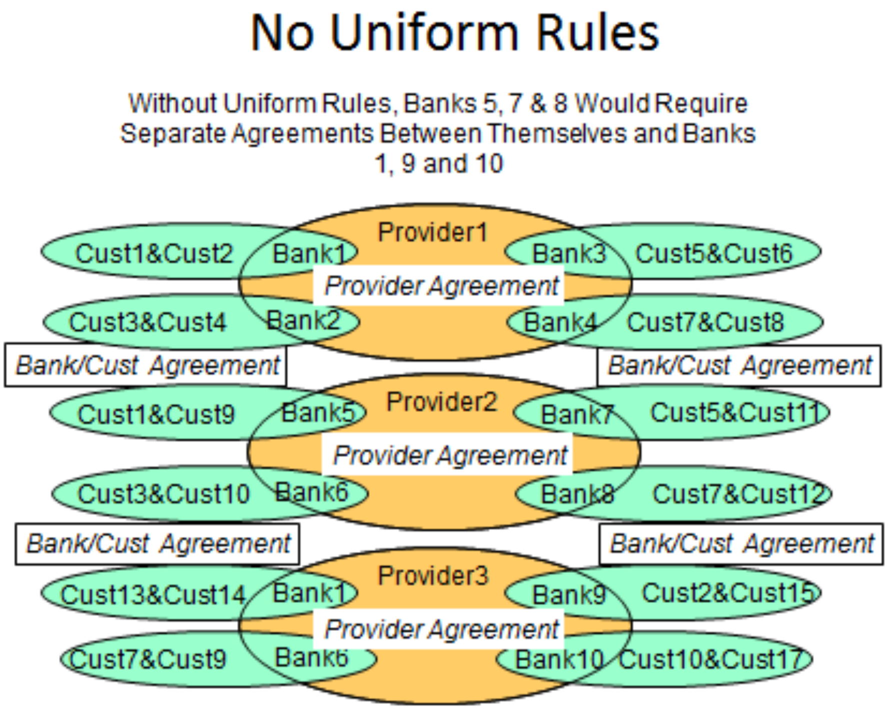
No questions

Legal

Legal Framework Approach/ Structure

Given that there is no existing, comprehensive statutory or regulatory law that addresses real-time payments in the U.S., quality agreements among all the parties with an interest in the payment system are critical. The approach to the legal framework assumes that the optimal solution to this void in payments law is a universal set of rules that will apply to all users and providers in a multiple provider/multiple bank environment. A universal set of rules will be provider and product/service independent and will therefore provide uniform rules (Uniform Rules) that will allocate liabilities consistently among the parties using and or providing all solutions.

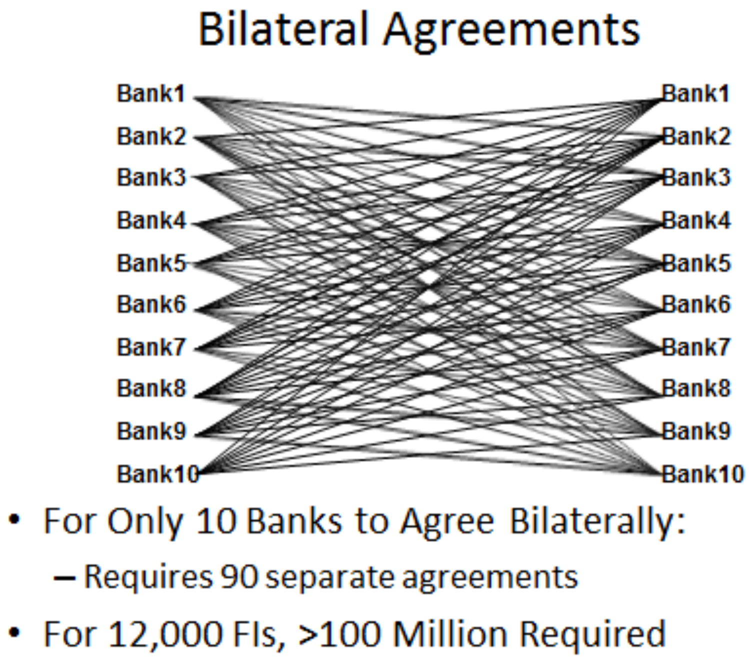
Without Uniform Rules, financial institutions require separate agreements making ubiquity and rapid adoption of real time payments virtually impossible.


No Uniform Rules

Without Uniform Rules, Banks 5, 7 & 8 Would Require Separate Agreements Between Themselves and Banks 1, 9 and 10

Figure 4 - Real-time payment system without uniform rules

While bilateral agreements are reasonable between key payments partners, it is not viable for the nation's 12,000 financial institutions to have bilateral agreements with every other financial institution. When you consider the number of bilateral agreements that would have to be created, it becomes unwieldy, even with just a very few financial institutions. Figure 5 below, a spider's web of a diagram, emphasizes the potential for quickly creating a convoluted environment. It was precisely this problem, the need for hundreds of millions of agreements, that required the Check Clearing for the Twenty-First Century Act (Check 21) which created federal law to allow paper check truncation through the unilateral decision of each financial institution and thus eliminated the need for every party with an interest in the check to agree to the truncation of the original paper check.



Bilateral Agreements

- For Only 10 Banks to Agree Bilaterally:
  - Requires 90 separate agreements
- For 12,000 FIs, >100 Million Required

Figure 5 - Real-time payment system with only bilateral agreements

Advantages to uniform rules

Uniform Rules provide many advantages—not just providing a simpler legal agreement environment. The advantages of this approach are numerous and include but are not limited to:

- Minimize the risk associated with expensive litigation to resolve disputes by assigning liabilities among the various parties in advance of any disputes,
- Minimize the risk of uncertainty of dispute resolution by providing consistent, uniform guidelines to the courts adjudicating disputes based on agreements under which the parties were using/providing the payments,
- Uniformly define real-time payments for all solutions,
- Minimize the number of agreements needed to achieve ubiquity while maximizing uniform coverage through one common, uniform, multiparty agreement,
- Minimize bias for one or more solution providers through the application of a common, uniform, multiparty agreement that includes provisions for all solutions and disadvantages none,

- Allow each solution provider to have its own agreements with its customer/users to prescribe the provisions that are unique to its products/services and that are not addressed in the Uniform Rules,
- Allow each financial institution to have its own agreements with its customers/users to prescribe the provisions that are unique to its products/services, and
- Focus the development and maintenance of evolving, detailed, universal legal provisions on a relatively small number of payments experts, while freeing key resources within provider and financial institution organizations to focus on their products and services that create value and make them unique.

Three Types of Agreements Required

The approach to the legal framework also assumes that three types of agreements are needed to achieve consistent, uniform predictable legal coverage with the flexibility to encourage financial institutions and solution providers to implement real-time payments. These three include:

1. **Uniform Rules** - Described above. The primary purpose of Uniform Rules is to define the obligations of financial institutions, allocate liabilities among the various parties, define exclusions not addressed in the Uniform Rules, reference the appropriate standards to be used, address errors, develop dispute resolution approaches between the financial institutions, and address payment finality and settlement.

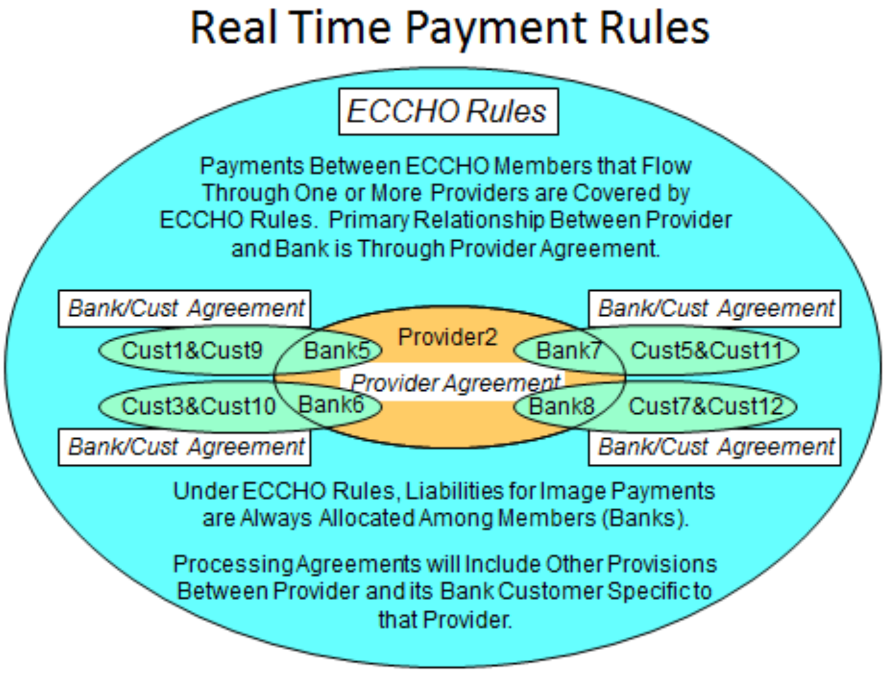

Real Time Payment Rules
ECCHO Rules
Payments Between ECCHO Members that Flow Through One or More Providers are Covered by ECCHO Rules. Primary Relationship Between Provider and Bank is Through Provider Agreement.
Bank/Cust Agreement
Cust1&Cust9
Bank5
Provider2
Bank7
Cust5&Cust11
Bank/Cust Agreement
Provider Agreement
Cust3&Cust10
Bank6
Bank8
Cust7&Cust12
Bank/Cust Agreement
Bank/Cust Agreement
Under ECCHO Rules, Liabilities for Image Payments are Always Allocated Among Members (Banks).
Processing Agreements will Include Other Provisions Between Provider and its Bank Customer Specific to that Provider.

Figure 6 - Uniform rules, bank agreements, and provider agreements

2. **Provider Agreements** – Provider agreements are needed to define the relationship between the solution provider and its customers. These agreements would typically include definitions

of the service(s) provided/offered by the provider to its customer, service pricing provisions, logistical provisions between the provider and the customer, definition of settlement method, obligations of provider and financial institution, etc. Additional provisions should include:

a. Authentication of entities and payments/messages;

b. Initiation of payment orders/authentication and termination of authorization;

c. Delayed or failed payments;

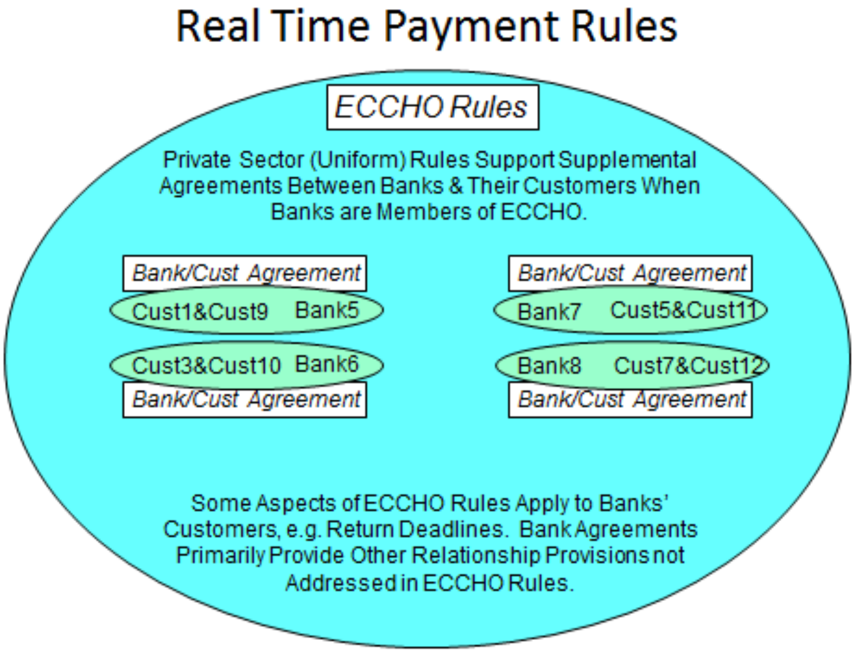
d. Timing of sending and receipt of payment;

e. Error resolution with the financial institution;

f. Timing of sending and receipt of payment; and

g. Performance standards that the financial institution should expect.

Provider agreements would not change or override provisions in the Uniform Rules but rather would supplement and complement the Uniform Rules with provisions that are unique or specific to that particular provider/customer relationship. The Uniform Rules would avoid, wherever possible, inserting itself between the provider and its customer.



Real Time Payment Rules

Private Sector (Uniform) Rules Support Supplemental Agreements Between Banks & Their Customers When Banks are Members of ECCHO.

Some Aspects of ECCHO Rules Apply to Banks' Customers, e.g. Return Deadlines. Bank Agreements Primarily Provide Other Relationship Provisions not Addressed in ECCHO Rules.

Figure 7 - Uniform rules and financial institution agreements

3. **Financial Institution Agreements** – Financial institution agreements are needed to define the relationship between the financial institution and its customers. Figure 7 above illustrates this relationship. These agreements would typically include definitions of the service(s) provided/offered by the financial institution to its customer, service pricing provisions, logistical provisions between the financial institution and its customer, right of offset

provisions, dispute resolution processes, customer notification processes, etc. Additional provisions should include:

a. Customer responsibilities;

b. Financial institution responsibilities; and

c. Processes and timing to resolve disputes, errors and customer cancelations of payments.

Financial institution agreements would not change or override provisions in the Uniform Rules but rather would supplement and complement the Uniform Rules with provisions that are unique or specific to that particular financial institution/customer relationship. The Uniform Rules would avoid wherever possible inserting itself between the financial institution and its customer.

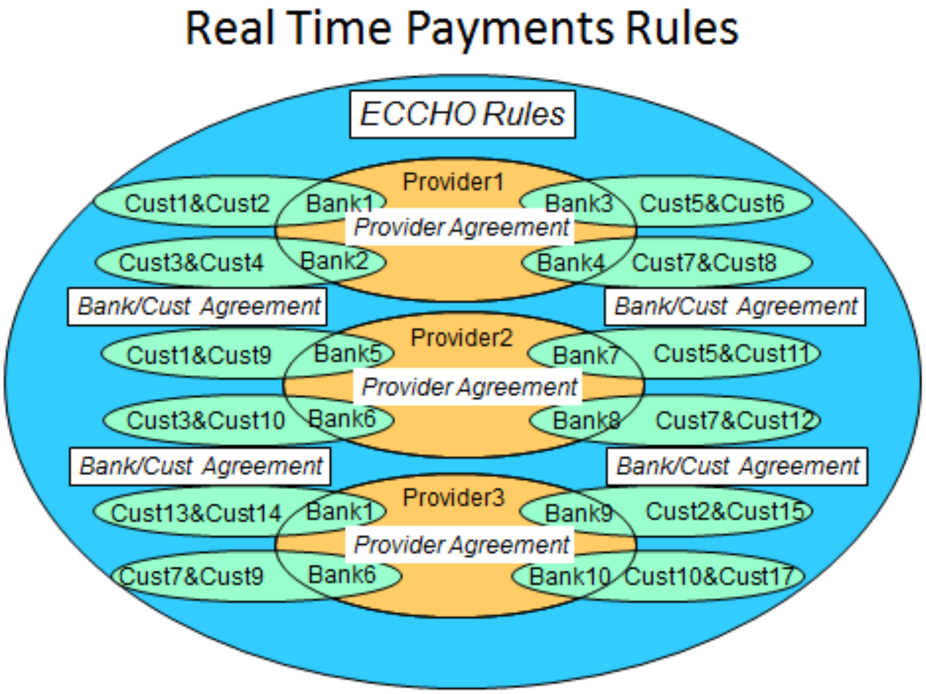


Figure 8 - Uniform rules with universal coverage

Under Uniform Rules, the allocation of liabilities is always between ECCHO members, regardless of the number of intermediary providers. Therefore, financial institutions can have as many provider relationships as needed.

Uniform Rules vs. Agreements

Not every legal provision needs to be addressed in the Uniform Rules. Some provisions are best addressed in the financial institution's agreements with its customers; financial institutions may want the flexibility to meet their regulatory/examination requirements differently than do their competitors.

The Uniform Rules would not seek to prescribe internal bank procedures nor internal solution provider procedures. The primary relationship between the financial institution and its customers would continue to be the financial institution and not the Uniform Rules. Likewise, the primary relationship between the solution providers and their customers would continue to be the solution providers. Determination of which provisions are best addressed in the Uniform Rules and which are best addressed in provider agreements and/or financial institution agreements will be decided in discussions within the Subcommittees, RTP Committee, and ultimately by the governance decision structure addressed below under Governance. Figure 8 above illustrates this structure.

The approach to the Legal Framework also assumes that a universal governance process is implemented to approve the Uniform Rules, and that the governance process must be vender/provider independent. Under this assumption, specific rules cannot be developed and implemented until the governance structure and processes have been implemented. The recommended governance approach is addressed later in this narrative under Governance. At the time of this writing, the Faster Payments Task Force is currently still discussing governance considerations.

Questions and answers

L.1: Please provide more details regarding the Legal Framework that will govern the Solution's operation and/or impose any compliance obligations on the Solution or End Users. In doing so, please specifically address how the Solution supports the five Legal Framework subcriteria.

Please see Legal Framework Approach/Structure above for the relationship between Uniform Rules, provider agreements and financial institution agreements--all of which are needed to optimize the legal framework. Please refer to the narrative and to figures 4 to 11. that graphically show that ECCHO will base the development of the Real Time Payments Legal framework on its existing process that has been successful for more than twenty-five years. That approach maximizes the value of Uniform Rules for application across all financial institutions, providers and users. It also maximizes the flexibility of financial institutions and providers to provide common as well as unique products and services to their customers without requiring changes to the Uniform Rules and without changing the underlying obligations designated in the Uniform Rules. This allows the providers and/or financial institutions to distinguish their services from other providers and/or financial institutions and thus foster competition, which also benefits both consumer and business customers. The success of the image implementation in the U.S. reflects the value of this approach, transitioning from 100% paper check clearing to virtually 100% electronic image clearing in only six years.

L.1.1 – Please see Legal Framework Approach/Structure and Governance and figures 9 to 11 that show the active participation of stakeholders in the analysis, development, and modification of the Uniform Rules initially through the various Subcommittees followed by direct input to the Real Time Payments (RTP) Committee where the final vetting takes place prior to recommendations to the ECCHO Board of Directors.

L.1.2 – Please see Legal Framework Approach/Structure narrative and to figures 4 to 11. Although this approach to rules making is more difficult than one entity unilaterally creating the rules, it is far superior in the end. The resulting rules will have been agreed to by many individuals representing many financial organizations and solution providers. The rules will be as fair as possible to all participants. Consequently, the ability to achieve ubiquity becomes more likely since a broad base of financial institutions and solution providers will have bought into and in fact, contributed to the development of the Uniform Rules. This is evidenced through the fact that ECCHO has achieved 3,000 image exchange members with no other private sector competition.

L.1.3 – Please see Legal Framework Approach/Structure narrative and to figures 4 to 11. The Uniform Rules would focus primarily on the responsibilities of the financial institutions. Financial institutions would then select their providers and create agreements with those providers and through those agreements determine how the financial institutions would meet their obligations under statutory law, regulatory provisions, litigation and Uniform Rules. Financial institutions would also create agreements with their customers and through those agreements determine how the financial institutions would meet their obligations under statutory law, regulatory provisions, litigation, Faster Payments Effectiveness Criteria and Uniform Rules. The Uniform Rules would bind the financial institutions and the financial institutions would bind their providers and customers as appropriate. Figures 6 to 8 show the scope of rules coverage. It begins with the financial institutions that are members of ECCHO. Under the Rules, financial institutions have supplemental agreements with their customers to provide provisions not needed or not desired in the Uniform Rules but needed between the financial institutions and their customers. Additionally, Figures 6 to 8 show that Provider Agreements also supplement the ECCHO Rules.

Figure 4 shows the problem created in the absence of a Uniform Set of Rules. For example: Banks 5, 7 and 8 use the same provider for various services while Banks 1, 9 and 10 use a different provider with different provider agreements. Without a common agreement (Uniform Rules) Banks 5, 7, and 8 cannot exchange payments with Banks 1, 9, and 10 without some other agreements in place. Bank 6 uses both providers and therefore could participate in payment exchanges with all banks.

Figure 5 shows the problems created when bilateral agreements are needed between each of the participating banks. The graphic shows that when only ten banks are exchanging with each other, 90 bilateral agreements are needed. Uniform Rules provide a single set of multi-lateral agreements in lieu of many, many bilateral agreements.

L.1.4 – Please see the Legal Framework Approach/Structure narrative, the response to L.1 and to figures 9 to 11. In the Governance section below.

L.1.5 – Please see the Legal Framework Approach/Structure narrative, the response to L.1 and to figures 9 to 11 in the Governance section below.

L.2 Payment system rules

L.2: Please provide more details regarding the Payment System Rules, including requirements, standards/protocols and procedures that govern the rights and obligations of all End Users, Providers, Payers and Payees. In doing so, please specifically address how the Solution supports the five Payment System Rules subcriteria.

L.2.1.1 – Including responses to L.2.1.1 – L.2.1.9 – Each of these criterion would be addressed through the Uniform Rules process described in Legal Framework Approach/Structure above and through the provider and bank agreements described in the response to L.1 above including the responses to L.1.1 – L.1.5.

L.2.2 – Please see Governance Approach and Structure narrative and figures below for governance questions. For questions about stakeholder participation please see Legal Framework Approach/Structure, the responses to L.1. L.1.1 – L.1.5 and to figures 9 to 11.

L.2.3 –Please see Governance Approach and Structure narrative and figures below.

L.2.4 – The Uniform Rules would designate the financial institution that is responsible for obtaining and maintaining the payer’s authorization, and the agreements between the financial institution and its solution provider(s) would designate the mechanics of how that authorization would be obtained and maintained. This would allow maximum flexibility to incorporate the best practices as those practices evolve and mature without the need to modify the Uniform Rules. This would allow the providers and/or financial institutions to distinguish their services from other providers and/or financial institutions and thus foster competition which would also benefit consumers.

L.2.5 – The Uniform Rules would designate the financial institution that is responsible for resolving payment errors and any required timeframes for resolving those errors. The specific process for resolving those errors would be determined by the financial institution through its customer agreement and its solution provider agreement. The Uniform Rules would not seek to designate the specific processes to meet the financial institution’s obligations under the Uniform Rules. This would allow maximum flexibility for the resolution processes to evolve as improved methods develop without the need to modify Uniform Rules. This would allow the providers and/or financial institutions to distinguish their services from other providers and/or financial institutions and thus foster competition which would also benefit customers.

L.3 Consumer protections

L.3: Please provide more details regarding consumer protections, including a Legal Framework and procedures that allocate legal and financial responsibility and support Error Resolution. In doing so, please specifically address how the Solution supports the three consumer protections subcriteria.

Please see the Legal Framework Approach/Structure and the response to L.1. The Uniform Rules would designate the responsibilities of each of the financial institutions in the payments process including those responsibilities listed in L.3. The financial institutions have the flexibility to determine how they meet those responsibilities and those decisions would be reflected primarily in their agreements with their solution providers, if any, and their agreements with their customers. This would allow maximum flexibility to incorporate the best practices as those practices evolve and mature without the need to modify the Uniform Rules. This would allow the providers and/or financial institutions to distinguish their services from other providers and/or financial institutions and thus foster competition which would also benefit consumers.

L.3.1 – Please see the response to L3, the Legal Framework Approach/Structure and the response to L.1. The Uniform Rules would designate the responsibilities of each of the financial institutions in the payments process including the allocation of legal and financial responsibility for unauthorized, fraudulent or erroneous consumer payments. The financial institutions have the flexibility to determine how they meet those responsibilities and those decisions would be reflected primarily in their agreements with their solution providers, if any, and their agreements with their customers.

L.3.2 – Please see the response to L.3, Legal Framework Approach/Structure and the response to L.1. The Uniform Rules would designate the responsibilities of each of the financial institutions in the payments process including the error resolution of consumer claims arising from payments fraud and unauthorized payments. The financial institutions have the flexibility to determine how they meet those responsibilities and those decisions would be reflected primarily in their agreements with their solution providers, if any, and their agreements with their customers.

L.3.3 – Please see the response to L.3, the Legal Framework Approach/Structure and the response to L.1. Should solution providers and/or financial institutions determine to provide consumer protections beyond those required by law, they would have the flexibility to do so without changing the Uniform Rules.

L.4 Data privacy

L.4: Please provide more details regarding data privacy, including an approach to identify whether and how payment and related information can be collected and disclosed, consistent with applicable policy, law, and End User preference, and an approach, consistent with law, to secure information that should not be disclosed. In doing so, please specifically address how the Solution supports the five data privacy subcriteria.

The Uniform Rules will designate the responsibilities of each of the financial institutions in the payments process including those responsibilities listed in L.4. The financial institutions have the flexibility to determine how they meet those responsibilities and those decisions would be reflected primarily in their agreements with their solution providers, if any, and their agreements with their customers. This would allow maximum flexibility to incorporate the best practices as those practices evolve and mature without the need to modify the Uniform Rules. This will allow the providers and/or financial institutions to distinguish their services from other providers and/or financial institutions and thus foster competition which would also benefit consumers.

L.4.1 **–** Please see the Legal Framework Approach/Structure and the responses to L.1 and L.4. The Uniform Rules will designate the responsibilities of each of the financial institutions in the payments process including data privacy and confidentiality of payment and related data. The financial institutions have the flexibility to determine how they meet those responsibilities and those decisions will be reflected primarily in their agreements with their solution providers, if any, and their agreements with their customers. This will allow maximum flexibility to incorporate the best practices as those practices evolve and mature without the need to modify the Uniform Rules.

L.4.2 - Please see the Legal Framework Approach/Structure and the responses to L.1 and L.4. The Uniform Rules will designate the responsibilities of each of the financial institutions in the payments process including data security of payment and related data. The financial institutions have the flexibility to determine how they meet those responsibilities and those decisions will be reflected primarily in their agreements with their solution providers, if any, and their agreements with their customers.

L.4.3 - Please see the Legal Framework Approach/Structure and the responses to L.1 and L.4. The Uniform Rules would designate the responsibilities of each of the financial institutions in the payments process including type of end-use data that may be required for security, legal compliance and authentication purposes. The financial institutions have the flexibility to determine how they meet those responsibilities and those decisions would be reflected primarily in their agreements with their solution providers, if any, and their agreements with their customers.

L.4.4 - Please see the Legal Framework Approach/Structure and the responses to L.1 and L.4. The Uniform Rules would designate the responsibilities of each of the financial institutions in the payments process including how end users may get visibility into the data being collected on them, limits on sharing of data. The financial institutions have the flexibility to determine how they meet

those responsibilities and those decisions would be reflected primarily in their agreements with their solution providers, if any, and their agreements with their customers.

L.4.5 - Please see the Legal Framework Approach/Structure and the responses to L.1 and L.4. The Uniform Rules would designate the responsibilities of each of the financial institutions in the payments process including data breaches at the payment system or at an end user/provider. The financial institutions have the flexibility to determine how they meet those responsibilities and those decisions would be reflected primarily in their agreements with their solution providers, if any, and their agreements with their customers.

L.5 Intellectual property

L.5: Please provide more details regarding intellectual property, including an approach to address any risks arising from third-party rights related to patents, trademarks, copyrights, and trade secrets. In doing so, please specifically address how the Solution supports the intellectual property subcriterion.

The Uniform Rules would designate the responsibilities of each of the financial institutions in the payments process including those responsibilities listed in L.5. The financial institutions have the flexibility to determine how they meet those responsibilities and those decisions would be reflected primarily in their agreements with their solution providers, if any, and their agreements with their customers. This would allow maximum flexibility to incorporate the best practices as those practices evolve and mature without the need to modify the Uniform Rules. This would allow the providers and/or financial institutions to distinguish their services from other providers and/or financial institutions and thus foster competition which would also benefit customers.

L.5.1 – The Uniform Rules would designate the responsibilities of each of the financial institutions in the payments process. The financial institutions have the flexibility to determine how they meet those responsibilities and those decisions would be reflected primarily in their agreements with their solution providers.

Governance

Governance Approach and Structure

Additional Information

The purpose of governance is to direct and approve the Uniform Rules under which financial institutions and providers service the financial institutions' customers which include consumers, businesses, financial institutions, government organizations and others. That purpose is best achieved through structures and processes that are inclusive and transparent.

Existing ECCHO Governance for Image Exchange

Since 1990, ECCHO has been using a process that is inclusive and transparent. ECCHO's processes evolved quickly in an environment in which there was no mandate initially for electronic check presentment and later for check image exchange. Neither of these were/are addressed in statutory or regulatory law so it has been critical to execute processes designed to achieve consensus among a broad base of financial institutions. Today the ECCHO membership holds approximately 80% of all the deposits in the U.S. and approximately 55% of all inter-bank checks are cleared under ECCHO's Rules (the remainder are cleared under the Federal Reserve's rules). The membership includes institutions in all segments of the industry from the smallest credit union (holding less than $10 million in total deposits) to the largest institution holding more than $1 trillion in total deposits and all others in between including community banks, bankers' banks, corporate credit unions, saving banks, state charter banks, national banks and middle tier institutions. ECCHO's membership includes approximately 3,000 financial institutions.

The structure and processes that support this successful governance is similar to that described in the Figure 11. The process includes three levels: subcommittees, ECCHO Operations Committee and the Board of Directors. Participants in the rules creation process include financial institution members described above and other representatives like:

- Providers that support the image deposit, clearing and settlement processes
- Vendors that support, image archive, return and adjustment processes
- Regional Payments Associations
- Consultants with knowledge of and interest in check processes
- Regulators
- Other invited guests where additional specialized knowledge might be needed. One example of guest participation is the inclusion of Payments Canada (formerly the Canadian Payments Association) and a number of Canadian financial institutions. They were included to assist in the development of rules for northbound exchange of images of Canadian cheques.

Structure for Real Time Payments Governance

ECCHO will leverage the governance structure, similar to the existing structure that it utilizes for image exchange, which will consist of three levels: ad hoc subcommittees, Real Time Payments (RTP) Committee, and Board of Directors.

Level One Uniform Rules Creation: Subcommittees

The subcommittees will initially identify legal issues that are not addressed elsewhere in statutory law/regulations/case law to begin development of the Uniform Rules. Beyond meeting the direct legal requirements, this approach supports the ongoing need to enhance and/or clarify the rules and commentary to address user/participant needs not originally addressed in the initial set of Uniform Rules.

Subcommittees are designed to reach in-depth understandings of issues, consensus positions on what actions, if any, should be taken, and then to bring that learning to the RTP Committee for additional analysis with the objective of reaching broader consensus positions.

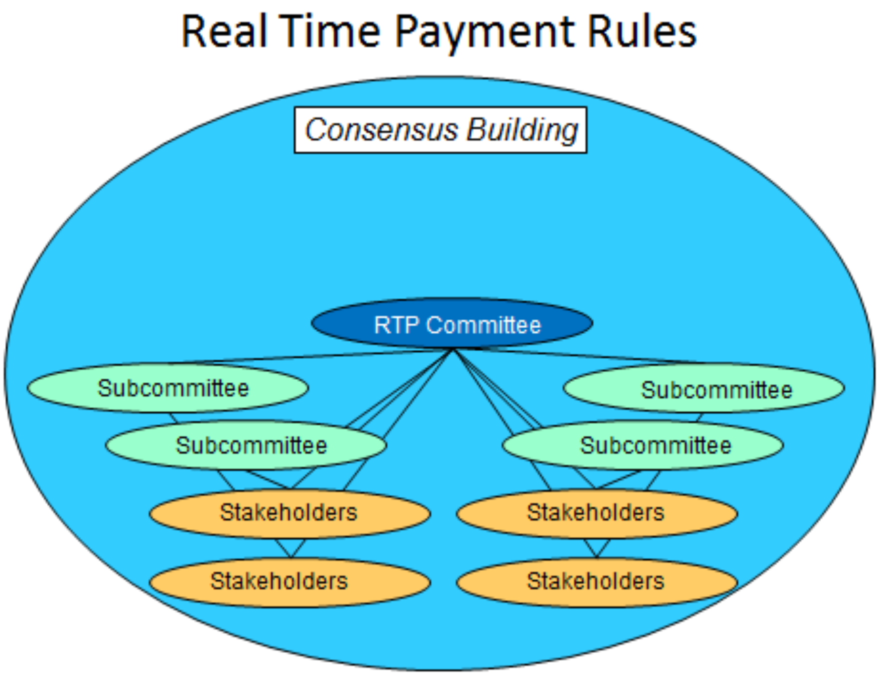


Figure 9 - Governance structure enables stakeholder input

This development process also provides the added benefit of educating the participants in the nuances of the existing or proposed laws, regulations and rules. Although Subcommittee meetings are typically accomplished via conference call for efficiency, initially in-person meetings might be more productive for the development of Uniform Rules.

Participants in the Subcommittees would include representatives from all segments of the industry including large and small banks, bankers' banks, credit unions, corporate credit unions, solution providers, payment legal experts and other interested parties, as appropriate, such as regulators. Because all segments are represented in the subcommittees and RTP Committee process, every rules related issue can be addressed through this process.

Level Two Uniform Rules Creation: RTP Committee

The RTP Committee would meet in person to debate and finalize Rules recommendations for the Board. Some will participate directly in the RTP Committee meeting while other members will be participating indirectly through representatives.

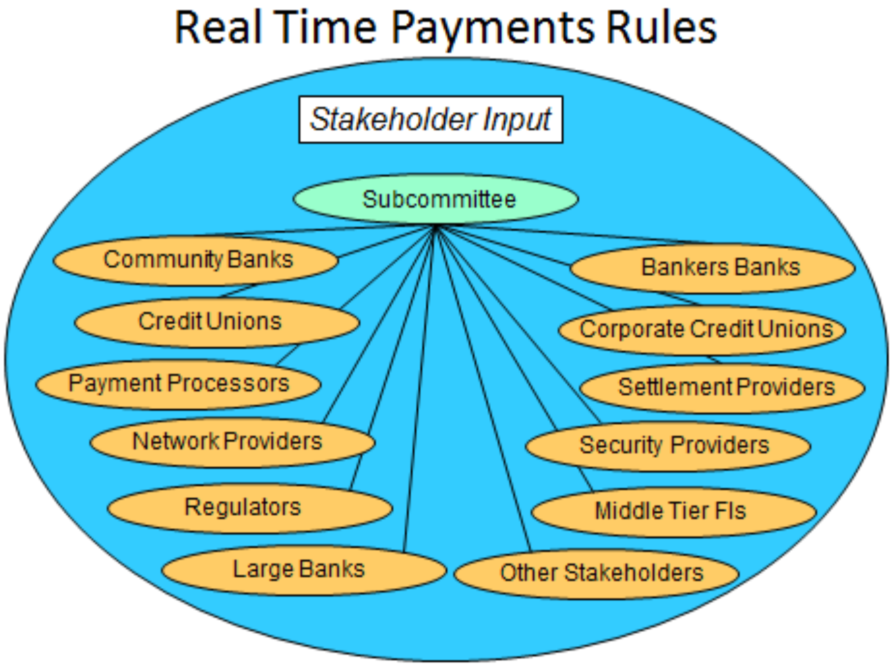


Figure 10 - Inclusive governance structure

It is important that all issues are discussed with the entire group present at the RTP Committee meetings. In-person meetings seek to be as large as possible while still providing the ability for all to participate in input and debate. Discussions would be facilitated through the use of one microphone for every three participants and a speaker system that allows every attendee to hear everyone and to actively contribute to the discussion.

If consensus positions are not reached, the issues would be tabled or sent back to the subcommittee for additional discussion. If a consensus position is reached, a recommendation to the Board would be agreed to at the in-person RTP Committee meeting with every participant present. Consensus means no substantive disagreement with the recognition and agreement from institutions in all segments of the industry and all providers and regulators at the meeting.

Level Three Uniform Rule Creation: Board of Directors

The Chair of the RTP Committee would take the exact recommendation developed at the RTP Committee meeting to the Board of Directors. This unique step is critical to preserve transparency.

The RTP Chair would be a banker that is elected by the Board of Directors. The Chair would be responsible for delivering a review of the RTP Committee's discussion and the recommendation of the RTP Committee directly and in person to the Board of Directors. This process is designed to ensure maximum transparency so the broad base of participants will know that their voices have been heard and represented in the final recommendations as agreed to at the RTP Committee meeting.

ECCHO's Board comprises 21 seats, which is sufficiently large to fairly represent the industry while small enough to effectively discuss and decide the Uniform Rules. Board members are executives from member financial institutions. The size of directors' financial institutions is representative of the industry with large and small member organizations represented (small financial institutions are represented by Bankers' Bank and Corporate Credit Unions).

Once the Board approves the Uniform Rules and Commentary, notification of the approval would be announced to the membership and the Uniform Rules posted to the ECCHO website where they would be publicly available.

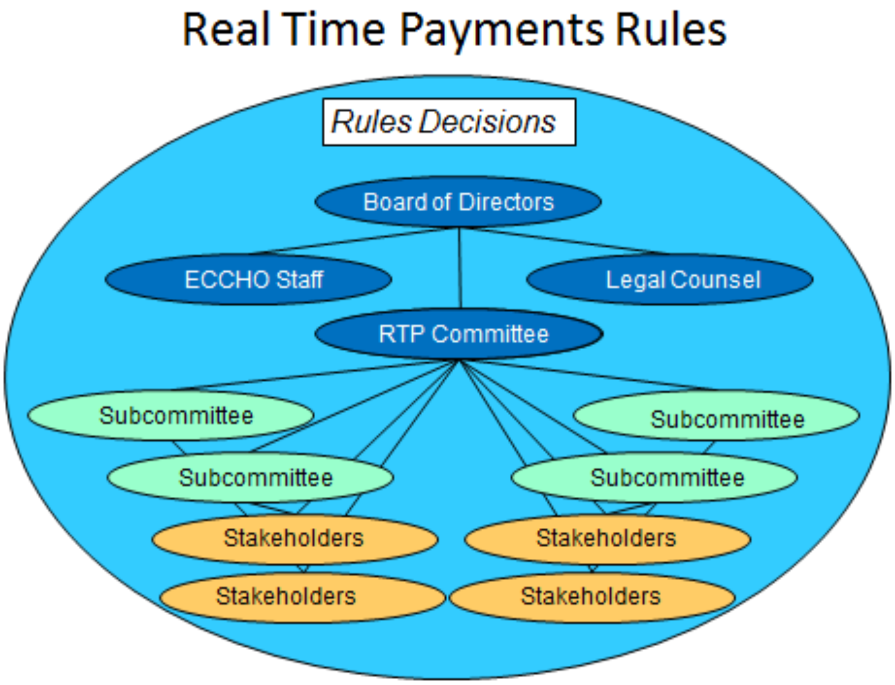


Figure 11 - Governance structure enables rules development

Governance synopsis: The process will begin with the contribution of a diverse set of stakeholders that participate in ad hoc subcommittees. These ad hoc subcommittees are created to fulfill specific purposes for as long as needed including: rules development, exceptions processing, legal issues, etc. The subcommittee participants would be experts who have the knowledge to create, review, edit and debate the purpose/intention of the Uniform Rules. Subcommittee members would be eligible to participate in the in-person Real Time Payment Committee as well. The RTP Committee exists to take input and strawman rules from the subcommittees, with the intention of producing rules recommendations to the Board of Directors. Finally, the Board will take these rules recommendations and approve them or send them back to the RTP Committee for additional work. Uniform Rules will be made available to the public on the ECCHO website.

Questions and answers

G.1 Effective governance

G.1: Please provide more details regarding effective governance, including decision and rule-making processes that are transparent and support both the Solution's objectives and Public Policy Objectives. In doing so, please specifically address how the Solution supports the four effective governance subcriteria.

Please see Governance Approach and Structure narrative and figures above.

G.1.1 - Please see Governance Approach and Structure narrative and figures above.

G.1.2 – Please see Governance Approach and Structure narrative and figures above. The ECCHO website includes the dates and location of ECCHO Operations Committee meetings and the ECCHO Board of Directors meetings. Every ECCHO employees' name and direct contact information is listed on ECCHO's website. Information about ECCHO subcommittee and Operations Committee meetings is distributed to hundreds of individuals in advance of the meetings.

G.1.3 - Please see Governance Approach and Structure narrative and figures and Legal Framework Approach and Structure above. Not every legal provision needs to be addressed in the Uniform Rules or through the governance process. Those that are addressed will follow the same process designed for all changes to the Uniform Rules. Because the legal framework includes agreements between financial institutions and their solution providers, and between financial institutions and their customers, appeals under those agreements will need to be handled through those organizations rather than through the Uniform Rules governance structure. This approach supports a Uniform Rules set that addresses the needs of the broadest base of participants and creates a stable, dependable set of legal provisions. Additionally, this approach supports resolution of the appeals by those closest to the processes and most affected by the issue under appeal--the financial institutions and/or the processors. Should an appeal result in the need for a change in the Rules, the recommendation to change the Rules would proceed through the normal Rules approval process to ensure that the full impact of the change has been considered by all of the stakeholders and that a consensus position, if possible, has been developed.

G.1.4 - Please see Governance Approach and Structure above. Validation of compliance with financial institutions' legal responsibilities falls primarily on the institution's internal auditors, external auditors and bank examiners. Additionally, financial institutions that fail to comply with the Rules are subject to claims from other financial institutions and should that process fail, the Rules provide for dispute resolution through arbitration. As a last resort, other remedies are available through the courts. Some conflicts can be avoided by institutions having a knowledgeable staff that understands the Rules and their responsibilities.

G.2 Inclusive governance

G.2: Please provide more details regarding inclusive governance, including input and representation from diverse stakeholders, and support for the public interest. In doing so, please specifically address how the Solution supports the five effective governance subcriteria

Please see Governance Approach and Structure narrative, Legal Framework Approach and Structure narrative, the response to L.1 and to figures 9 to 11.

G.2.1 – Please see Governance Approach and Structure narrative, Legal Framework Approach and Structure, the response to L.1 and to figures 9 to 11.

G.2.2 – Please see Governance Approach and Structure narrative, Legal Framework Approach and Structure, the response to L.1 and to figures 9 to 11.

G.2.3 – Please see Governance Approach and Structure narrative, Legal Framework Approach and Structure, the response to L.1 and to figures 9 to 11.

G.2.4 – Please see Governance Approach and Structure narrative, Legal Framework Approach and Structure, the response to L.1 and to figures 9 to 11. ECCHO's membership includes financial institutions that hold more than $9 trillion in deposits and all are represented in ECCHO's governance process. These institutions include community banks, credit unions, bankers' banks, corporate credit unions, state charter banks, nationally charter banks, savings banks, large banks and middle tier banks. Additionally, more than 100 service providers are included in the governance process, including the Federal Reserve. These service providers process and clear payments, return payments, adjust payments, settle payments, archive payment records, provide network services, consult about payments, and every other aspect of payments services.

G.2.5 - Please see Governance Approach and Structure, Legal Framework Approach and Structure and the response to L.1. The membership is open to every depository financial institution in the U.S. as defined by the Federal Reserve Act. The ECCHO Rules are solution provider and product/service independent. Many solution providers actively participate in the development and maintenance of the Uniform Rules. The Uniform Rules will apply exactly the same provisions to every member regardless of size or type of financial institution. The rules recommendations will be developed openly at the RTP Committee meetings based on consensus by the participants and the exact recommendations agreed to at the RTP Committee meeting will be brought to the Board of Directors by the Chair of the RTP Committee. Then the ECCHO Board of Directors can approve the Uniform Rules recommendation or send back to the RTP Committee for additional work. Note: The ECCHO Board of Directors has a history of always approving recommended image exchange rules recommendations from the Operations Committee. Some rules recommendations have been sent back for additional information or re-work but ultimately have been approved.

Faster Payments QIAT

DRAFT ASSESSMENT

Property of the Federal Reserve Bank of Kansas City and the Federal Reserve Bank of Chicago (“Banks”)

Not for distribution or publication without the express written permission of the Banks

Faster Payments QIAT

DRAFT ASSESSMENT

Proposer: Kalypton Group Limited and The Electronic Check Clearing House Organization

Summary Description of solution:

Kalypton's solution, Tereon, is described by the proposer as a "full transaction processing engine, not just a payment platform" (p.104). The proposer describes a technology delivering "blockchain-like capabilities." As such, Tereon does not provide a distributed ledger: it provides distributed authentication of private ledgers. The identified challenges of Distributed Ledger Technology (DLT) —including scalability, security, privacy, interoperability and sustainability—thus do not affect the solution.

Tereon consists of a "bank-grade" central core that is fully integrated into the banking system. A highly configurable software layer sits on top of the core platform. Tereon is a powerful, flexible transaction processing solution that moves funds from account to account in real time. The solution supports real-time payments using internet-enabled sessions or mobile data networks. The solution requires access to provider core accounts via an API. The solution is available to banks and non-bank providers and will support the unbanked. It provides a tool kit to facilitate ongoing innovation by providers and other third parties. All use cases are enabled at launch. Kalypton is in the process of deploying its first commercial implementation of Tereon in Central America.

.

EXECUTIVE SUMMARY OF THE PROPOSAL

- **Major strengths**
  - The solution is flexible and can be configured to support all transaction types and different currencies. It has been designed to serve the banked and unbanked. Tereon facilitates payments to and from all types of accounts and is able to support all use cases at launch.
  - The solution requires that all funds and fund transfers operate within the regulated banking environment to ensure that funds are protected and regulated.
  - Tereon is a secure solution that supports device and user authentication for every session and transaction as determined by the provider.
  - The solution consists of multiple, standalone Tereon systems operated by providers. The failure of one server does not affect the overall network of servers, and the network should be available 100% of the time. The solution can connect any authorized user on one system to transact with any authorized user on another system. The two systems are linked using a directory system. Tereon can associate multiple devices and multiple users with a single account, and it can associate multiple accounts (in different currencies) with a single device.
  - The solution does not expose any personal data during a transaction and includes a data access capability to support data management. Kalypton is currently implementing its first commercial deployment of the solution in Central America.
- **Areas for improvement and enhancement**
  - The proposal does not define the transaction information to be shared between Tereon servers and banks. It is unclear how much visibility will be allowed into the accounts held on Tereon

servers. More details about the flow of information within and between providers, as well as requirements related to risk management, would be helpful.

  - Few details are provided regarding the infrastructure required or the accounts that providers must create and manage to support Tereon.
  - The proposal describes settlement within the solution as hypothecation of the transaction funds to a Tereon settlement account. Non-banks must set up “control accounts” at FIs to manage the movement of funds. Ultimately settlement between FIs occurs using the providers’ existing settlement mechanism(s).

- **Use cases addressed**
  - The solution addresses all four major use cases (P2P, P2B, B2P, and B2B) and includes cross-border capabilities.
- **Proposer’s overall ability to deliver proposed solution**
  - This proposal is well thought-out and considers FPTF requirements. The solution relies on access to existing end-users’ or providers’ bank accounts and leverages existing settlement capabilities. The value that Tereon delivers is faster, more secure, lower-cost transactions.
  - The proposal does not describe the investment and implementation effort required for provider participation.
  - The solution includes technology that is subject to a patent application. As a result, the solution’s technology has not been fully described in the proposal.
  - The proposal does not define the implementation timeline, other than to state that Tereon can be implemented within a matter of months and within the Task Force’s proposed time frame.
  - Additional information would be beneficial in several areas related to implementation, including building a critical mass of users and merchants, identifying scheme operator(s), and developing and implementing scheme rules and governance frameworks.
  - The proposal suggests that it may be necessary to create one or more specialist payment banks to compete with existing banks in providing services.
  - A commercial implementation of the solution is underway in Central America. It would be helpful to understand the similarities between the Central American implementation and the proposed solution for the U.S. market and how the lessons learned from the Central American implementation will inform roll-out in the U.S.

ASSESSMENT

Ubiquity

U.1 Accessibility

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale

The solution supports payments to and from any account and is available both to FI providers and to non-FI providers that meet deposit-taking regulations. Non-FI PSPs (payment service providers) provide access for the unbanked (U.1.1). The solution uses a directory look-up service that supports the routing of payments between providers. The directory lookup capability enables providers to trust one another as both parties to the transaction must be authorized in order to interconnect. If an end-user does not have a Tereon account, there is an option to withdraw received funds through a service provider. The initiator of the payment is ultimately responsible for identifying the payee and to ensure that the payee receives the transaction number (Tereon will provide by email /SMS if possible) and PIN (payer must ensure provision of the PIN to the payee).

Regarding funds access, any entity with a smart phone and a cash box can act as a merchant supporting the withdrawal of funds. If the recipient does not withdraw the funds within a specified time period, the transaction is nullified and the funds are returned to the payer (U.1.2). The solution can support multi-currency payments (U.1.3). Tereon makes no distinction between banked and unbanked users (U.1.4)

Implementation of the solution requires providers to allow access to core account systems via APIs and to invest in high-end commodity servers. The solution uses a standardized messaging protocol and can support most communication formats via a translator. Kalypton provides a set of Tereon protocols (a tool kit) that providers can use to develop new, proprietary services. Transaction information can be transmitted over the internet or mobile data networks, simplifying implementation. Merchants can accept payments using a smart device, thereby avoiding upgrades at the POS (point of sale); however, integration may be required in operational systems to support a new payment option (U.1.5).

U.2 Usability

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale

The solution supports almost any payment channel and device (U.2.1). Payments can be routed using the payee’s Tereon ID, which can be an email address, mobile number, name, etc. (U.2.2). Account information is never shared as part of the transaction (unless the payment vehicle is a check). Payments to non-registered users require payee name and address to allow for authentication. Tereon is designed to be available 24x7x365, though full-time access will depend on the availability of the provider’s system (U.2.3). Tereon allows providers to select authentication credentials for end-users, and supports multiple options for doing so. The solution supports multiple languages and multiple use cases (U.2.4).

U.3 Predictability

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution clearly defines a consistent, baseline set of transactions that any provider will be able to support at implementation. Baseline services are available via any channel or device and are delivered using standard communications and messaging protocols (U.3.1, U.3.2, U.3.4). All fees will be clearly communicated to the payer before a payment is initiated. The solution can support multiple communications and messages originating in multiple protocols and supports communications in any language (U.3.3).

No system rules exist for the solution at this time, and a dispute management process has not yet been defined. The legal framework for the system rules and dispute resolution mechanisms will be based on the existing ECCHO Operating Rules for electronic check presentment, but with the necessary amendments to provide for the operational nature of Tereon. The rules will set out an error resolution process will allow users to resolve any errors that might occur. Kalypton will also leverage the system rules and dispute mechanisms that are part of the planned implementation in Central America (U.3.4).

“Tereon’ is the name of Kalypton’s transaction processing software platform and does not need to be the user-facing brand for ad service or scheme built on Tereon (U.3.5).

U.4 Contextual data capability

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale

Tereon transmits its data, including any contextual data, in an obfuscated, serialized and encrypted form. Data that is received from a sender’s system is translated into Kalypton’s own internal data format before it is transmitted to the recipient system Tereon server, where it is translated into the recipient’s data format (whatever that may be). The solution supports contextual data across all use cases. Contextual data capabilities seem broad and are extensible to include targeted offers or similar non-transaction-related information (U.4.1). The solution’s multi-currency capability allows for the processing of loyalty points (U.4.2).

The solution can interface with business finance systems, personal finance systems, banking systems, etc. The solution supports ISO8583 and ISO20022 and can be adapted to support any communication standard as required (U.4.3).

Tereon captures data that has not (yet) been defined by ISO 20022 (e.g., no ISO 20022 message schema is currently defined for geolocation data). Kalypton can leverage the supplementary data field and will work with industry participants to define the format for data to be included in this field. Tereon will retain all transaction data in its own internal audit logs, and providers can use other Big Data systems to access and process this data. Kalypton will define contextual data requirements at the start of the implementation phase.

U.5 Cross-border functionality

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution is well-designed to support multi-currency payments. If a payee and payer operate in different currencies, the solution supports a foreign exchange capability, including notification of the exchange rate and fees prior to initiation of the transaction (U.5.3; U.5.4).

While Tereon can connect and communicate with payment systems in other countries, it will require providers to accept any associated settlement risks, which could hinder widespread adoption. More clarity is needed on how it can be interoperable with payment systems in other countries (U.5.2). With regards to ISO 20022, Tereon makes no distinction between domestic or cross-border transactions and provides all data for all transactions regardless of endpoints, as described in U.4.

Tereon acts as an RTGS (real-time gross settlement) system in its default mode but can operate as a DNS (deferred net settlement) system or an RTGS-DNS hybrid. In every mode, a user must have sufficient credit or funds to make a payment or transfer, and the provider cannot approve the payment unless it has the funds to settle the payment or transfer. This good-funds model eliminates settlement risk.

U.6 Applicability to multiple use cases

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution supports all of the required use cases in its initial implementation.

Efficiency

E.1 Enables competition

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The proposal states that any end-user can change providers at any time without any loss of "in-air" payments (E.1.1). Any transactions that are in when the end-user switches providers will move seamlessly to the new provider. Tereon requires providers to share all fees associated with the Tereon service as part of the enrollment process (E.1.3). Any provider that is willing to abide by the governance and payment rules can offer a service using Tereon (E.1.4). All providers are required to support baseline services, regardless of size. Non-bank PSPs must hold an account at a regulated FI to ensure that funds are kept within the existing banking system. All providers have access to a tool kit that will support the introduction of new products and services on the Tereon platform.

When end-users switch providers, their account history will transfer from the old provider to the new. A user can register multiple IDs with a single provider or register the same ID and device with multiple providers. The directory look-up service can differentiate among providers based on the services they provide to a user (U.1.2).

E.2 Capability to enable value-added services

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

So that all providers can integrate with Tereon and offer value-added services to any user, Kalypton will publish all protocols and standards. A third party needs to link to only one provider’s Tereon server to offer its services to any user who is allowed to use that service. Kalypton has already published APIs and protocols for earlier versions of Tereon. As new services and functions are added, Kalypton will publish APIs and protocols to enable third parties to use those functions and services. The solution puts the user in control of the additional service(s) used (E.2.1; E.2.2). Tereon will clearly disclose value-added services as optional extras (E.2.3).

E.3 Implementation timeline

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

FI providers’ willingness to participate in this solution will play a substantial role in determining its long-term success. The solution will not be successful without access to core deposit accounts at FIs. The proposal states that the implementation of technology is not the limiting factor in a deployment timeline, and that the solution is designed to be implemented within months. Retailers may be more likely adopters due to the reduced costs associated with PCI requirements and transaction processing.

The proposal provides a very detailed implementation plan that describes key tasks and provides estimated timelines based on past experience in implementations in other jurisdictions. The proposal acknowledges that there will be differences that are particular to the U.S. market. There are some concerns as to whether the implementation milestones can be achieved in the time frames provided. Retailers are expected to actively adopt the solution due to reduced costs. Banks’ adoption may lag behind the proposed timeline. The proposal would be strengthened by more clearly articulating the value proposition for banks, and the provision of a more detailed implementation timeline. (E.3.1).

E.4 Payment format standards

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution uses its own internal message protocol to support communication between servers and devices. It can interface with any existing message format through translation, if required (E.4.1-E.4.2), and is designed to support upgraded or new message formats (E.4.4). There are some concerns about the effectiveness of translation engines generally, which may impact the effectiveness of this approach. Each provider will determine the message format to be used.

The solution’s modular design makes APIs a natural conduit to support the implementation of upgraded or new functionality. Tereon publishes a set of APIs to integrate to core systems within account providers, and at a level that the account providers can choose.

Tereon has been designed to retain all information that is captured and generated when processing a transaction, whether or not the communication format can accept that data. This data is retained in its original format and can be utilized as message formats evolve.

E.5 Comprehensive

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution can enable all aspects of the payment process (E.5.1). The proposal does not describe any requirements related to end-user accounts. The technical solution will support all the features described. The solution describes several options for settlement, and describes its preferred solution to involve the central bank (E.5.2).

E.6 Scalability and adaptability

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The solution addresses a core set of baseline use cases (E.6.1). The solution is designed to process millions of transactions per second per provider based on a peer-to-peer architecture, and it can be easily modified to add new services or volumes (E.6.2). The proposal indicates that when a provider’s system exceeds a set threshold, Tereon will scale itself horizontally to manage the additional load. Tereon has defined four metrics that determine when automatic horizontal scaling will be initiated: network load, CPU load, transaction volume, and system temperature. Kalypton and the provider will determine the exact loading of each metric based on hardware and configuration.

Tereon claims it can support provider hardware upgrades with no impact to end-users (E.6.3). The proposal states that Tereon is designed to operate on standard carrier-grade equipment that may already be in place at provider locations. A provider’s hardware investment will depend on the volume of services and number of users to be supported. Kalypton has worked with a financial services hardware provider to define three hardware configurations (servers, storage systems, networking infrastructure).

E.7 Exceptions and investigations process

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The existing ECCHO rules and procedures will inform Tereon's process for resolving exceptions and disputed transactions. Because Tereon is a real-time solution, the proposer anticipates that exceptions or disputes will be rare. The system rules will include effective, economic mechanisms to enable users and providers to resolve any exceptions or disputed payments that may occur (E.7.1). The Tereon messaging service can be used to send alerts and notifications to support an exceptions and investigations process (E.7.1).

Tereon records every transaction in real time, and each record includes the time and date. All users are made aware of the audit trail and can access the information at any time. The audit trail captures all contextual data surrounding the transaction and stores this in a searchable, anonymized state (E.7.2). Tereon can render data anonymous if required, aggregate data into a monitoring service, and share that data among providers. This data can be provided as a real-time feed so that an aggregator can use Big Data analytics to monitor transaction traffic for suspicious patterns (E.7.3).

The ECCHO rules to support faster payments have not yet been developed and therefore cannot be evaluated (E.7.1). It would be helpful if the solution developed tools to support exceptions and investigations (E.7.1).

Safety and Security

S.1 Risk management

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The solution is configurable and enables a provider to amend a service and/or track required data in the event of an unexpected change in law, regulation, or rule (S.1.1).

Tereon can settle a transaction a number of ways, depending on the settlement mechanism that providers wish to use. The solution relies on providers' existing settlement capabilities, which may or may not be batched. The solution hypothecates payment transactions to settlement accounts and requires those funds to be used to settle Tereon payments; in this way, it addresses liquidity and settlement risks associated with deferred settlement (S.1.2).

Tereon automates as much of the payments system as possible to minimize the risks of human error. The solution is designed to limit access based on role. The solution is designed with built in redundancy and automatic scaling to address any infrastructure issues or dramatic increases in usage (S.1.3). To address the risk of fraudulent transactions, the solution requires end user authorization, very limited sharing of transaction information (no PII), places to authorization or authentication credentials on the device, and has mechanisms that allow an end users to manage induced payments made under duress. The solution is designed to minimize errors in payment. (S.1.4).

Legal and risk management frameworks will be reviewed at least every six months to address any changes in law and/or regulation (S.1.6)... To fully address liquidity and settlement-related risks, the solution could integrate with, or even require integration with real-time settlement mechanisms as they are introduced into the market.

S.2 Payer authorization

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution requires payer authorization for every transaction. Authentication involves several steps, some of which can be optional, depending on the provider's requirements (S.2.1). The solution also allows for preauthorized payments (S.2.2), which the end-user can modify (S.2.3). Clearing and settlement take place when the payment is made. However, the user can configure the account to "block" the funds when payment is initiated. The solution can also support low-value transactions without authorization (such as transit) that are guided by parameters within the solution.

S.3 Payment finality

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The solution requires the provider to approve each payment to ensure good funds (S.3.1). The proposal states that payments become irrevocable once they are hypothecated to the settlement account and the recipient has received the funds (S.3.2).

While the proposal is clear about the need for operating rules and goes as far as to say that the ECCHO framework will be used, the rules, policies and regulations have yet to be developed. The proposal states that the payment rules will provide a mechanism to compensate payers/payees if a payment is disputed successfully. The operating rules, when written, should provide clarification on a dispute process and a mechanism to compensate payers or payees if a payment is successfully disputed (S.3.3).

S.4 Settlement approach

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The solution requires payers to have sufficient funds to support a transaction through the hypothecation of funds. The proposal describes hypothecating funds to a settlement account but relies on providers' existing settlement capabilities for final settlement (S.4.1). Tereon can be overlaid onto existing Deferred Net Settlement (DNS) systems to add the functionality of a secured DNS settlement option. This step is not optimal, however, as it may require intra-day credit or liquidity to ensure available funds to support transaction processing (S.4.2). The proposal states that Tereon's preferred settlement method is for providers to hold settlement accounts with the central bank and to settle in central bank money, and to leverage real time (RTGS) settlement capabilities to remove settlement liquidity risks (S.4.3). The solution requires participants to treat transactions as irrevocable once funds have been hypothecated for settlement and received by the recipient.

The proposal could be strengthened by detailing the method(s) that will be in place to manage intra-day credit/liquidity (S.4.2).

S.5 Handling disputed payments

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

Users, devices, accounts, or providers can be blocked from the system if an unauthorized, fraudulent, or erroneous payment is detected (S.5.1). The Tereon solution is designed to enable a provider to conform to consumer protection law and will support the reversal of erroneous payments (S.5.2). The Tereon audit capability provides detailed and searchable information for every transaction and action by account. The solution supports the initiation of a dispute, end-user refunds, and transaction reversals (S.5.3).

The proposer clearly acknowledges the need for operating rules and will base those rules on ECCHO's rules framework the rules have yet to be created. The proposer can strengthen the proposal by directly outlining how disputed payments will be handled, delineating each party's rights, confirming roles, responsibilities and liability allocation, and providing the timelines associated with disputed payments (S.5.2, S.5.3).

S.6 Fraud information sharing

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The solution has a well-defined audit capability and tracks and retains all aspects of a transaction (S.6.6). Tereon can share that information in real time (S.6.3), supplying a suitably structured data feed into a Big Data analytical tool or to a third party for data analysis (S.6.1).

Tereon strictly controls access to data based on ownership and roles. Tereon also offers the tools to combat fraud by allowing approved administrators access to users' full transaction history to investigate those transactions further (S.6.5). Access to this data is tightly controlled, and the audit system tracks all administrator actions.

The solution would be strengthened by requiring the sharing of key data elements to support identification of fraudulent activity beyond a single provider (S.6.1) and defining how data owned by other entities would be aggregated and anonymized to support fraud information sharing (S.6.2).

.7 Security controls

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

Tereon's security controls are layered, and all access to the system is recorded by the audit capability (S.7.1). Access is not permitted to any aspect of the solution unless security measures have been met. All data is encrypted with independent keys before transmission to or from any endpoint or server (S.7.1). The solution is designed to guarantee the data's integrity and to protect against system failure.

As with several aspects of the solution that require operating rules and a governance model, the participation agreement, when created, should define participation requirements pertaining to physical and environmental security, managerial policies, operational security, monitoring, and incident response (S.7.2-3).

S.8 Resiliency

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution is designed to provide a fully redundant, resilient, and efficient payments service. Tereon is designed to be available 24x7x365 with full n+2 redundancy (two independent back-up components). The solution's target availability for each provider is 99.95% for each individual component, and 100% for the service as a whole (S.8.1).There is no single point of failure in the system as servers communicate on a peer-to-peer basis (S.8.2). Although individual components may fail, multiple redundancy and the ability to start up replacement instances to replace any failures would deliver 100% uptime overall (S.8.3). Tereon is self-monitoring, and each provider will have the tools necessary to monitor the uptime of both individual components and the solution as a whole (S.8.4). As indicated in the proposal, payment rules will need to define requirements and procedures for provider contingency testing (S.8.5).

S.9 End-user data protection

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution includes strong controls and mechanisms for administrator access. Tereon's audit capability captures all interactions with the system (S.9.1). The solution supports the initiation and routing of payments using a Tereon ID, and account information is never exposed at any time during the transaction (S.9.2, S.9.3)).

S.10 End-user/provider authentication

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution supports multi-factor authentication ranging from PIN to biometric options (S.10.1) and is clearly aligned with industry standards for end-user authentication (S.10.3). The solution ensures that payments will reach the intended end user (S.10.2). The solution's design is modular, and the addition/decommission of authentication models should be easily accomplished without impact to the solution overall (S.10.6). The solution includes a directory lookup capability that routes payments from payee to payer using only a Tereon ID (S.10.2). Every end-user device and Tereon server must be approved and licensed to communicate on the Tereon platform (S.10.1). The solution requires the same authentication procedure irrespective of the transaction's value (S.10.4).

Providers will be held responsible for authenticating end-users. It would be helpful for Tereon to define authentication requirements for providers in addition to KYC and AML procedures (S.10.1)...

S.11 Participation

Very Effective Effective [✓ Somewhat Effective] Not Effective

Rationale:

Participation rules have yet to be written. When available, the rules will set out the duties and obligations of provider and will define sanctions for failure to comply with rules (S.11.1). The rules will ensure that providers are able to fulfill their obligations (S.11.2). Tereon will monitor (in real time) and flag providers that appear to be introducing risk into the solution (S.11.3).

The proposal states that Kalypton has a standard user license agreement that will be tailored to U.S. law once the preliminary rules and agreements (Uniform Rules) have been drafted to ensure that the Uniform Rules are correctly referenced in the agreement.

Speed (Fast)

F.1 Fast approval

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

Tereon is designed to approve or deny a transfer or a payment in less than one second from the moment of payer initiation.

F.2 Fast clearing

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

Tereon is designed to clear a transfer or payment in less than one second from the moment of payer initiation.

F.3 Fast availability of good funds to payee

[✓ Very Effective]   Effective   Somewhat Effective   Not Effective

Rationale:

Tereon hypothecates funds to a settlement account and credits a recipient's account with funds in less than one second from the moment of payer initiation. There is one exception, however: if a recipient does not have a Tereon ID, the funds will remain available for a period of time (defined by the transferor) so that the recipient may retrieve them from a Tereon "agent" or set up a Tereon account. If the funds are not claimed, they are returned to the payer.

F.4 Fast settlement among depository institutions and regulated non-bank account provider

Very Effective   [✓ Effective]   Somewhat Effective   Not Effective

Rationale

Tereon hypothecates funds to a settlement account in less than one second. However, final settlement of the transaction relies on the individual providers' existing settlement options which are not yet real time, and do not operate 24/7/365 potentially creating risk (F.4.1).. The solution is designed to operate 24/7/365, which addresses concerns related to different time zones (F.4.2). Tereon has the capability to net transfers and payments for providers. Regulatory authorities may determine liquidity levels that providers must maintain, and Tereon can enforce those levels.

The proposal states that the preferred settlement option is for providers to hold settlement accounts at the central bank and to settle using central bank money. This option would remove all settlement risk, and would allow Tereon to settle transactions immediately acting as an RTGS solution.

F.5 Prompt visibility of payment status

[✓ Very Effective]   Effective   Somewhat Effective   Not Effective

Rationale:

The status of a payment is immediately reported to the payer's systems. Tereon always notifies the payer when the account has been debited and when the recipient has received the funds, and notifies the recipient when a pending transfer or payment has been approved and when the funds have been credited to the account (F.5.1-2).

Legal

L.1 Legal framework

Very Effective   [✓ Effective]   Somewhat Effective   Not Effective

Rationale:

ECCHO will identify and analyze all relevant laws and regulations that will form the basis of the legal framework for Faster Payments at the industry level (Uniform Rules) (L.1.1). The governance and legal frameworks for the Tereon solution will be based on these industry-level requirements and will define each process and participants' responsibilities in the solution (Provider Agreement) (L.1.3).

L.2 Payment system rules

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

ECCHO will identify and analyze all relevant laws and regulations that will form the basis of the legal framework for Faster Payments at the industry level. The payment system rules defined for the Tereon solution will be based on these industry-level requirements and will define each process and the accountabilities of solution participants (L.2.1). The proposal defines which aspects of the rules will be addressed once defined and describes a high-level rules amendment process (L.2.2).

L.3 Consumer protections

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The proposal acknowledges that although Tereon is designed to limit the likelihood of disputed payments, the solution does require a legal framework to provide protection and certainty for consumers to drive adoption. The legal framework will define the legal and financial responsibilities of all users and providers related to unauthorized, fraudulent or erroneous consume payments (L.3.1). The rules will support error mechanisms to meet, and perhaps exceed protections required under applicable law (L.3.2). The legal framework may allow providers to exceed protections that are currently required under applicable law (L.3.3).

L.4 Data privacy

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The Uniform Rules will define each party's data privacy responsibilities in the payments process. The proposal indicates that the data protection framework may be modeled on parts of the EU General Data Protection Regulations and may exceed the protection currently afforded under applicable law (L.4.2). The legal framework will define the data that end-users must provide to enroll and to send payments to non-registered users (L.4.3), end-user visibility to data that is collected (L.4.4), and providers' obligations related to access and data protection (L.4.5).

L.5 Intellectual property

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

A number of patents that address the solution and its capabilities are pending. Kalypton and ECCHO will continue to conduct ongoing due diligence reviews of all applicable IP rights.

The proposer recognizes the need to develop an approach to manage intellectual property rights. The approach will be developed in cooperation with ECCHO.

Governance

G.1 Effective governance

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

At the industry level, ECCHO will leverage the governance structure, which is similar to the existing structure that it uses for image exchange. This governance arrangement consists of three levels: ad hoc subcommittees, an RTP committee, and a board of directors. The governance structure for the Tereon platform will be determined by the bylaws of the solution's rules organization. The proposal describes a board of directors comprising representatives from various stakeholder groups. The board will set policy objectives and approve the rules with consideration for the interests of all stakeholders. The governance arrangements will be made public (G.1.2). High-level guidelines are provided regarding the appeals process (G.1.3) and independent validation of compliance. Governance arrangements will provide for independent validation of the governing organization's compliance with the solution's governance and legal frameworks (G.1.4). Kalypton will work with ECCHO to develop a governance framework.

G.2 Inclusive governance

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The proposal suggests that the solution's governance rules will ensure that public and stakeholder interest will be considered when making rules and decisions (G.2.1-2). Board decisions will rely on input from governance substructures/subcommittees (G.2.2). The proposal describes a high-level issue resolution process. An operations committee will be formed, and this committee's chair will present recommendations at board meetings. Bylaws will include provisions for managing conflicts of interest (G.2.5). Kalypton will work with ECCHO to develop a governance framework.

APPENDIX A: ASSESSMENT SUMMARY

✓= QIAT Assessment ○ = Proposer Self-Assessment

UBIQUITY	Very Effective	Effective	Somewhat Effective	Not Effective
U.1: Accessibility	○✓			
U.2: Usability	○✓			
U.3: Predictability	○✓			
U.4: Contextual data capability	○✓			
U.5: Cross-border functionality	○✓			
U.6: Multiple use case applicability	○✓			

EFFICIENCY	Very Effective	Effective	Somewhat Effective	Not Effective
E.1: Enables competition	○✓			
E.2: Capability to add value-added services	○✓			
E.3: Implementation timeline	○	✓		
E.4: Payment format standards	○✓			
E.5: Comprehensive	○✓			
E.6: Scalability and adaptability	○	✓		
E.7: Exceptions and investigations process	○	✓		

SAFETY AND SECURITY	Very Effective	Effective	Somewhat Effective	Not Effective
S.1: Risk management	○	✓		
S.2: Payer authorization	○✓			
S.3: Payment finality	○	✓		
S.4: Settlement approach	○	✓		
S.5: Handling disputed payments	○	✓		
S.6: Fraud information sharing	○	✓		

✓= QIAT Assessment ○ = Proposer Self-Assessment

SAFETY AND SECURITY (cont'd)	Very Effective	Effective	Somewhat Effective	Not Effective
S.7: Security controls	○	✓		
S.8: Resiliency	○✓			
S.9: End-user data protection	○✓			
S.10: End-user/provider authentication	○✓			
S.11: Participation requirements		○	✓	

SPEED (FAST)	Very Effective	Effective	Somewhat Effective	Not Effective
F.1: Fast approval	○✓			
F.2: Fast clearing	○✓			
F.3: Fast availability of good funds to payee	○✓			
F.4: Fast settlement	○	✓		
F.5: Prompt visibility of payment status	○✓			

LEGAL	Very Effective	Effective	Somewhat Effective	Not Effective
L.1: Legal framework		○✓		
L.2: Payment system rules		○✓		
L.3: Consumer protections		○✓		
L.4: Data privacy		○✓		
L.5: Intellectual property		○✓		

GOVERNANCE	Very Effective	Effective	Somewhat Effective	Not Effective
G.1: Effective governance		○✓		
G.2: Inclusive governance		○✓		

APPENDIX B: PROPOSER RESPONSE TO QIAT ASSESSMENT

Firstly, Kalypton and ECCHO want to thank the Federal Reserve Banks, the Faster Payments Task Force and the QIAT for the opportunity to present our capabilities to you all. Overall, we feel that the assessment is balanced and fair within the constraints of the process.

We separate the criteria into two classes; those where the assessment is based primarily on the technology deployed and those where the assessment is based primarily on how it is deployed and by whom; all issues yet to be resolved.

Without exception, where the dominant basis for the assessment is the inherent capabilities of the technology, we believe that our proposal warrants a “very effective”. That is the rationale for the difference between our self-assessment and the QIAT assessment highlighted above.

However, we have the benefit of proprietary information that we have not felt able to share under this process as that information is still the subject of patent applications. Going forward, and if there is an appetite, we are willing to share that information with a sub-group of the Faster Payments Task Force willing to sign non-disclosure agreements. In the meanwhile, the summary rationale for our self-assessments is that in the following criteria, Tereon should have been marked at a higher level because:

- E3: the proposal provides a very detailed plan by way of an example. In order to draw up an even more detailed and accurate project plan, we would need to know more details about each provider’s infrastructure and internal readiness to implement the solution. The detailed plan that the proposal outlines can easily be tailored to fit individual providers once those details are known and disclosed. The criteria do not disclose any of those details.

  In the experience of ECCHO, financial institutions are most willing to participate in a solution that they have a stake in developing and managing the rules initially, and on an on-going basis. This ensures buy-in but more importantly fairness to all participants. While solutions that have already created rules are known commodities, they tend to be slanted towards their creators/owners. Although financial institutions basically perform the same functions within payments, there are essential differences that must be recognized and reflected in the rules. There are differing issues across large and small banks, as well as credit unions. It is our belief that community banks, bankers’ banks, processors, credit unions, corporate credit unions and other stakeholders will find the value proposition reflected in participation within rules creation and maintenance processes.

- E6: the proposal has indicated the type of hardware that a provider will require and the considerations that may guide a provider should it need to obtain further resources. In order to draw up a more detailed and accurate estimate of the investment that a provider would need to make, we would need to know more details about that provider’s infrastructure and its preferred hardware vendors. The criteria do not disclose any of those details.

- E7: Tereon is already designed to interface with a provider’s existing tools to support exceptions and investigations, tools that the provider already knows how to use. This is a central design aim of Tereon’s ability to integrate with existing tools and systems by way of its APIs. We can, of course, create new tools and monitoring services if required to do so.

- S1: the proposal states and shows in several locations that Tereon can integrate to any number of settlement systems, whether these systems exist at the time of implementation or come into being at some point in the future.

- S3: Tereon’s settlement mechanism, whether provided by Tereon or provided by a combination of Tereon overlaying an existing settlement mechanism, provides a means to enable a recipient to receive funds in real time as soon as the transferor or payer has authorized the transfer or payment and to secure those funds for settlement. There is no need to define or deem a transfer or payment as final, as can be the case with existing systems. This will be reflected in the final governing rules and agreements.

- S4: where the proposal correctly states that a suboptimal approach would be to overlay Tereon on to an existing designated-time net settlement (DNS) system, that does not necessarily mean that Tereon would forfeit the certainty that it could otherwise provide to a settlement system, or that such a settlement solution would present settlements risks. Rather it simply means that the combination of Tereon and an existing settlement system would incur higher operational costs than a system based on Tereon alone.

  The proposal details some of the methods that could be put in place to manage intra-day credit or liquidity should it prove necessary to do so, such as where Tereon is overlaid on to an existing DNS system.

- S5: the proposal sets out the procedure by which the rules and agreements will be created in order to take into account any of the requirements that the relevant regulatory agencies may have or raise regarding the solution as proposed by the Task Force. The working paper "*Risks in Faster Payments*", by Julius Weyman of the Federal Reserve Bank of Atlanta, mentions just some of the agencies that will regulate aspects of any faster payments solution.

  The proposal does make it clear that the rules will cover the matters set out in the criteria. The proposal includes the provision for rules and complementary sets of agreements. The rules would provide the overarching allocation of liabilities with the assignment of responsibilities among the parties. These rules would be supplemented with agreements; 1) between the solution providers and their users and 2) between the financial institutions and their customers. The supplemental agreement sets would specify how the various parties would satisfy their respective responsibilities as defined in the overarching rules. For the reasons given below, it is presumptuous to attempt to impose a set of rules or agreements at this stage.

- S6: sharing elements of key data to support identification of fraudulent activity may or may not be allowed by the agencies. In some jurisdictions, such sharing is prohibited unless that data is completely anonymized and pre-approved by the agencies.

  The proposal makes it clear that Tereon will support the sharing of any data, including data that has been anonymized, where it is lawful to do so. If a solution mandates that information must be shared without first clarifying that it is lawful to do so, then that would render such a solution unusable where such sharing is prohibited.

- S7: the proposal makes it clear that the rules and agreements will define the participation requirements that pertain to physical and environmental security, managerial policies, operational security, monitoring, and incident response. The proposal includes the provision for rules and complementary sets of agreements. The rules would provide the overarching allocation of liabilities with the assignment of responsibilities among the parties. These rules would be supplemented with agreements; 1) between the solution providers and their users and 2) between the financial institutions and their customers. The supplemental agreement sets would specify how the various parties would satisfy their respective responsibilities as defined in the overarching rules. For the reasons given below, it would be presumptuous to attempt to impose a set of rules or agreements at this stage.

- S11: the process set out in the proposal will result in a participation agreement that is supported by the Faster Payments Task Force, rather than an agreement that is imposed without any thought as to its suitability and sustainability. The participation agreement poses some questions that remain unanswered by the published criteria. What qualitative restrictions, if any, will the agreement contain? Will providers that cannot offer credit be allowed to participate in the solution? These and other issues must be decided by the Faster Payments Task Force before the participation agreement can be drafted. It would be presumptuous to attempt to impose a participation agreement at this stage, though we can use our standard license agreement as a foundation for such a participation agreement, as we state in the proposal.

- F4: the availability of a real time settlement system would eliminate the credit and liquidity exposure for providers, as the proposal explains. It would remove the need for a provider to provide credit to participate in the solution. The working paper "*Risks in Faster Payments*" quotes from a report by the Reserve Bank of Australia that states that –

  "[a] second benefit of the removal of the need to provide credit would be to facilitate participation by entities that would not be in a position to provide credit."

Turning to the other type of criteria, there are many questions that still need to be answered. We know that there is a keen appetite from many users of payment services for new, more secure, more cost-effective, real-time services. But what about the settlement and clearing levels?

Will existing settlement houses wish to upgrade to real-time settlement processes? Is there room in the market for a new real-time settlement house? Will operators of existing rails consider using Tereon to upgrade those rails to a real-time process? Will existing rails, or new rails under implementation, support interoperability with other new rails? Is there room in the market and sufficient support from institutional users for new, truly real-time rails?

We suspect that our proposal has been marked down for lack of clarity on rules. However, our passionate belief is that rules should be developed in a collaborative process involving all stakeholders including the multiple regulatory bodies. Clarity is certainly provided when providers of new rails impose their rules. That short term benefit is perhaps represented in the QIAT assessment. In the longer term however, lasting value derives from a collaborative process rather than an imposition. That collaborative process will deliver a comprehensive set of rules and agreements that every stakeholder will "own".

As mentioned above in the point dealing with S5, the working paper "*Risks in Faster Payments*" mentions just some of the agencies that will regulate aspects of any faster payments solution. Any rules or agreements to handle participation, consumer protection, privacy, disputed payments (including any rights granted to the users) and so forth must, at a minimum, comply with any regulations drawn up by those agencies, or be agreed with those agencies. As those agencies have yet to draw up regulatory provisions to govern faster payments, and have yet to examine the solution proposed by the Faster Payments Task Force (as the Task Force has yet to publish its final proposal), it would be presumptuous to attempt to impose a set of rules or agreements at this stage.

At this time of writing, we do not yet know where our proposal sits in relation to all of the other proposals. We have no doubt whatsoever that our Tereon software can be deployed to deliver a "very effective solution" against all 36 criteria. It relies simply on the completion of commercial discussions, and processes (like rule-making), that we or the Task Force have in hand. We look forward to further engagement with the Faster Payments Task Force to support that assertion and to explore how it might be achieved.

With grateful thanks,

The proposers

KALYPTON PROPOSAL

TASK FORCE ASSESSMENT COMMENTS

Please share your concerns about this proposal's assessment against the Effectiveness Criteria.

My concerns are with the legal and governance effectiveness criteria. The partnership with ECCHO and the use of their electronic check presentment rule as a foundation for the legal structure of the faster payments solution is a work-in-process. None of these criteria should be rated as being "effective."

Same issue with Governance - G1 and G2. How can these be rated "effective" when there is an acknowledgement that Kalypton will work with ECCHO to develop a governance framework?

Their solution is not suitable yet for the US market.

The proposal is not in conformance with the requirements of a full solution proposal. The requirements were designed to ensure that McKinsey and Task Force time and resources are focused on end-to-end solution proposals that can be thoroughly and credibly assessed against the criteria. This proposal does not meet the requirements. Proposal has answered all sections of the template but in many cases the response does not provide information that would allow the QIAT to evaluate the proposal. The Proposal Template included instructions for Part C: Self-Assessment against Effectiveness Criteria that asked proposers to include a "detailed discussion of why the rating is justified and how the solution meets each criterion" (page 22 of template). It does not include specific information in Part C as to how or why the proposed solution meets each of the criteria. As a result, the QIAT is unable to evaluate the solution with the information provided. Altering the existing process defined to offer an opportunity for the proposer to include more explicit information in its submission to make the proposal "assessable" would be unfair to proposers who provided complete proposals before the submission deadline. A few of the reasons why the proposal did not meet the requirements are as follows: The solution's rules have not been developed for participation, policies, regulations, or operations.

Please submit any comments about this proposal's assessment against the Effectiveness Criteria.

It is not clear who would develop and run the system.

Speed with no security or usability tradeoff. Rails, toolkit, 31 services. Multiple standalone services operated by providers provide failover capability. Systems linked via directory. Single real-time transaction moves funds over Internet or mobile networks. Settlement via settlement accounts at FIs. Not restricted to bank accounts. Push and pull transactions. Blockchain-like auditability. "Millions of transactions per second." Partnered with ECCHO for governance. All use cases including cross-border. Unclear whether UX included. Appears to have strong value proposition. Directory might drive interoperability.

Interesting solution. Appears to have met many of the effectiveness criteria –serves banked and unbanked customers, use of directory, multi-currency payments, and more. Concern about lack of KYC and AML requirements.

An impressive solution. Observations include Accessibility/ubiquity is rated as Very Effective, but in U.1.1, Tereon does not demonstrate how the solution would reach all payees within its closed solution.

Based on the information that Kalypton can currently provide, I feel the QIAT assessment was right on target—to the credit of the McKinsey team.

I think McKinsey got the Kalypton proposal correct. They appropriately recognized not only the solution that was put forth, but also the work that Kalypton had done with ECCHO to establish a legal and governance framework.

The proposed solution offered not defined legal framework within the solution to be "effective."

Accessibility is rated too highly, as proposal does not demonstrate how the solution allows users to reach any and all payees, nor how widespread adoption will be achieved – 2 key criteria for accessibility/ubiquity. Settlement approach appears to be rated too highly (in comparison to other proposals) as settlement outside of those participating in the closed loop is not well defined. Disputes and rules are rated too highly as they are not written cannot be evaluated at this time.

The QIAT correctly identified several difficulties with this proposal's implementation plans, but included them under "Proposer's Ability to Deliver." These issues should have been called out in the section "Areas for Improvement."

Strongly Agree that Kalypton has been appropriately assessed against the Effectiveness Criteria. They proposed a rail-based, real-time, innovative solution with a full transaction processing engine, "rails," comprehensive base lines, and 31 use cases with push and pull capabilities. Provides distributed authentication of private ledgers, configurable to a full range of devices and cases and transaction types, power and flexible processing tool. It is not a blockchain or legacy system, and not a central payments hub. The solution delivers all of the anticipated benefits of the block chain, but without the delays and process overheads that blockchain entails. Supports the banked and unbanked ("regulations & legislation will determine the services that the banked and unbanked can access, not the technology"). Scalable—"millions of transactions per second" on commodity servers ("Teron Server") and will work with ECCHO for legal framework and process of securing patents.

Inclusion of unbanked individuals is a plus but somewhat offset by a difficult to follow set of technical specs. Still, I believe the QIAT got it right.

(1) Don't have to be a bank customer (2) Supports unbanked (3) Funds regulated in banking environment (4) Can switch providers as end-users with account history following end-user (5) does not expose personal data (6) uses directory lookup service to route payments between providers (7) Supports multi-currency payments (8) could generate efficiencies for bank operations (9) can build integrations into different systems (10) can process fractions of a penny.

Agree that the solution is very robust and very effectively meets most requirements. It does, however, lack details on some critical pieces such as implementation and adoption. In general, I am concerned that the vast number of players necessary to adopt for successful widespread usage may not be achievable in a reasonable timeframe.

S.4. Settlement approach should be “very effective,” and not “effective.” The system creates a system that allows transactions to settle via both banks (for banked consumers) and via Tereon server to a clearing house (for both banked and unbanked). They system may contemplate an additional method for DNS, but the preferred method (settlement accounts inside partner banks) will function adequately. We like that settlement risk can be handled even if there is no payer or payee bank, as long as the participant has registered in to the system prior to the transaction.

L.3. Consumer protections: could be “very effective” were it to be the case that the system did not allow for some batch processing. That could lead to overages, costs a cascade of overdraft charges in cases where payer banks still allowed for overages and implemented a fee in those situations. Still, the system does allow for reversal when there is no evidence of good funds. Nonetheless, the fact that ECCHO served on the legal committee of the FPTF suggests that the proposers are committed to protecting the interests of consumers.

G.2. Inclusive governance should be “very effective.” We give great weight to proposals that call for the governance body to be populated with consumer representatives. Some solutions have put forth the idea that only industry needs to be at the table. We applaud Kalypton for making this commitment from the outset.

F.4. Fast settlement among depository institutions and regulated non-bank account providers: We support the “effective” rating. However, we think this rating reflects aspects of a solution that is both “very effective” and “somewhat effective.” For example, if the service does not work 24-7-365, then it is not effective to the standards of the FPTF. But because it is the case that the inconsistent settlement is a product of participant FIs, it is not very fair to downgrade the whole system just because of the lack of advancement among some partner institutions.

While legal framework and rules have not been specifically identified and realistically cannot be fully identified at this point in the faster payments arena, having ECCHO be part of this solution supports the ratings in that area since they are a payment rules entity.

Kalypton Group's proposal is somewhat vague on the matter of security, declaring that they do not depend on any of the existing security schemes, but not making clear how they will assure security of transactions. The claim of 10-millisecond transactions doesn't seem feasible but without a clear description of what elements of the transaction are included (e.g. clearing? settlement?) it is hard to evaluate. The proposal that a single, private organization would handle all directory matters is unlikely to be accepted by many paying and receiving institutions. While their statement that the transaction and the audit happen simultaneously is in a technical sense true of a hash chain approach, it is unlikely that it would pass muster with existing audit practice enforcement organizations. Their 30 use cases seem to cover the field well.

TASK FORCE SOLUTION-ENRICHING COMMENTS

Ubiquity

Thank you for your submission to this effort. I felt your design was well conceived operating within the existing regulated banking network and with very robust redundancy capabilities.

Kalypton is to be congratulated on the development of a robust, flexible system. However, lack of implementation requirements and ancillary costs make adoption levels unclear.

The solution relies on a Tereon ID, which appears to be a proprietary implementation using email address, etc. Would it be possible to just implement based upon email and take away the proprietary nature of the IDs? I see this as furthering interoperability and adoption.

I struggle with the ability to make the solution work in today's payment world. Currently, a few core service providers control a lot of what products small and medium financial institutions are able to provide. The use of the Tereon solution relies on these organizations to provide access to bank FIs' core data through APIs. To date, these companies have been unwilling to do this without significant compensation choosing instead to provide their own solutions. I would like to see a road map for how you will be able to work with these core providers in rolling out your solution and thus have it used by small to medium-sized financial institutions.

Credit to Proposer that the solution provides multi-use of mobile, ATM, eComm and face-to-face with a POS answer.

The solution could be enriched by providing information on how the solution will interoperate with other faster payment systems. Also, a roadmap on how the solution would achieve adoption amongst end-users would enrich the proposal, given the use of private-block chain technology is being utilized in the proposal.

I really believe that this proposal embraces ubiquity and I want to commend this proposal for thinking about all users. Allowing downstream non-financial institutions to participate, in appropriately limited ways, is a very nice addition.

Provide more information on how a payer can reach any account throughout the US to pay any other individual. If each node may have a different relationship with its bank and implement different processes and messages, more fully describe how each entity knows what to expect and how to integrate that with the rest of their systems

This is one of the stronger proposals submitted. Well thought out and strong when measured against all criteria. More clarity around how the Tereon solution will interface with other systems and FIs.

Very Effective across the board and categories.

Need core providers to be on board with this solution as well as their FI customers.

The elements of your solution in this area are very strong. The abilities to have various settlement methods and support multiple currencies are great features.

Even though this proposal scored very highly on all aspects of the Ubiquity criteria, I don't see a high level of ubiquity being achieved for "casual" consumer payments or less structured types of business payments. Requiring registration and a bank account (or similar type of account) for the most efficient use of the system creates an obstacle for those who may prefer to remain unbanked or underbanked. There is a P2P use case described where the recipient is unregistered, but it appears to require a fairly cumbersome and "unfriendly" process—and relies on being able to find a "Tereon merchant" that is convenient to the recipient. A relatively good saturation of Tereon merchants would be required to make such a use case practical. A use case describing how the system might be utilized in the ATM channel, including transferring and receiving of cash, would be helpful to better understand how the system will function outside of a business payments environment.

Efficiency

Describe how one financial institution (or one end-user) will know what information is flowing with a payment from another node – and how to deal with it when it is received (and/or to be able to anticipate what information to receive and have their systems ready for such).

It would be helpful if Kalypton can articulate the value proposition for FIs in order to ensure a fast or timely adoption of the solution.

Very Effective & Effective across the board and categories.

Requires access to provider core accounts via API—will core providers for smaller and medium-sized FIs be willing to do this? What is their motivation?

Uses existing settlement methods.

Seems very time intensive.

It was not clear to me if new accounts would need to be created by users or if existing bank (or bank-like) accounts would be used.

Safety and Security

Describe how counter-party risk is managed when money is flowing in and out of Tereon accounts. Describe more fully who specifically would operationally run the system.

Very Effective across the board and categories and with S. 11 Participation requirements – being the only category rated Somewhat Effective, pending the “participation rules.”

Regarding S.9., it is difficult to determine how well the solution satisfies the criterion given the vague reference to the fact that it is part of Terion's design. I'd ask for more details in order to truly ascertain the level the solution satisfies the criterion.

There could also be more details related to user authentication. It appears that the solution allows providers to set levels of authentication, but it would seem that the solution should have a minimum standard of some sort for user authentication.

Speed (Fast)

Real-time answer, which is high on priority of faster payments.

The solution could be enriched to incorporate a more real-time settlement for/between participating financial institutions.

Very Effective across the board and categories.

The flexibility of the system for different types of settlement options is good. The ability to perform both push and pull transactions may be very helpful. The proposal does seem to leave open potential concerns for settlement delays. In the ATM channel, this could create significant challenges. Consumers are already complaining about added transaction time for EMV.

Legal

Not an enriching comment, but thank you for addressing the legal framework within your proposal.

The solution could be enriched by addressing the overall legal framework, payment system rules, consumer protections and data privacy, as opposed to referencing agreements between various parties, which tend to be unique to each financial institution.

Describe how the system capabilities support the rules which will be developed in the areas of exceptions, disputes.

Effective across the board and categories.

Governance

I appreciate you addressing a governance framework within your proposal. To the extent that you can ensure that small to medium-sized financial institutions have an equal and fair voice in whatever process is created would be beneficial.

The solution could be enriched by providing a more defined governance model.

Overall I think the governance structure was adequate. From an end-user perspective, leading with ECCHO as a rule-making partner was somewhat troubling at the beginning as that is the antithesis of an inclusive body. That being said, the Board of Directors was mentioned as being inclusive. My question is how inclusive is inclusive? 1 seat for end-users and consumer groups and 10 or 20 for others? While I understand that locking in expectations is dangerous, providing some floor as to the expected involvement for each group would be helpful.

There are also some questions about the substructures. Will these be mandated to be inclusive as well?

Tereon's proposed governance structure appears to adhere to the principles outlined in the FP criteria. The proposal explicitly calls for a board of directors comprised from a wide range of stakeholders including merchants and consumer groups.

Effective across the board and categories.

Faster Payments Answers to Respondents’ Comments & Questions

Proposer: Kalypton Group Limited and The Electronic Check Clearing House Organization

APPENDIX B: QUESTIONS AND COMMENTS FOR PROPOSER

Kalypton and ECCHO thank the FPTF and SPTF members who took the considerable time required to read and comment on its proposal. Kalypton would like to make some general comments before responding directly to selected observations.

GENERAL COMMENTS

The QIAT assessment

Kalypton notes that 94% of respondents agreed or strongly agreed with the assessment of its proposal. Three respondents thought the solution over rated; and the reasons for that seem to centre on the issues of rules, governance, adoption, and technical maturity. Kalypton would like to deal with each of those issues in turn.

Conversely, Kalypton believes that its proposal was underrated in a couple of key technical areas, certainly in comparison to other proposals. Kalypton articulated that concern in its response to the second QIAT assessment. One or two respondents commented in similar vein.

Technical capability and maturity

Tereon’s technical capabilities go beyond pure payments. Tereon offers benefits in e.g. post-trade settlement, in digital transformation for banks with complex legacy environments, in helping users to dynamically manage their environment and transaction processes, and in helping organizations to extract full value from their customer data while preserving their customers’ privacy. Kalypton demonstrated a prototype of its post-trade settlement solution on November 22, 2016 at the finals of the Dassault Systèmes 3D FinTech Challenge 2016, which it won. This talks to the return on investment for adoption by banks.

The first version of Tereon has been running successfully in the field in Africa for approximately eight years. Version 3 was demonstrated at the Capability Showcase running a subset of the 31 use cases in our proposal including payments P2P and merchant, phone to phone, card to card terminal and phone to card terminal, with dynamic currency conversion and with a back end running thousands of transactions per second on a laptop. A prototype of version 5 was demonstrated two months ago, and will be available for proof-of-concept exercises within a few months. Certain capabilities are patent pending, including the mechanisms by which Tereon achieves its speed and throughput.

Rules and governance

The Task Force members seem to diverge quite sharply in this area. Some comments marked the proposal down for failing to impose rules. Others commented that the proposed approach is in the spirit of the Task Force as they see it.

Quite simply, the goal is that ECCHO applies its proven consensus building model to create appropriate rules. Kalypton also anticipates that ECCHO could form the basis of the governing body for the new scheme or schemes, albeit with a membership and Board that reflects the wider range of stakeholders in the new faster payments system.

While it may seem advantageous to have rules already written – for the review of Task Force – it is far better to have experts from all around the industry contribute to the writing of the rules. Ultimately lawyers write the rules since they are legal agreements, but lawyers do not know the technical, operational, and business considerations that can impact rules. A collaborative environment including business people, technicians, and legal enables more effective and equitable rules. Because the process will include many voices the rules will be intentionally interoperable.

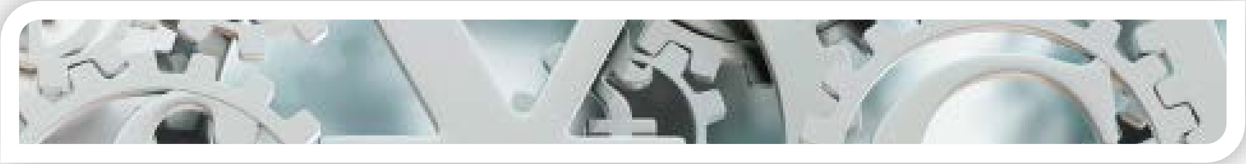
The path to ubiquity

Kalypton agrees with many commentators that adoption is a major challenge. The industry is large, highly fragmented, and heterogeneous. Adoption is a challenge, even for very well-funded organizations owned by the major banks. Kalypton also notes that a new scheme is unlikely to be mandated by government or regulators. It recognizes the “high bar” to certain types of public sector engagement.

However, Kalypton notes that the major banks are not necessarily averse to supporting another new scheme if the return on investment is sufficiently attractive. Kalypton is fortunate that it is already in discussion with some of those banks to offer them support in markets other than US domestic payments. Kalypton also seeks to further explain its proposition to smaller financial institutions, to merchants, to corporates, and to non-bank PSPs targeting the unbanked, the underbanked and other niche populations or applications.

An important part of Kalypton’s developing strategy is to set up one or more proof-of-concept exercises. Kalypton intends to start with three or four banks with a phased program to encompass domestic payments, international payments, and post-trade settlement for transactions in other digital assets. Over time, Kalypton intends to expand or complement this by engaging with other stakeholders in each of the segments. These exercises will demonstrate the security, scalability, cost effectiveness, and flexibility of Tereon. This will not ensure widespread adoption but, together with consensus driven rules, an inclusive governance model, and interoperability with other new and legacy schemes, it will go a long way towards achieving that goal.

Kalypton invites Task Force members to provide input to its plans and to explore participation in this preparatory work. Kalypton commits to sharing the results of these exercises with the Task Force (or any successor organization).



RESPONSES TO SPECIFIC QUESTIONS AND COMMENTS

The following section sets out the proposers' comments to specific comments and questions raised by some Task Force members. The comments and questions are set in italics to distinguish them from the responses. The segment from which the comment or question came is set in blue in square brackets.

Concerns about this proposal's assessment against the Effectiveness Criteria

1 [Other Stakeholders] *It is not clear who would develop and run the system.*

Kalypton proposes establishing a new organization to deploy the technology capable of pull and push payments with a fully inclusive governance model. The fact that Tereon deploys a mesh architecture rather than hub and spoke structure, simplifies the challenge compared to legacy systems and schemes.

In a hub and spoke environment, a financial institution or other payments service provide would either need to connect to each hub and spoke system that it intended to use, or connect via a routing organization for each of those systems. Tereon's mesh architecture is different. Once a financial institution or other payments service provider is connected to Tereon (it either operates a service or accesses a service operated on its behalf, as outlined below), that organization can connect to and transact with any other Tereon user. It can also access any other service that interconnects to Tereon. As an example, in one proof-of-concept Kalypton connected Tereon to an EMV Gateway, which enabled the Tereon operators in that proof-of-concept to both interconnect with each other and to transact with EMV users on the EMV systems.

Kalypton expects that, where possible, each financial institution or other payment service provider will operate its Tereon service under the rules and agreements set by the governance organization. Tereon is designed to be operated by an organization of any size. If an organization cannot operate, or does not want to operate, a Tereon service, then an aggregator or other intermediary can operate and provide a Tereon service on behalf of that organization.

Kalypton, itself, will develop the system, However, it will work with established systems integrators to help organizations implement and launch the system. Kalypton does not intend to be a payment service provider, and so will not act as a restriction of the speed with which financial institutions and other payment service providers can provide Tereon-based services to their customers. Financial institutions and other payment service providers will operate the system and interconnect with each other on an ad hoc basis. Kalypton is, however, prepared to become a payments service provider should this become necessary.

2 [Other Stakeholders] *Interesting solution - appears to have meet many of the effectiveness criteria - serves banked and unbanked customers, use of directory, multi-currency payments, and more. Concern about lack of KYC and AML requirements.*

Tereon does not specify KYC or AML requirements as these are for the regulators to specify. Instead, Tereon is designed to support existing AML and KYC requirements as these are currently defined, and to be extensible so that it can continue to support these requirements as they develop further in response to perceived threats and requirements. One feature that enables

Tereon to do so is its extensible data formats. Another is its ability to provide tailored data feeds to third party analytical engines and tools. Tereon is designed to be extensible so that it can meet future requirements as they arise; it will not restrict organizations to legacy tools or systems.

3 [Other Stakeholders] *Kalypton Group's proposal is somewhat vague on the matter of security, declaring that they do not depend on any of the existing security schemes, but not making clear how they will assure security of transactions. The claim of 10-millisecond transactions doesn't seem feasible but without a clear description of what elements of the transaction are included (e.g. clearing?; settlement?) it is hard to evaluate. The proposal that a single, private organization would handle all directory matters is unlikely to be accepted by many paying and receiving institutions. While their statement that the transaction and the audit happen simultaneously is in a technical sense true of a hash chain approach, it is unlikely that it would pass muster with existing audit practice enforcement organizations. Their 30 use cases seem to cover the field well.*

The mechanisms by which Tereon achieves its speed and throughput are subject to patent applications, and Kalypton cannot yet divulge those mechanisms here. Kalypton did demonstrate a prototype of its settlement solution on November 22, 2016 at the finals of the Dassault Systèmes 3D FinTech Challenge 2016 in a ‘black box’ demonstration, which kept all the confidential mechanisms hidden but which demonstrated the results that Tereon could achieve.

The proposed directory service does not contain the names and bank account details of any user. Such a system would present severe privacy issues. The directory service instead simply directs the financial institution or other payments service provider that one side of a transaction uses to the financial institution or other payments service provider used by the other party to a transaction. It combines the functions of an alias directory, a lookup directory, and a routing directory, without disclosing personal data or account data. It simply contains the Tereon IDs, the services for which those IDs are registered, and the ID and addresses of the Tereon systems of the financial institution or other payments service provider that processes each service for each Tereon ID. Neither party to a transaction need know the financial institution or other payments service provider that the other uses. Neither party need know the account details, or indeed the names, of the other party. The directory service, when used in conjunction with or supported by Tereon’s settlement mechanism, allows Tereon to authenticate, authorize, and clear a transaction in real time. See, for example, page 36 of the proposal (page 37 of the combined document) and the use cases on pages 60-99 of the proposal (pages 61-100 of the combined document) for examples of both pull and push transactions.

The proposal only sets out one option for operating the directory service, though it does hint at others. Another option, for example, is for 12 organizations to operate the directory matters in a structure that resembles the coverage of the Federal Reserve Banks. A third option may be for one or more organizations to operate the directory matters for each State or territory. The structure is still open for discussion and Kalypton believes that this will be agreed by the organization that will govern the system.

What is important is that the organization or organizations that manage the directory matters do not see any of the transactional data that passes between the paying and receiving institutions. All that the directory service does is point the paying institution to the receiving institution, and enable each to validate the other’s identity. Thus, regardless of who operates the directory service, only the parties to a transaction, and others authorized to do so, will see the transaction data. This is a central to Tereon’s design.

The audit system is designed to remove the temporal gap between a transaction and the audit record for that transaction. It is this temporal gap that bedevils the legal treatment of records generated by computer systems. The information contained within the audit for an institution will be that required by both the institution operating the system and the regulators who may require to examine those records. The difference between existing systems and Tereon is that Tereon generates and validates those records contemporaneously with the transaction to which those records relate.

4 [Other Stakeholders] *My concerns are with the legal and governance effectiveness criteria. The partnership with ECCHO and the use of their electronic check presentment rule as a foundation for the legal structure of the faster payments solution is a work-in-process. None of these criteria should be rated as being "effective".*

Same issue with Governance - G1 and G2. How can these be rated "effective" when there is an acknowledgement that Kalypton will work with ECCHO to develop a governance framework?

The Tereon solution will not use the ECCHO Rules for Image Exchange. Those rules are specific to check image clearing and exchange and do not apply to faster payments. New rules will be developed specifically for the Tereon faster payments system. ECCHO brings to the table its experience in creating equitable rules environments that are transparent and inclusive.

One criterion that was missed by the Task Force was the need for cross-solution rules. Given that there are nineteen proposals, it is a good assumption that more than one proposal will be viable and operational. This proposal assumes that there is a need for a set of uniform legal provisions across multiple providers. In the absence of a uniform, cross-solution set of rules, banks and other participants will be subjected to varying sets of warranties, obligations and liabilities which will create uncertainty and confusion and will defeat ubiquity achievement in the near term. In addition, any single provider that has already developed rules will have done so without the inclusion of multiple providers and users and, therefore, will have violated the inclusiveness tenant of the Task Force. It is the proposers' opinion that effective, transparent, inclusive cross-solution rules cannot be developed at this early stage. To create those rules correctly, an inclusive governance process must be implemented before inclusive those cross-solution rules can be developed. The inclusion of ECCHO and its successful rules and governance structure is specifically designed to address these considerations.

The ECCHO legal and governance framework will be used to involve a wide variety of stakeholders in both governance and creation of a fair rule set that appropriately recognizes all. Kalypton could have chosen to create an out-of-the-box rules set. However, it believes that the ECCHO approach is preferable for its customers, stakeholders, and participants. Stakeholders will have input to the rules that will be employed (e.g., large banks, small banks, credit unions, payments processors, consumer groups, etc.). This group will thoroughly discuss the issues to create a better rule set than a set of rules for one specific solution and possibly a limited stakeholder group. This type of solution, with its attendant governance and rules, may take a bit longer to implement but the result is far superior. It also creates a mechanism for update as technology and compliance change across time.

The roadmap for creating the rules is in place and the rules will be developed as the technical elements of the system are implemented.

5 [Other Stakeholders] *An impressive solution. Observations include Accessibility/ubiquity is rated as Very Effective, but in U.1.1, Tereon does not demonstrate how the solution would reach all payees, within its' closed solution.*

Tereon provides a rich set of APIs that enable any financial institution or other payment service provider to incorporate its functionality into its user applications. In this way, institutions and other payment service providers can quickly and efficiently provide Tereon services to their customers using client applications that those customers already have.

Tereon can connect to other new schemes via ISO 20022 or other formats, and to legacy schemes via their message protocols. It has already successfully connected to an EMV Gateway, for example. Kalypton sees no technical difficulty creating an ACH connector, or interfaces with the debit card systems, credit card systems, ATM systems, etc. Therefore, whilst the system evolves its path to ubiquity, transactions can begin in Tereon and complete in another form or vice-versa. Of course, such a transaction would deliver only a sub-set of the benefits that Tereon offers.

The language in the proposal uses the term merchant device. This is a term of art and does not refer to the need to have manned devices. It refers to the functions provided by a device. An ATM that operates Tereon is as much a merchant device as a PoS terminal that operates Tereon. The difference is that the ATM is a self-standing device, whereas a merchant terminal may or may not be operated by a merchant. Financial institutions and payment service providers are not restricted to mobiles or merchant PoS terminals, and can use any number to devices to provide services to both banked and unbanked customers. Tereon can easily be used to form the basis of a new credit and debit scheme.

Kalypton does not intend to be a payment service provider, and so will not act as a restriction of the speed with which financial institutions and other payment service providers can provide Tereon-based services to their customers. Financial institutions and other payment service providers will operate the system and interconnect with each other on an ad hoc basis. Please see the response to comment 1. However, Kalypton is prepared to become a payments service provider should this become necessary.

Concerns about this proposal's assessment against the Effectiveness Criteria

6 [Other Stakeholders] *Accessibility is rated too highly, as proposal does not demonstrate how the solution allows users to reach any and all payees, nor how widespread adoption will be achieved – 2 key criteria for accessibility/ubiquity. Settlement approach appears to be rated too highly (in comparison to other proposals) as settlement outside of those participating in the closed loop is not well defined. Disputes and rules are rated too highly as they are not written cannot be evaluated at this time.*

For the issue of accessibility, please see the response to comment 5, which states that Tereon provides a rich set of APIs that enable any financial institution or other payment service provider to incorporate its functionality into its user applications. In this way, institutions and other payment service providers can quickly and efficiently provide Tereon services to their customers using client applications that those customers already have.

The proposal did not set out a detailed explanation of settlement between a Tereon-based system and a third-party system as that was not requested. However, figure 33 of the proposal (the check payment use case; figure on page 89 of the proposal, page 90 of the combined document) alludes to settlement between two or more separate systems. Here the settlement between two systems, in central bank money or commercial bank money, would occur at the interconnection between those systems, either within a single settlement agent that served both systems, or in a connection between the settlement agents for those systems. If Tereon acts as an overlay for that connection, then it will hypothecate funds that will transfer from the Tereon system to the third-party system and can, if the third-party system supports such function, require the third-party system to hypothecate the funds that will transfer to the Tereon system. This, of course, assumes that the operators of a Tereon service wish to interconnect to a third-party service.

For the issues of rules that are not yet written, please see the response to comment 4.

7 [Consumer Interest Organization] *S.4. Settlement approach should be "very effective," and not "effective." The system creates a system that allows transactions to settle via both banks (for banked consumers) and via tereon server to a clearing house (for both banked and unbanked). They system may contemplate an additional method for DNS, but the preferred method (settlement accounts inside partner banks) will function adequately. We like that settlement risk can be handled even if there is no payer or payee bank, as long as the participant has registered in to the system prior to the transaction.*

L.3. Consumer protections: could be "very effective" were it to be the case that the system did not allow for some batch processing. That could lead to overages, costs a cascade of overdraft charges in cases where payer banks still allowed for overages and implemented a fee in those situations. Still, the system does allow for reversal when there is no evidence of good funds. Nonetheless, the fact that ECCHO served on the legal committee of the FPTF suggests that the proposers are committed to protecting the interests of consumers.

G.2. Inclusive governance should be "very effective." We give great weight to proposals that call for the governance body to be populated with consumer representatives. Some solutions have put forth the idea that only industry needs to be at the table. We applaud Kalypton for making this commitment from the outset.

Tereon supports batch processing, but does so in a way that eliminates the settlement risks usually associated with such processing. Where Tereon must support batch processing, it does so by first verifying that the funds (or an approved credit line) exist to cover a transaction and then hypothecating sufficient funds for that transaction before queueing the settlement instructions. This is the mode by which Tereon will overlay a DNS system to remove the settlement risks otherwise associated with batch processing, as Tereon is designed to support settlement in central bank money or commercial bank money. Tereon does not batch authentication, authorization, approval, and clearing.

8 [Other Stakeholders] *Speed with no security or usability tradeoff. Rails, toolkit, 31 services. Multiple standalone services operated by providers provides failover capability. Systems linked via directory. Single realtime transaction moves funds over Internet or mobile networks. Settlement via settlement accounts at FIs. Not restricted to bank accounts*

Push and pull transactions. Blockchain-like auditability. "millions of transactions per second" Partnered with ECCHO for governance. All use cases including cross-border. Unclear whether UX included. Appears to have strong value proposition. Directory might drive interoperability

Kalypton can provide a set of UX designs and criteria that it designed to show all the features of Tereon. However, financial institutions and other payment services providers are free to use their own UX designs and simply incorporate Tereon into their existing UX designs via Tereon's APIs.

9 [Medium Financial Institutions] *The proposed solution offered not defined legal framework within the solution to be 'effective.'*

Although the legal framework has not been implemented, it has been defined (see figure 1 below). ECCHO's rules development methodology is unique and preferred across the check industry for its transparency and inclusion. ECCHO facilitates grass-roots development of rules from stakeholders. Direct stakeholders participate in all subcommittees and operations committee while indirect stakeholders have sponsoring organizations to represent them. Sponsoring organizations comprise processors, solutions providers, RPAs, bankers' banks, correspondent banks, etc.

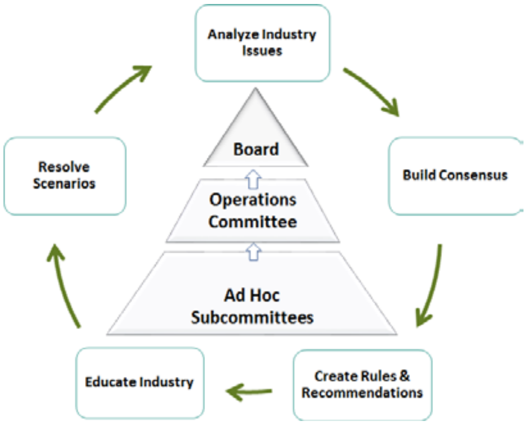


Figure 1 - ECCHO's rule development methodology

The process begins by gaining input from the ground up. Initial discussions begin in Ad Hoc Subcommittees, which are targeted to certain aspects of the rules. Examples of subcommittees might include rules development, exceptions and dispute management, legal and compliance issues, etc. Members discuss how best to address the issues. Subcommittee meetings are teleconferences for the widest participation. ECCHO is experienced at hosting hundreds on a call while still encouraging input from all who wish to voice opinions and offer ideas. Rules drafts are created and refined in subcommittee. Subcommittees operate contiguously for the most efficiency.

Following discussion in subcommittee, draft rules are finalized in the operations committee meeting and sent on to the Board for final approval or sent back to subcommittee for further refinement. The rules language approved in the Operations Committee is the exact rule that proceeds to the Board for approval – no language is ever changed without subcommittee approval. Legal counsel is used throughout the process for rules drafting, legal research, knowledge of existing law, etc.

Solution enriching comments

10 [Non-Bank Providers] *The solution relies on a Tereon ID, which appears to be a proprietary implementation using email address, etc. Would it be possible to just implement based upon email and take away the proprietary nature of the IDs. I see this as furthering interoperability and adoption.*

I struggle with the ability to make the solution work in today's payment world. Currently, a few core service providers control a lot of what products small and medium financial institution's are able to provide. The use of the Tereon solution relies on these organizations to provide access to bank FI's core data through APIs. To date, these companies have been unwilling to do this without significant compensation choosing instead to provide their own solutions. I would like to see a road map for how you will be able to work with these core providers in rolling out your solution and thus have it used by small to medium sized financial institutions.

If a user wants to use his or her email address, and that email address is unique to the user, then that user can use the email address as a credential for Tereon; that email address becomes one of that user's Tereon IDs. The term "Tereon ID" refers to the credential used to identify each party to a transaction. That may be a user's email address (so long as it is unique to that user), a mobile telephone number, a card number, and so on. If the users carry out a transaction with NFC devices, then the credentials could be internal codes unique to each device; a code that the users will not see. The unique or proprietary nature of the internal identifiers that Tereon uses simply ensures that each actor in the Tereon system, be that actor a user or a service, is globally unique. Ultimately, Tereon can plug and play any authentication technique that the customer base requires, including QR codes, biometrics etc. Tereon does not dictate the authentication mechanism, although it does have clear preferences.

Kalypton acknowledges the difficulty that core system providers can represent, and will present them with three options:

- They can write to the Tereon APIs
- Kalypton can write to the core provider's APIs
- They can create a client-side product to connect and support real-time payments

Kalypton will seek commercial terms from the core providers for all the options that they are prepared to contemplate. Kalypton can also interconnect to a different level, such as the services levels that financial institutions build on top of their core systems, if a core provider refuses to supply APIs, write to Tereon's APIs, or create a client-side product.

11 [Medium Financial Institutions] *The solution could be enriched by providing information on how the solution will interoperate with other faster payment systems. Also, a roadmap on how the solution would achieve adoption amongst end-users would enrich the proposal, given the use of private-block chain technology is being utilized in the proposal.*

Please see the responses to comments 5, 6, 10, 13, 15, 21, 22, and 23.

The proposal does not use block chain technology, private or otherwise. Tereon's audit and monitoring system provides distributed authentication while enabling operators to retain their own records themselves in private data stores (or ledgers). Tereon delivers the functionality that blockchain has long promised, but it does not use blockchain technology in any of its guises. To do otherwise would severely limit its performance, extensibility, and its ability to meet legal and regulatory requirements. Tereon offers distributed trust in private data stores (sometimes referred to as private ledgers) rather than the problematic Distributed Ledger Technology (DLT) behind blockchain and other solutions.

12 [Government-End User] *Overall I think the governance structure was adequate. From an end user perspective, leading with ECCHO as a rule making partner was somewhat troubling at the beginning as that is the antithesis of an inclusive body. That being said, the Board of Directors was mentioned as being inclusive. My question is how inclusive is inclusive? 1 seat or end users and consumer groups and 10 or 20 for others? While I understand that locking in expectations is dangerous, providing some floor as to the expected involvement for each group would be helpful.*

There are also some questions about the substructures. Will these be mandated to be inclusive as well?

The proposer's intention to include ECCHO as a rule-making partner was simply to benefit from ECCHO's experience in creating equitable rules environments that are transparent and inclusive, as set out in the responses above. The solution would mandate an equal representation for each of the identified stakeholder groups. If there was to be an unequal representation, then that would most likely favor the merchant and end-user groups as the ultimate users of the faster payments system. Several countries have experimented with such representation and have found that this engenders more respect for and trust in the payments service providers, as it is they who will serve the end-user groups. The substructures will also be mandated to be inclusive.

As for the comment that ECCHO is the antithesis of an inclusive body, ECCHO's rules are interbank rules only. Agreements between financial institutions and their customer are the purview of the financial institutions and not ECCHO. The current ECCHO rules process includes representatives from every segment in the industry involved in inter-bank check image exchange including but not limited to community banks, bankers' banks, credit unions, corporate credit unions, mid-tier financial institutions, large financial institutions, processors, archive providers, settlement providers, network providers, adjustment providers, return providers, the Federal Reserve, etc. This is the most inclusive inter-bank rules organization in the U.S. – including around 3,000 members. The current ECCHO membership for check rules is limited by the Uniform Commercial Code to financial institutions only. Faster payments as envisioned by the Faster Payments Task Force would not be limited in interbank exchanges and would therefore include a broader array of stakeholders.

13 [Other Stakeholders] *Provide more information on how a payer can reach any account throughout the US to pay any other individual. If each node may have a different relationship with its bank and implement different processes and messages, more fully describe how each entity knows what to expect and how to integrate that with the rest of their systems.*

Tereon's APIs can be tailored to each bank's systems and internal data formats. Tereon is designed to be able to interconnect disparate systems, and so is designed to support multiple data formats. It adheres to the mantra of accept a wide variety of inputs, but be strict on any output. An example is its support for ISO 20022. As stated in its answers to the QIAT's questions (pages 7-10 of the answers to the QIAT questions, pages 163-166 of the combined proposal document) Tereon supports far more data fields than declared in the ISO 20022 message formats, and does so for a variety of reasons. The most important reason is to preserve all the data surrounding a transaction, data that may not be reflected in the existing message formats defined under ISO 20022. Tereon will extend the message definitions where necessary to capture that data, and instruct the nodes on how to process that data.

Tereon's support for multiple data formats means that it can interconnect to third party payment systems to enable user on those systems to transact with users on Tereon. One such example comes from Tereon's ability to support ISO 8583, which enabled it to interconnect with an EMV gateway in one proof-of-concept to demonstrate how a Tereon user could transact with an EMV user.

14 [Other Stakeholders] *Describe how one financial institution (or one end user) will know what information is flowing with a payment from another node – and how to deal with it when it is received (and/or to be able to anticipate what information to receive and have their systems ready for such.*

Tereon supports full contextual information for each transaction type. In a domestic transaction, where both nodes to a transaction reside in the same jurisdiction, the transaction type will define the information that each node requires from the other. Tereon will ensure that each node receives the required contextual information. Pages 7-10 and 21-23 of the response to the questions from the QIAT (pages 193-166 and 177-179 in the combined document) set out how Tereon presents the data in a format in that the nodes will understand and so act upon.

If the transaction requires additional information, then the nodes will inform each other of that requirement as part of the handshake that established the transaction, and the nodes will transmit that information to each other.

15 [Other Stakeholders] *Describe how counter-party risk is managed when money is flowing in and out of Tereon accounts. Describe more fully who specifically would operationally run the system.*

Tereon is designed to remove the settlement risks faced by counterparties to a transaction, regardless of whether Tereon acts as the RTGS system or whether it overlays a DNS system. Tereon will only allow a transaction to proceed if the user has sufficient funds or approved credit to cover the transaction. If Tereon operates an RTGS system between the nodes, then it will immediately settle the transaction, thus removing the settlement risks. If Tereon must overlay a DNS system, or a queued RTGS system, then Tereon will hypothecate the required sums needed to settle the transaction, net or otherwise, before queuing the transaction to the settlement process.

The fact that Tereon deploys a mesh architecture rather than hub and spoke structure, simplifies the challenge compared to legacy systems and schemes. In a hub and spoke environment, a financial institution or other payments service provide would either need to connect to each hub and spoke system that it intended to use, or connect via a routing organization for each of those systems. Tereon's mesh architecture is different.

Once a financial institution or other payments service provider is connected to Tereon (it either operates a service or accesses a service operated on its behalf, as outlined below), that organization can connect to and transact with any other Tereon user. It can also access any other service that interconnects to Tereon. As an example, in one proof-of-concept, Kalypton connected Tereon to an EMV Gateway, which enabled the Tereon operators in that proof-of-concept to both interconnect with each other and to transact with EMV users on the EMV systems.

Kalypton expects that, where possible, each financial institution or other payment service provider will operate its Tereon service under the rules and agreements set by the governance organization. Tereon is designed to be operated by an organization of any size. If an organization cannot operate or does not want to operate a Tereon service, then an aggregator or other intermediary can operate and provide a Tereon service on behalf of that organization.

Kalypton, itself, will develop the system, However, it will work with established systems integrators to help organizations implement and launch the system. Kalypton does not intend to be a payment service provider, and so will not act as a restriction of the speed with which financial institutions and other payment service providers can provide Tereon-based services to their customers. Financial institutions and other payment service providers will operate the system and interconnect with each other on an ad hoc basis. Kalypton is, however, prepared to become a payments service provider should this become necessary.

16 [Other Stakeholders] *Describe how the system capabilities support the rules which will be developed in the areas of exceptions, disputes.*

Tereon is designed to work within existing financial services regulations. It does not require a regulatory sandbox, regulatory exemptions, or any other form of special treatment. It is designed to support settlement in central bank money or commercial bank money.

Tereon provides real-time transactions and settlements in its default mode. As the responses above state, Tereon can remove the settlement risks if it must operate with DNS systems (or queued RTGS systems) if it overlays those systems. Tereon is also designed to be extensible and configurable so that it can adapt to meet future requirements. As the rules change, so Tereon can change, if necessary, to conform to and support those rules.

The directory service, when used in conjunction with or supported by Tereon’s settlement mechanism, allows Tereon to authenticate, authorize, approve, and clear a transaction in real time. See, for example, page 36 of the proposal (page 37 of the combined document) and the use cases on pages 60-99 of the proposal (pages 61-100 of the combined document) for examples of both pull and push transactions (please also see the response to comment 3). This reduces dramatically the possibility for consumer disputes, and other clearance errors, such as where a consumer cancels a transaction before it settles, but after a merchant has supplied a good or service.

Most disputes that occur in payments on legacy systems would not occur in Tereon due to its real-time nature. For example, there would be no “returns” in faster payments since a payment is vetted and final once it has been cleared for settlement, all of which occurs in real time. The rules and agreements that will govern the solution will, however, facilitate the creation of an automated dispute system and rules for processing disputes, and will include rules for all types of dispute and errors.

17 [Non-Bank Providers] *It would be helpful if Kalypton can articulate the value proposition for FIs in order to ensure a fast or timely adoption of the solution.*

Tereon removes all settlement lags and provides a financial institution or other payments service provider with an immediate view of its exposure to counterparties. It supports real ‘smart contracts’ than can be revoked or reversed if required. Tereon provides a consistent data format and view across multiple systems. Tereon enables a financial institution or other payments service provider to offer a full set of financial services to existing customers, as well as to the unbanked; it allows organizations to grown their customer base, provides them with a full 360 view of their customers and their customers’ transactions, and allows then to create new services and revenue streams. Tereon can do this for less than the cost of existing payments services.

Tereon’s design will enable a financial institution or other payments service provide to connect to and operate Tereon, irrespective of that organization’s size. This will not only be mandated by the rules and governance structure; it is mandated by Tereon’s design. Tereon is designed to be operated by an organization of any size. If an organization cannot operate, or does not want to operate, a Tereon service, then an aggregator or other intermediary can operate and provide a Tereon service on behalf of that organization.

Tereon implements a mesh environment rather than a hub and spoke environment to simplify the way that financial institutions or other payment service providers can connect to and operate Tereon. In a hub and spoke environment, a financial institution or other payments service provide would either need to connect to each hub and spoke system that it intended to use, or connect via a routing organization for each of those systems. Tereon’s mesh architecture is different.

Once a financial institution or other payments service provider is connected to Tereon, that organization can connect to and transact with any other Tereon user. It can also access any other service that interconnects to Tereon. As an example, in one proof-of-concept, Kalypton connected Tereon to an EMV Gateway, which enabled the Tereon operators in that proof-of-concept to both interconnect with each other and to transact with EMV users on the EMV systems. With Tereon, a financial institution or other payment service provider would only need to connect to Tereon to achieve ubiquity.

18 [Business End Users] *Regarding S.9., it is difficult to determine how well the solution satisfies the criterion given the vague reference to the fact that it is "Part of Tereon's design. I'd ask for more details in order to truly ascertain the level the solution satisfies the criterion.*

There could also be more details related to user authentication. it appears that the solution allows providers to set levels of authentication, but it would seem that the solution should have a minimum standard of some sort for user authentication.

Tereon allows the operator to increase the levels of authentication that the operator requires for a service. However, it does not allow an operator to reduce the levels of authentication below the minimum level set by Tereon. Tereon sets a minimum level of authentication that no operator will be able to reduce.

Tereon is designed to protect the privacy of each user. The exact details are subject to a patent application, but Tereon is designed to meet the needs of the most stringent data protection regimes everywhere it is either running or has been proposed to run and will do the same in the U.S. and across the globe. Tereon simply will not expose any personal data unless the law requires that personal data to accompany the transaction. See, for example, page 36 of the proposal (page 37 of the combined document) and the use cases on pages 60-99 of the proposal (pages 61-100 of the combined document).

19 [Medium Financial Institution] *Requires access to provider core accounts via API - will core providers for smaller and medium size FIs be willing to do this? What is their motivation?*

Uses existing settlement methods

Seems very time intensive

Tereon can provide a genuine RTGS system, or it can overlay existing DNS or queued RTGS systems to provide a functionally equivalent settlement service to that provided by Tereon itself.

Kalypton acknowledges the difficulty that core system providers can represent. As stated in the response to comment 10, Kalypton will present them with three options:

- They can write to the Tereon APIs
- Kalypton can write to the core provider's APIs
- They can create a client side product to connect and support real-time payments

Kalypton will seek commercial terms from the core providers for all the options that they are prepared to contemplate. Kalypton can also interconnect to a different level, such as the services levels that financial institutions build on top of their core systems, if a core provider refuses to supply APIs, or write to Tereon's APIs.

Please also see the responses to comments 7, 17, and 21.

20 [Small Financial Institution] *It was not clear to me if new accounts would need to be created by users or if existing bank (or bank like) account would be used.*

Tereon offers the flexibility to support both scenarios. The choice is that of the financial institution or the payment service provider that offers services to end-users. If that organization integrates Tereon into its core account management systems, then it can offer Tereon as a service to its customers using its existing customer accounts. If that organization decides to offer Tereon as a stand-alone service, then Tereon can provide a full account management system for that organization's customers. Accounts can therefore be, existing or new, bank or non-bank, permanent or one-time use (to send money to the unbanked).

21 [Small Financial Institution] *This is one of the stronger proposals submitted. Well thought out and strong when measured against all criteria. More clarity around how the Tereon solution will interface with other systems and FIs.*

As Kalypton states in its response to comment 5, Tereon provides a rich set of APIs that enable any financial institution or other payment service provider to incorporate its functionality into its user applications. In this way, institutions and other payment service providers can quickly and efficiently provide Tereon services to their customers using client applications that those customers already have.

Tereon can connect to other new schemes via ISO 20022 or other formats, and to legacy schemes via their message protocols. It has already successfully connected to an EMV Gateway, for example. Kalypton sees no technical difficulty creating an ACH connector. Therefore, whilst the system evolves its path to ubiquity, transactions can begin in Tereon and complete in another form or vice-versa. Of course, such a transaction would deliver only a sub-set of the benefits that Tereon offers.

Tereon implements a mesh environment rather than a hub and spoke environment to simplify the way that financial institutions or other payment service providers can connect to and operate Tereon. In a hub and spoke environment, a financial institution or other payments service provide would either need to connect to each hub and spoke system that it intended to use, or connect via a routing organization for each of those systems. Tereon's mesh architecture is different.

Once a financial institution or other payments service provider is connected to Tereon, that organization can connect to and transact with any other Tereon user. It can also access any other service that interconnects to Tereon. With Tereon, a financial institution or other payment service provider would only need to connect to Tereon to achieve ubiquity.

22 [Other Stakeholders] *Even though this proposal scored very highly on all aspects of the Ubiquity criteria, I don't see a high level of ubiquity being achieved for "casual" consumer payments or less structured types of business payments. Requiring registration and a bank account (or similar type of account) for the most efficient use of the system creates an obstacle for those who may prefer to remain unbanked or underbanked. There is a P2P use case described where the recipient is unregistered, but it appears to require a fairly cumbersome and "unfriendly" process - and relies on being able to find a "Tereon merchant" that is convenient to the recipient. A relatively good saturation of Tereon merchants would be required to make such a use case practical. A use case describing how the system might be utilized in the ATM channel, including transferring and receiving of cash, would be helpful to better understand how the system will function outside of a business payments environment.*

The term 'Tereon merchant' is a term of art and does not refer to the need to have manned devices. It refers to the functions provided by a device. An ATM that operates Tereon is as much a merchant device as a PoS terminal that operates Tereon. The difference is that the ATM is a self-standing device, whereas a merchant terminal may or may not be operated by a merchant. Financial institutions and payment service providers are not restricted to mobiles or merchant PoS terminals, and can use any number to devices to provide services to both banked and unbanked customers.

Tereon is designed to support payments to and from any user, whether that user is banked or unbanked, and whether that user has an account with a Tereon-based service. It does not require a user to have an account to make or receive a payment; it is simply more efficient if the user does have an account.

As an example of use case of a transfer by a non-Tereon user to a non-Tereon recipient, if the non-Tereon user (that is a user who does not have a Tereon account, whether banked or unbanked) wishes to transfer funds to another non-Tereon user then the transferor will first go to a Tereon terminal and select the transfer menu. If the terminal can accept cash, then it can be a stand-alone terminal. If not then the terminal will be manned by a merchant, cashier, or some other individual responsible for operating that terminal. The transferor confirms than he or she is

not a Tereon user and enters the recipient’s mobile telephone number as the recipient’s ID. Tereon identifies the fact that the mobile number is unregistered and asks the transferor to confirm that he or she wants to transfer funds to a non-Tereon user with that number. The transferor confirms this and enters the amount to transfer. Tereon detects any prior receipt of funds received, and ensures that the new transfer will not, alone or in aggregate, exceed a reporting threshold.

Tereon asks the transferor to enter the details of the recipient, such as the recipient’s name, address, and other contact details, confirms that these are the same as those registered against that number, and then requests that the transferor submit the correct cash. If the terminal accepts cash, then the terminal will check that the transferor has submitted the correct cash. If the terminal is manned, then the operator will confirm that he or she has received the correct cash and enter his or her PIN.

The terminal will now provide the transferor with the transaction number, a cancellation PIN, and a collection PIN. Tereon will also send the transaction number to the recipient by SMS and email. The transferor will send the collection PIN to the recipient by a separate channel.

If the transferor needs to cancel the transfer before the recipient accesses some or all the funds, then the transferor can do so with the cancellation PIN.

Tereon’s design is modular, and this enables organizations to build services for new use cases by using existing components. The use case above is an amendment to the first part of the use case set out on pages 93-96 of the proposal (pages 94-97 of the combined document). Thus, to build use cases for a non-Tereon transferor to a Tereon recipient, Tereon would use the components that enable a non-Tereon user to initiate a transaction, and the components that enable a Tereon user to receive funds. In a similar way, a user case to support a Tereon user to Tereon user transfer would simply use the components that hat enable a Tereon user to initiate a transaction, and the components that enable a Tereon user to receive funds. Tereon is designed to be flexible, and it is this flexibility that enables it to support the 31 use cases listed in the proposal.

23 [Other Stakeholders] *The flexibility of the system for different types of settlement options is good. The ability to perform both push and pull transactions may be very helpful. The proposal does seem to leave open potential concerns for settlement delays. In the ATM channel, this could create significant challenges. Consumers are already complaining about added transaction time for EMV.*

Tereon is designed to settle transactions between devices in real time, regardless of the device or devices used for a transaction. An ATM is simply one such device.

Tereon removes all settlement lags and provides a financial institution or other payments service provider with an immediate view of its exposure to counterparties. Tereon authenticates, authorizes, approves, and clears a transaction in real time. See, for example, page 36 of the proposal (page 37 of the combined document) and the use cases on pages 60-99 of the proposal (pages 61-100 of the combined document) for examples of both pull and push transactions. Tereon’s ability to support both push and pull transactions in real time is supported by the structure of its directory service, which combines the functions of an alias directory, a lookup directory, and a routing directory, without disclosing personal data or account data. It simply contains the Tereon IDs, the services for which those IDs are registered, and the ID and addresses of the Tereon systems of the financial institution or other payments service provider that processes each service for each Tereon ID.

24 [Medium Financial Institution] *The solution could be enriched to incorporate a more real-time settlement for/between participating financial institutions.*

Tereon is designed to work 24-7-365. It is designed to operate as a genuine, real-time payments and settlements system that enables transactions to settle in central bank money or commercial bank money. As the response to the comments above show, Tereon can overlay a DNS or a queued RTGS system to provide a full RTGS functionality by securing and hypothecating the funds required to settle a queued transaction. In doing so, Tereon can provide a migration path from a DNS or queued RTGS system to a full RTGS system without disrupting the services that it offers.

See also the responses to comments 13, 14, 15, and 21.

25 [Consumer Interest Organization] *F.4. Fast settlement among depository institutions and regulated non-bank account providers: We support the 'effective' rating. However, we think this rating reflects aspects of a solution that is both "very effective" and "somewhat effective." For example, if the service does not work 24-7-365, then it is not effective to the standards of the FPTF. But because it is the case that the inconsistent settlement is a product of participant FIs, it is not very fair to downgrade the whole system just because of the lack of advancement among some partner institutions.*

If an institution cannot operate on a 24-7-365 basis then Tereon can still support that institution without any detrimental effect. For example, if the institution has a pre-approved exposure level that is backed by a secured credit facility, then Tereon can continue to process and settle transactions to and from that institution so long as the exposure of that institution does not exceed a pre-approved level. This will be hypothecated credit within that institution's secured credit facility. Once the institution opens again, it will clear and settle its settlement exposure from its credit facility. Tereon will not allow users or institutions to make a transaction where they do not have the funds or approved credit to cover that transaction.

26 [Medium Financial Institution] *The solution could be enriched by addressing the overall legal framework, payment system rules, consumer protections and data privacy, as opposed to referencing agreements between various parties, which tend to be unique to each financial institution.*

Please see the response to comments 3, 4, 9, 12, and comments to the QIAT assessment.

Additionally, this proposal proposes to use the ECCHO model for Rules and Governance. Under that model, ECCHO would provide a uniform, cross-solution set of rules to address legal provision that are common to all solutions. Each solution would also provide the supplemental agreements with its users that are needed to support its individual solution but that do not conflict with the uniform rules. Likewise, each financial institution or other payment service provider would provide its own complementary agreements with its customers.

27 [Non-Bank Provider] *I appreciate you addressing a governance framework within your proposal. To the extent that you can ensure that small to medium sized financial institution's have an equal and fair voice in whatever process is created would be beneficial.*

Please see the response to comments 3, 4, 9, 12, 26, and comments to the QIAT assessment.

Additionally, the current ECCHO governance structure includes a community bank representative and a credit union representative. While the details of the ECCHO Faster Payments governance have not been finalized, it is anticipated that it would be at least as inclusive as is the current ECCHO governance structure.

28 [Medium Financial Institution] *The solution could be enriched by providing a more defined governance model.*

Please see the response to comments 3, 4, 9, 12, 26, and comments to the QIAT assessment.

Faster Payments QIAT

FINAL ASSESSMENT

Property of the Federal Reserve Bank of Kansas City and the Federal Reserve Bank of Chicago (“Banks”)

Not for distribution or publication without the express written permission of the Banks

Faster Payments QIAT

FINAL ASSESSMENT

Proposer: Kalypton Group Limited and the Electronic Check Clearing House Organization

Summary Description of solution:

The proposer describes Kalypton's solution, Tereon, as a "full transaction processing engine, not just a payment platform" (p.104). The proposer further describes a technology delivering blockchain-like capabilities. As such, Tereon does not provide a distributed ledger; rather, it provides distributed authentication of private ledgers. The identified challenges of distributed ledger technology (DLT) — including scalability, security, privacy, interoperability and sustainability—thus do not affect the solution.

Tereon consists of a "bank-grade" central core (p. 6) that is fully integrated into the banking system. A highly configurable software layer sits on top of the core platform.

Tereon is a powerful, flexible transaction processing solution that moves funds from account to account in real time. The solution supports real-time payments using internet-enabled sessions or mobile data networks. The solution requires access to providers' core accounts via an API. The solution is available to banks and non-bank providers and will support the unbanked. It provides a tool kit to facilitate ongoing innovation by providers and other third parties. All use cases are enabled at launch. Kalypton is in the process of deploying its first commercial implementation of Tereon in Central America.

The proposer advises that certain details regarding the technology to be deployed are only available under NDA (non-disclosure agreement), as the information is still the subject of patent applications. For this reason, the solution's full details are not available for assessment.

.

EXECUTIVE SUMMARY OF THE PROPOSAL

- **Major strengths**
  - The solution is flexible and can be configured to support all transaction types and multiple currencies. It has been designed to serve the banked and unbanked. Tereon facilitates payments to and from all types of accounts and is able to support all use cases at launch.
  - The solution requires that all funds and funds transfers operate within the regulated banking environment to ensure that funds are protected and regulated.
  - Tereon is a secure solution that supports device and user authentication for every session and transaction as determined by the provider.
  - The solution consists of multiple, standalone Tereon systems operated by providers. The failure of one server does not affect the overall network of servers, and the network should be available 24x7x365. Using a directory system, the solution can connect any authorized user on one system to transact with any authorized user on another system. Tereon can associate multiple devices and multiple users with a single account, and it can associate multiple accounts (in different currencies) with a single device.
  - The solution does not expose any personal data during a transaction and includes a data access capability to support data management. The solution's first commercial deployment is currently underway in Central America.

- **Areas for improvement and enhancement**
  - The proposal does not define the transaction information to be shared between Tereon servers and banks. It is unclear how much visibility will be allowed into the accounts held on Tereon servers. More details about the flow of information within and between providers, as well as requirements related to risk management, would be helpful.
  - Few details are provided regarding the infrastructure required or the accounts that providers must create and manage to support Tereon.
  - The proposal describes settlement within the solution as hypothecation of the transaction funds to a Tereon settlement account. Non-banks must set up “control accounts” at FIs to manage the movement of funds. Ultimately, settlement between FIs occurs using the providers’ existing settlement mechanism(s).
- **Use cases addressed**
  - The solution addresses all four major use cases (P2P, P2B, B2P, and B2B) and includes cross-border capabilities.
- **Proposer’s overall ability to deliver proposed solution**
  - This proposal is well thought-out and considers the Faster Payments Task Force’s requirements. The solution relies on access to existing end-users’ or providers’ bank accounts and leverages existing settlement capabilities. Tereon delivers value by enabling faster, more secure, lower-cost transactions.
  - The proposal does not describe the investment and implementation effort required for provider participation.
  - The solution includes technology that is subject to a patent application. As a result, the solution’s technology has not been fully described in the proposal.
  - The proposal does not define the implementation timeline, other than to state that Tereon can be implemented within a matter of months and within the Task Force’s proposed time frame.
  - Additional information would be beneficial in several areas related to implementation, including building a critical mass of users and merchants, identifying scheme operator(s), and developing and implementing scheme rules and governance frameworks.
  - The proposal suggests that it may be necessary to create one or more specialist payment banks to compete with existing banks in providing services.
  - A commercial implementation of the solution is underway in Central America. It would be helpful to understand the similarities between the Central American implementation and the proposed solution for the U.S. market, as well as how the lessons learned from the Central American implementation will inform roll-out in the U.S.

ASSESSMENT

Ubiquity

U.1 Accessibility

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale

The solution supports payments to and from any account and is available both to FI providers and to non-FI providers that meet deposit-taking regulations. Non-FI PSPs (payment service providers) provide access for the unbanked (U.1.1). The solution uses a directory look-up service that supports the routing of payments between providers. The directory look-up capability allows providers to trust one another, as both parties to the transaction must be authorized in order to interconnect. If an end-user does not have a Tereon account, s/he may withdraw received funds through a service provider. The initiator of the payment is ultimately responsible for identifying the payee and ensuring that the payee receives the transaction number (provided by Tereon via email /SMS if possible) and PIN (provided by the payer to the payee).

Regarding funds access, any entity with a smart phone and a cash box can act as a merchant supporting the withdrawal of funds. If the recipient does not withdraw the funds within a specified time period, the transaction is nullified, and the funds are returned to the payer (U.1.2). The solution can support multi-currency payments (U.1.3). Tereon makes no distinction between banked and unbanked users (U.1.4).

Implementation of the solution requires providers to allow access to core account systems via APIs and to invest in high-end commodity servers. The solution uses a standardized messaging protocol and can support most communication formats via a translator. Kalypton provides a set of Tereon protocols (a tool kit) that providers can use to develop new, proprietary services. Transaction information can be transmitted over the internet or mobile data networks, simplifying implementation. Merchants can accept payments using a smart device, thereby avoiding upgrades at the POS (point of sale); however, integration may be required in operational systems to support a new payment option (U.1.5).

U.2 Usability

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale

The solution supports almost any payment channel and device (U.2.1). Payments can be routed using the payee's Tereon ID, which can be an email address, mobile number, name, etc. (U.2.2). Account information is never shared as part of the transaction (unless the payment vehicle is a check). Payments to non-registered users require payee name and address to allow for authentication. Tereon is designed to be available 24x7x365, though full-time access will depend on the availability of the provider's system (U.2.3). Tereon allows providers to select authentication credentials for end-users and supports numerous options for doing so. The solution supports multiple languages and use cases (U.2.4).

U.3 Predictability

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution clearly defines a consistent, baseline set of transactions that any provider will be able to support at implementation. Baseline services are available via any channel or device and are delivered using standard communications and messaging protocols (U.3.1-2, U.3.4). All fees will be clearly communicated to the payer before a payment is initiated. The solution can support multiple communications and messages originating in multiple protocols and supports communications in any language (U.3.3).

No system rules exist for the solution at this time, and a dispute management process has not yet been defined. The legal framework for the system's rules and dispute resolution mechanisms will be based on the existing ECCHO Operating Rules for electronic check presentment, but with the necessary amendments to provide for the operational nature of Tereon. The rules will set out an error resolution process to allow users to resolve any errors that might occur. Kalypton will also leverage the system rules and dispute mechanisms that are part of the planned implementation in Central America (U.3.4).

"Tereon' is the name of Kalypton's transaction processing software platform and does not need to be the user-facing brand for an ad service or scheme built on Tereon (U.3.5).

U.4 Contextual data capability

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale

Tereon transmits its data—including any contextual data—in an obfuscated, serialized, encrypted form. Data received from a sender's system is translated into Kalypton's own internal data format before it is transmitted to the receiving system's Tereon server, where it is translated into the recipient's data format (whatever that may be). The solution supports contextual data across all use cases. Contextual data capabilities seem broad and are extensible to include targeted offers or similar non-transaction-related information (U.4.1). The solution's multi-currency capability allows for the processing of loyalty points (U.4.2).

The solution can interface with business finance systems, personal finance systems, banking systems, etc. The solution supports ISO 8583 and ISO 20022 and can be adapted to support any communication standard as required (U.4.3).

Tereon captures data that has not (yet) been defined by ISO 20022 (for example, no ISO 20022 message schema is currently defined for geolocation data). Kalypton can leverage the supplementary data field and will work with industry participants to define the format for data to be included in this field. Tereon will retain all transaction data in its own internal audit logs, and providers can use other Big Data systems to access and process this data. Kalypton will define contextual data requirements at the start of the implementation phase.

U.5 Cross-border functionality

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution is well-designed to support multi-currency payments. If a payee and payer operate in different currencies, the solution supports a foreign exchange capability, including notification of the exchange rate and fees prior to initiation of the transaction (U.5.3; U.5.4).

While Tereon can connect and communicate with payment systems in other countries, it will require providers to accept any associated settlement risks, which could hinder widespread adoption. More clarity is needed on how the solution will ensure interoperability with payment systems in other countries (U.5.2). With regards to ISO 20022, Tereon makes no distinction between domestic or cross-border transactions and provides all data for all transactions regardless of endpoints, as described in U.4.

Tereon acts as an RTGS (real-time gross settlement) system in its default mode but can operate as a DNS (deferred net settlement) system or an RTGS-DNS hybrid. In every mode, a user must have sufficient credit or funds to make a payment or transfer, and the provider cannot approve the payment unless it has the funds to settle the payment or transfer. This good-funds model eliminates settlement risk.

U.6 Applicability to multiple use cases

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution supports all of the required use cases in its initial implementation.

Efficiency

E.1 Enables competition

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The proposal states that any end-user can change providers at any time without any loss of "in-air" payments (E.1.1). Any transactions that are in process when the end-user switches providers will move seamlessly to the new provider. Tereon requires providers to share all fees associated with the Tereon service as part of the enrollment process (E.1.3). Any provider that is willing to abide by the solution's governance and payment rules can offer a service using Tereon (E.1.4). All providers are required to support baseline services, regardless of size. Non-bank PSPs must hold an account at a regulated FI to ensure that funds are kept within the existing banking system. All providers have access to a tool kit that will support the introduction of new products and services on the Tereon platform.

When end-users switch providers, their account history will transfer from the old provider to the new one. A user can register multiple IDs with a single provider or register the same ID and device

with multiple providers. The directory look-up service can differentiate among providers based on the services they provide to a user (U.1.2).

E.2 Capability to enable value-added services

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

So that all providers can integrate with Tereon and offer value-added services to any user, Kalypton will publish all protocols and standards. A third party need only link to one provider's Tereon server to offer its services to any user who is allowed to use that service. Kalypton has already published APIs and protocols for earlier versions of Tereon. As new services and functions are added, Kalypton will publish APIs and protocols to enable third parties to use those functions and services. The solution puts the user in control of the additional service(s) used (E.2.1; E.2.2). Tereon will clearly disclose value-added services as optional (E.2.3).

E.3 Implementation timeline

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

FI providers' willingness to participate in this solution will play a substantial role in determining its long-term success. The solution will not succeed without access to core deposit accounts at FIs. The proposal states that the implementation of technology is not the limiting factor in a deployment timeline, and that the solution is designed to be implemented within months. Retailers may be more likely adopters due to the solution's ability to reduce the costs associated with PCI requirements and transaction processing.

The proposal provides a detailed implementation plan that describes key tasks and offers estimated timelines based on past experience with implementations in other jurisdictions. The proposal acknowledges that there will be differences that are particular to the U.S. market.

The proposal indicates that each provider's infrastructure and internal readiness may impact implementation timelines. This raises concerns as to whether the implementation milestones can be achieved in the time frames provided. The proposers believe that community banks, bankers' banks, processors, credit unions, corporate credit unions, and other stakeholders will find value in helping to create and maintain solution rules.

Retailers are expected to actively adopt the solution because it will reduce costs, but banks' adoption may lag behind the proposed timeline due to implementation challenges. The proposal would be strengthened by more clearly articulating the solution's value proposition for banks and by providing a more detailed implementation timeline (E.3.1).

E.4 Payment format standards

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution uses its own internal message protocol to support communication between servers and devices. It can interface with any existing message format through translation, if required (E.4.1-E.4.2), and is designed to support upgraded or new message formats (E.4.4). There are some concerns about the effectiveness of translation engines generally, which may impact the effectiveness of this approach. Each provider will determine the message format to be used.

The solution's modular design makes APIs a natural conduit to support the implementation of upgraded or new functionality. Tereon publishes a set of APIs to integrate to core systems within account providers at a level that account providers can choose.

Tereon has been designed to retain all information that is captured and generated when processing a transaction, whether or not the communication format can accept that data. This data is retained in its original format and can be used as message formats evolve.

E.5 Comprehensive

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution can enable all aspects of the payment process (E.5.1). The proposal does not describe any requirements related to end-user accounts. The technical solution will support all of the features described. The proposal describes several options for settlement and states that its preferred solution would involve the central bank (E.5.2).

E.6 Scalability and adaptability

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The solution addresses a core set of baseline use cases (E.6.1). It is designed to process millions of transactions per second per provider based on a peer-to-peer architecture, and it can be easily modified to add new services or volumes (E.6.2). The proposal indicates that when a provider's system exceeds a set threshold, Tereon will scale itself horizontally to manage the additional load. Tereon has defined four metrics that determine when automatic horizontal scaling will be initiated: network load, CPU load, transaction volume, and system temperature. Kalypton and the provider will determine the exact loading of each metric based on hardware and configuration.

Kalypton claims that Tereon can support provider hardware upgrades with no impact to end-users (E.6.3). The proposal states that Tereon is designed to operate on standard carrier-grade equipment that may already be in place at provider locations. A provider's hardware investment will depend on the volume of services and number of users to be supported. Kalypton has worked with a financial services hardware provider to define three hardware configurations (servers, storage systems, and networking infrastructure).

E.7 Exceptions and investigations process

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The existing ECCHO rules and procedures will inform Tereon's process for resolving exceptions and disputed transactions. Because Tereon is a real-time solution, the proposer anticipates that exceptions or disputes will be rare. The system's rules will include effective, economic mechanisms to enable users and providers to resolve any exceptions or disputed payments that may occur (E.7.1). The Tereon messaging service can be used to send alerts and notifications to support an exceptions and investigations process. The solution is designed to interface with a provider's existing tools to support exceptions and investigations through the use of APIs. Tereon can also create new tools and monitoring services if needed (E.7.1).

Tereon records every transaction in real time, and each record includes the transaction time and date. All users are made aware of the audit trail and can access the information at any time. The audit trail captures all contextual data surrounding the transaction and stores this in a searchable, anonymized state (E.7.2). Tereon can render data anonymous if required, aggregate data into a monitoring service, and share that data among providers. This data can be provided as a real-time feed so that an aggregator can use Big Data analytics to monitor transaction traffic for suspicious patterns (E.7.3).

The ECCHO rules to support faster payments have not yet been developed and therefore cannot be evaluated (E.7.1). It would be helpful if the solution developed tools to support exceptions and investigations (E.7.1).

Safety and Security

S.1 Risk management

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The solution is configurable and enables a provider to amend a service and/or track required data in the event of an unexpected change in law, regulation, or rule (S.1.1).

Tereon can settle a transaction in a number of ways, depending on the settlement mechanism that providers wish to use. The solution relies on providers' existing settlement capabilities, which may or may not be batched. The solution hypothecates payment transactions to settlement accounts and requires those funds to be used to settle Tereon payments; in this way, it addresses liquidity and settlement risks associated with deferred settlement (S.1.2).

Tereon automates as much of the payments system as possible to minimize the risks arising from human error. The solution is designed to limit access based on role. The solution is designed with built-in redundancy and automatic scaling to address any infrastructure issues or dramatic increases in usage (S.1.3). To address the risk of fraudulent transactions, the solution requires end-user authorization, limits the sharing of transaction information (no PII), places no authorization or authentication credentials on the device, and has mechanisms that allow end-users to manage payments made under duress. The solution is designed to minimize errors in payment (S.1.4).

Legal and risk management frameworks will be reviewed at least every six months to address any changes in law and/or regulation (S.1.6). To fully address liquidity and settlement-related risks, the solution could integrate with, or even require integration with, real-time settlement mechanisms as they are introduced into the market.

S.2 Payer authorization

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution requires payer authorization for every transaction. Authentication involves several steps, some of which can be optional, depending on the provider's requirements (S.2.1). The solution also allows for preauthorized payments (S.2.2), which the end-user can modify (S.2.3). Clearing and settlement take place when the payment is made; however, the user can configure the account to "block" the funds when payment is initiated. The solution can also support low-value transactions without authorization (such as transit payments) that are guided by parameters within the solution.

S.3 Payment finality

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The solution requires the provider to approve each payment to ensure good funds (S.3.1). The proposal states that payments become irrevocable once they are hypothecated to the settlement account and the recipient has received the funds (S.3.2).

While the proposal is clear about the need for operating rules and goes as far as to say that the ECCHO framework will be used, the rules, policies, and regulations themselves have yet to be developed. The proposal states that the payment rules will provide a mechanism to compensate payers/payees if a payment is disputed successfully. The operating rules, when written, should provide clarification on a dispute process and a mechanism to compensate payers or payees if a payment is successfully disputed (S.3.3).

S.4 Settlement approach

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The solution requires payers to have sufficient funds to support a transaction through the hypothecation of funds. The proposal describes hypothecating funds to a settlement account but relies on providers' existing settlement capabilities for final settlement (S.4.1). Tereon can be overlaid onto existing deferred-net-settlement (DNS) systems to add the functionality of a secured DNS settlement option. This step is not optimal, however, as it may require intra-day credit or liquidity to ensure available funds to support transaction processing (S.4.2). The proposal states that

Tereon’s preferred settlement method is for providers to hold settlement accounts with the central bank and to settle in central bank money, and to leverage real time (RTGS) settlement capabilities to remove settlement liquidity risks (S.4.3). The solution requires participants to treat transactions as irrevocable once funds have been hypothecated for settlement and received by the recipient.

The proposal suggests that the combination of Tereon and an existing settlement system would incur higher operational costs than a system based on Tereon alone. The proposal could be strengthened by detailing the method(s) that will be in place to manage intra-day credit/liquidity in a scenario where settlement occurs through existing settlement capabilities (S.4.2).

S.5 Handling disputed payments

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

Users, devices, accounts, or providers can be blocked from the system if an unauthorized, fraudulent, or erroneous payment is detected (S.5.1). The Tereon solution is designed to enable a provider to conform to consumer protection law and will support the reversal of erroneous payments (S.5.2). The Tereon audit capability provides detailed and searchable information for every transaction and action by account. The solution supports dispute initiation, end-user refunds, and transaction reversals (S.5.3).

The proposer clearly acknowledges the need for operating rules and will base those rules on ECCHO’s rules framework, but the rules have yet to be created. The proposer can strengthen the proposal by directly outlining how disputed payments will be handled; delineating each party’s rights; confirming roles, responsibilities and liability allocation; and providing the timelines associated with disputed payments (S.5.2-3).

S.6 Fraud information sharing

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The solution has a well-defined audit capability and tracks and retains all aspects of a transaction (S.6.6). Tereon can share that information in real time (S.6.3), supplying a suitably structured data feed into a Big Data analytical tool or to a third party for data analysis (S.6.1).

Tereon strictly controls access to data based on ownership and roles. Tereon also offers the tools to combat fraud by allowing approved administrators access to users’ full transaction history to investigate those transactions further (S.6.5). Access to this data is tightly controlled, and the audit system tracks all administrator actions.

The solution would be strengthened by requiring the sharing of key data elements to support identification of fraudulent activity beyond a single provider (i.e., at the network level) (S.6.1) and by defining how data owned by other entities would be aggregated and anonymized to support fraud information-sharing (S.6.2).

S.7 Security controls

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

Tereon's security controls are layered, and all access to the system is recorded by the audit capability (S.7.1). No aspect of the solution is accessible unless security measures have been met. All data is encrypted with independent keys before transmission to or from any endpoint or server (S.7.1). The solution is designed to guarantee the data's integrity and to protect against system failure.

As with several aspects of the solution that require operating rules and a governance model, the participation agreement, when created, should define participation requirements pertaining to physical and environmental security, managerial policies, operational security, monitoring, and incident response (S.7.2-3).

S.8 Resiliency

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution is designed to provide a fully redundant, resilient, and efficient payments service. Tereon is designed to be available 24x7x365 with full n+2 redundancy (two independent back-up components). The solution's target availability for each provider is 99.95% for each individual component, and 100% for the service as a whole (S.8.1). The system ensures there is no single point of failure, as servers communicate on a peer-to-peer basis (S.8.2). Although individual components may fail, multiple redundancy and the ability to start up replacement instances to replace any failures would deliver 100% uptime overall (S.8.3). Tereon is self-monitoring, and each provider will have the tools necessary to monitor the uptime of individual components and the solution as a whole (S.8.4). As indicated in the proposal, the solution's payment rules will need to define requirements and procedures for providers' contingency testing (S.8.5).

S.9 End-user data protection

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution includes strong controls and mechanisms for administrator access. Tereon's audit capability captures all interactions with the system (S.9.1). The solution supports the initiation and routing of payments using a Tereon ID, and account information is never exposed at any time during the transaction (S.9.2, S.9.3).

S.10 End-user/provider authentication

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The solution supports multi-factor authentication ranging from PIN to biometric options (S.10.1) and is clearly aligned with industry standards for end-user authentication (S.10.3). The solution ensures that payments will reach the intended end-user (S.10.2). The solution's design is modular, and the addition/decommission of authentication models should be easily accomplished without impact to the solution overall (S.10.6). The solution includes a directory look-up capability that routes payments from payee to payer using only a Tereon ID (S.10.2). Every end-user device and Tereon server must be approved and licensed to communicate on the Tereon platform (S.10.1). The solution requires the same authentication procedure irrespective of the transaction's value (S.10.4).

Providers will be responsible for authenticating end-users. It would be helpful for Tereon to define authentication requirements for providers in addition to KYC and AML procedures (S.10.1).

S.11 Participation

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

Participation rules have yet to be written. When available, the rules will set out the duties and obligations of provider and will define sanctions for failure to comply with rules (S.11.1). The rules will ensure that providers are able to fulfill their obligations (S.11.2). Tereon will monitor (in real time) and flag providers that appear to be introducing risk into the solution (S.11.3).

The proposal acknowledges that there are issues that must be addressed by the Faster Payments Task Force to support the creation of Uniform Rules, which will inform the creation of participation rules.

Kalypton has a standard user license agreement that will be tailored to U.S. law once the preliminary rules and agreements (Uniform Rules) have been drafted to ensure that the Uniform Rules are correctly referenced in the agreement.

Speed (Fast)

F.1 Fast approval

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

Tereon is designed to approve or deny a transfer or a payment in less than one second from the moment of payer initiation.

F.2 Fast clearing

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

Tereon is designed to clear a transfer or payment in less than one second from the moment of payer initiation.

F.3 Fast availability of good funds to payee

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

Tereon hypothecates funds to a settlement account and credits a recipient’s account with funds in less than one second from the moment of payer initiation. There is one exception, however: if a recipient does not have a Tereon ID, the funds will remain available for a period of time (defined by the transferor) so that the recipient may retrieve them from a Tereon “agent” or set up a Tereon account. If the funds are not claimed, they are returned to the payer.

F.4 Fast settlement among depository institutions and regulated non-bank account provider

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale

Tereon hypothecates funds to a settlement account in less than one second. However, final settlement of the transaction relies on the individual providers’ existing settlement options, which are not yet real time and do not operate 24x7x365, potentially creating risk. The solution can support settlement on a real-time settlement system when implemented by providers (F.4.1). The solution is designed to operate 24x7x365, which addresses concerns related to different time zones (F.4.2). Tereon has the capability to net transfers and payments for providers. Regulatory authorities may determine liquidity levels that providers must maintain, and Tereon can enforce those levels.

The proposal states that the preferred settlement option is for providers to hold settlement accounts at the central bank and to settle using central bank money. This option would remove all settlement risk and would allow Tereon to settle transactions immediately acting as an RTGS solution.

F.5 Prompt visibility of payment status

[✓ Very Effective] Effective Somewhat Effective Not Effective

Rationale:

The status of a payment is immediately reported to the payer’s systems. Tereon always notifies the payer when the account has been debited and when the recipient has received the funds. It also notifies the recipient when a pending transfer or payment has been approved and when the funds have been credited to the account (F.5.1-2).

Legal

L.1 Legal framework

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

ECCHO will identify and analyze all relevant laws and regulations that will form the basis of the industry-level legal framework for Faster Payments (Uniform Rules) (L.1.1). Tereon's governance and legal frameworks will be based on these industry-level requirements and will define each process, as well as participants' responsibilities in the solution (Provider Agreement) (L.1.3).

L.2 Payment system rules

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

ECCHO will identify and analyze all relevant laws and regulations that will form the basis of the industry-level legal framework for Faster Payments (Uniform Rules).. Tereon's payment system rules will be based on these industry-level requirements and will define each process, as well as the accountabilities of solution participants (L.2.1). The proposal articulates which aspects of the Uniform Rules will be addressed once defined and describes a high-level payment system rules amendment process (L.2.2).

L.3 Consumer protections

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The proposal acknowledges that, although Tereon is designed to limit the likelihood of disputed payments, to drive adoption the solution must have a legal framework that provides protection and certainty for consumers. This legal framework will define all users' and providers' legal and financial responsibilities related to unauthorized, fraudulent, or erroneous consumer payments (L.3.1). The rules will support error-resolution mechanisms that meet and perhaps exceed protections required under applicable law (L.3.2). The legal framework may also allow providers to exceed protections that are currently required under applicable law (L.3.3).

L.4 Data privacy

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The Faster Payments Task Force's Uniform Rules for the faster payment system will define each party's data privacy responsibilities in the payments process. The proposal indicates that the solution's data protection framework may be modeled on parts of the EU's General Data Protection Regulations and may exceed the protections currently afforded under applicable law (L.4.2). The legal framework will define: 1) the data that end-users must provide to enroll and to send payments to non-registered users (L.4.3), 2) end-user visibility into data that is collected (L.4.4), and 3) providers' obligations related to access and data protection (L.4.5).

L.5 Intellectual property

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

A number of patents that address the solution and its capabilities are pending. Kalypton and ECCHO will continue to conduct ongoing due diligence reviews of all applicable IP rights.

The proposer recognizes the need to develop an approach to managing intellectual property rights. This approach will be developed in cooperation with ECCHO.

Governance

G.1 Effective governance

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

At the industry level, ECCHO will leverage a governance structure that is similar to the existing structure that it uses for image exchange. This governance arrangement consists of three levels: ad hoc subcommittees, an RTP committee, and a board of directors. The bylaws of the solution's rules organization will determine the governance structure for the Tereon platform. The proposal describes a board of directors comprising representatives from various stakeholder groups. The board will set policy objectives and approve the solution's rules with consideration for all stakeholders' interests. The governance arrangements will be made public (G.1.2). High-level guidelines are provided regarding the appeals process (G.1.3) and independent validation of compliance. Governance arrangements will provide for independent validation of the governing organization's compliance with the solution's governance and legal frameworks (G.1.4). Kalypton will work with ECCHO to develop a governance framework.

G.2 Inclusive governance

Very Effective [✓ Effective] Somewhat Effective Not Effective

Rationale:

The proposal suggests that the solution's governance rules will ensure that public and stakeholder interests will be considered when making rules and decisions (G.2.1-2). Board decisions will rely on input from governance substructures/subcommittees (G.2.2). The proposal describes a high-level issue resolution process. An operations committee will be formed, and this committee's chair will

present recommendations at board meetings. Bylaws will include provisions for managing conflicts of interest (G.2.5). Kalypton will work with ECCHO to develop a governance framework.