Faster Payments QIAT

Proposer: Token, Inc.

February 21, 2017

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Proposal</td>
<td>2</td>
</tr>
<tr>
<td>Q&amp;A Response</td>
<td>72</td>
</tr>
<tr>
<td>Draft QIAT Assessment</td>
<td>82</td>
</tr>
<tr>
<td>(Includes proposer comment in Appendix A &amp; B)</td>
<td>97</td>
</tr>
<tr>
<td>Task Force comments</td>
<td>100</td>
</tr>
<tr>
<td>Proposer response to Task Force comments</td>
<td>106</td>
</tr>
<tr>
<td>Final QIAT Assessment</td>
<td>107</td>
</tr>
</tbody>
</table>
Faster Payments Task Force Proposal

The Token Faster Payments System

April 30, 2016
Submitted by: Marten Nelson, Token, Inc.
# TABLE OF CONTENTS

**Executive summary** .................................................................................................................. 3

**Use Case Coverage** .................................................................................................................. 6
  Supported Use Case Coverage Summary .................................................................................... 6
  Cross-border Use Case Coverage (If Applicable) ........................................................................ 6
  Proposal Assumptions (Optional) ................................................................................................. 7

**PART A: DETAILED END-TO-END PAYMENTS FLOW DESCRIPTION** ................................. 8
  Part A, Section 1: Solution Description ....................................................................................... 8
  **Token System Components** ..................................................................................................... 8
    Token Provider Software (TPS) .................................................................................................. 8
    Token Hub .................................................................................................................................. 9
    Token Authority Service ............................................................................................................ 10
    Partner SDK - mobile & back-office ......................................................................................... 11
    Token Currency Ledger (TCL) .................................................................................................... 11
    Token Foreign Exchange Service (TFXS) .................................................................................. 12
  **Smart Token Capability** ........................................................................................................ 12
    Token Security .......................................................................................................................... 14
    Provider Mobile App Integration .............................................................................................. 18

**Detailed Description of Payment Phases** ................................................................................ 18
  Direct Payment Initiation ........................................................................................................ 19
    Detailed Example of Initiating a Direct Payment ..................................................................... 20
  Pre-Authorized Payment ........................................................................................................ 20
    Detailed Example of a Pre-Authorized Payment ..................................................................... 22
    Common Elements of Both Payment Types .......................................................................... 23
    Payment Execution .................................................................................................................. 25
    Approval by the Payer’s Provider ............................................................................................ 25
    Clearing ..................................................................................................................................... 26
    Receipt ...................................................................................................................................... 27
    Detailed Example of Payment Execution .................................................................................. 28
  Settlement ................................................................................................................................. 29
  Reconciliation .............................................................................................................................. 30
  Payment Process Flow Diagrams ................................................................................................ 31

**Multi-currency & cross-border** ................................................................................................. 33
  Part A, Section 2: Use Case Description ...................................................................................... 34
    Business to Business (B2B) ...................................................................................................... 34
    Business to Person (B2P) .......................................................................................................... 36
    Person to Business (P2B) .......................................................................................................... 37
    Person to Person (P2P) ............................................................................................................. 39
  Part A, Section 3: Use Case by Effectiveness Criteria ................................................................. 40

© 2016 Token, Inc.
PART B: BUSINESS CONSIDERATIONS

1. Implementation Timeline
   - Development timeline
   - Typical customer engagement plan
   - Market ubiquity plan
   - Interoperability with existing solutions
   - Initial and subsequent features
   - Key dependencies and risks

2. Value Proposition and Competition
   - Business to Business (B2B)
   - Business to Person (B2P)
   - Person to Business (P2B)
   - Person to Person (P2P)

3. Integration Effort
   - Business to Business (B2B)
   - Business to Person (B2P)
   - Person to Business (P2B)
   - Person to Person (P2P)

PART C: SELF-ASSESSMENT AGAINST EFFECTIVENESS CRITERIA

1. Ubiquity
2. Efficiency
3. Safety and Security
4. Speed (Fast)
5. Legal Framework
6. Governance
EXECUTIVE SUMMARY

Today’s payment rails were designed and built before the invention of the Internet and the global 24/7 economy. As a result, existing payment rails don’t offer adequate security measures, don’t allow transfer of funds as fast as required by consumers and businesses, lack open interfaces that allow third party developers to build innovative services, and leave Payers with little control of their payments regardless of use case.

There is no worldwide standard open API to banks and no worldwide standard open API for moving money. We want to fix these two problems.

Token proposes a new digital payment network that is modern, secure, fast, and open. This digital payment network is based on Token’s new, from-the-ground-up system which leverages modern concepts, technologies and methods. At the core of the Token system is a smart tokenization module that provides a powerful set of rules that control access to a Payer’s bank account for the purpose of making payments.

Token does not use username and passwords, or payment card numbers for authentication and authorization. Instead, Payer and Payee authentication and payment authorization are completed using digital signatures based on Ed25519, a state-of-the-art public-key signature system standard. Digitally signing all payment transactions provides non-repudiation for all payments and eliminates the potential for mass breaches.

The Token payment system is accessed through an open RESTful API, secured using digital signatures. This open model allows third party developers to innovate and create new applications never before possible with existing payment methods.

The Token system handling all of the payment lifecycle stages can be represented as a modular stack (see Figure 1). At the top of the stack are applications (apps) developed by third parties (e.g. e-commerce checkout, disbursement, etc.). Apps access the payment rail through the open API. Payment authorizations (“smart tokens”, or in this document also mentioned as just “tokens”) are created using the tokenization module running inside each bank. The transaction is authenticated and validated and the rules of the smart token are verified before the payment is posted and cleared and then finally settled. The Token modules running at the bank are collectively called the Token Provider Software (TPS).
Token offers two payment types: “direct (push) payments” and “pre-authorized (pull) payments.”

**Direct payments**
Direct, one-time payments are initiated by the Payer to the Payee via an API call to the Token Provider Software at the Payer’s Provider. It’s essentially a Push Payment, or analogous to a SEPA Credit Transfer payment.

**Pre-authorized payment**
The pre-authorized payment type is based on the “smart token” paradigm provided by the Token Provider Software. Smart tokens provide a way for Payers to allow Payees to access funds in a Payer’s account, under a predefined set of terms specified by the Payer. It can be used for Pull Payments and is similar to SEPA Direct Debit payments with pre-defined set of terms.

**Multi-level security**
Token was designed with security being a top priority. Therefore, the Token system offers multi-level end-to-end security:

- **Account authentication** using public-key cryptography
- **Payment authorization** using public-key cryptography
- **Restricted account access/smart contracts** using smart tokens
- **DDOS and intrusion protection** through hub-spoke model for inter-bank communications
## USE CASE COVERAGE

### Supported Use Case Coverage Summary

<table>
<thead>
<tr>
<th>Use case</th>
<th>Supported (Y/N)</th>
<th>Cross-border (Y/N)</th>
<th>Examples of payments supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business to Business (B2B)</td>
<td>Y</td>
<td>Y</td>
<td>Bill pay, business purchases</td>
<td>No restrictions on types of payments</td>
</tr>
<tr>
<td>Business to Person (B2P)</td>
<td>Y</td>
<td>Y</td>
<td>Salary payments, legal settlements, insurance claims</td>
<td>No restrictions on types of payments</td>
</tr>
<tr>
<td>Person to Business (P2B)</td>
<td>Y</td>
<td>Y</td>
<td>E-commerce, in-store checkout</td>
<td>No restrictions on types of payments</td>
</tr>
<tr>
<td>Person to Person (P2P)</td>
<td>Y</td>
<td>Y</td>
<td>Rent payments, split restaurant bill, purchases from classifieds</td>
<td>No restrictions on types of payments</td>
</tr>
</tbody>
</table>

### Cross-border Use Case Coverage (If Applicable)

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Non-US Corridor(s) and Systems</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business to Business (B2B)</td>
<td>Any Provider in any jurisdiction that operates Token and complies with the Token terms and that jurisdiction’s regulatory framework.</td>
<td></td>
</tr>
<tr>
<td>Business to Person (B2P)</td>
<td>Any Provider in any jurisdiction that operates Token and complies</td>
<td></td>
</tr>
<tr>
<td>Person to Business (P2B)</td>
<td>Any Provider in any jurisdiction that operates Token and complies with the Token terms and that jurisdiction’s regulatory framework.</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Person to Person (P2P)</td>
<td>Any Provider in any jurisdiction that operates Token and complies with the Token terms and that jurisdiction’s regulatory framework.</td>
<td></td>
</tr>
</tbody>
</table>

**Proposal Assumptions (Optional)**
PART A: DETAILED END-TO-END PAYMENTS FLOW DESCRIPTION

Part A, Section 1: Solution Description

The Token System is a set of software and service components that function together to implement a fast, secure payment system using the latest communications and security technologies. Payments made via Token are typically completed within milliseconds and Token assures that all payments are made to and from the authorized parties to the payment.

The various components of the Token system are deployed to Providers and other entities within the financial system, such as the Central Bank. Token defines a model for the initiation and execution of payments, and the components of the Token system provide the technology to implement this model across the various parties.

Each component in the Token system provides an open RESTful API for the functions it implements. The components communicate with one another over secured channels using standard Internet technology. All participants engage the system by calling the appropriate APIs served up by the components. All calls are authenticated via the use of digital signature technology.

The Token system runs on top of and is integrated into the existing account management systems at Providers. Token does not replace these “core banking systems” but rather augments them to provide secure, fast payments for the Providers’ customers.

Token System Components

This section describes the various technological and operational components of the Token system.

Token Provider Software (TPS)

The Token Provider Software is a software product that is intended to be installed at a participating Provider to support that Provider’s participation in the Token system. The TPS is typically installed within the IT infrastructure of the Provider, though it may be deployed in a cloud service or other hosting provider.

The TPS includes the following:

- A RESTful API implementing the services necessary for the Provider to participate in the Token payment network
- Outbound integration points to the other components of the Token system, including the Token Hub and other TPS instances, and the Token Currency Ledger.
• An Identity Management capability that uses advanced cryptography and other techniques to implement strong customer and partner authentication. The TPS includes the technology to generate and verify digital signatures using Ed25519.

• A unique “smart token” capability that allows Provider End-users to create powerful payment authorizations with terms that control the amounts of the payments and the conditions. See the section on Smart Tokens.

• Pre-defined integration points to account management systems and other back-office systems at a Provider. These integration points are used to trigger actions during the payment execution flows on the actual Provider accounts. These integration points include:
  ○ Account balance
  ○ Account transaction history
  ○ Debit and credit of funds to accounts

Token Hub
The Token Hub provides central services to all other components of the Token system to facilitate fast, reliable and secure payments. Token Hub services include:

• Routing all messages between components of the Token system, including the instances of the TPS installed at various Providers

• Ensuring delivery of messages to their destination

• Maintaining an always-accurate “net balance” of funds between any two Providers
  ○ Incremented/decremented on each IOU passed between TPS instances
  ○ Incremented/decremented on each receipt from the Token Currency Ledger receipts passed between TPS instances. For example, if Provider A sends Provider B an IOU for $10 and Provider B sends Provider A an IOU for $7 the Token Hub will report the net balance “A owes B $3”.

• Providing a place for Providers to post a “credit limit” for every other Provider

For information on how the net balance and credit limit capabilities are used to support near-real-time payments between Providers, see the section on Settlement.

Benefits of the Token Hub include:
IT security: each provider only needs to provision outbound network connections to one central service, rather than to the TPS system of each individual Provider that it might interact with.

IT reliability: the Token system can be engineered to support reliable communication between instances of the TPS and the Token Hub, including assured delivery to the destination TPS

Business relationship management: the Token Hub monitors the exchange of IOUs between Providers and keep track of the “net balance” between each Provider pair. This net balance will be used to drive the Settlement phase described in the next section.

Token Authority Service

The Token Authority Service is responsible for:

- Managing the mapping between IDs of participants (subjects) in the Token system, and their public keys through the use of digital certificates.
- Managing signed certificates for subjects, which provide proof of the subject’s name, identity, and public keys. Certificates for end-users are signed by the end user’s Provider, and certificates for Providers are signed by the Authority Service. See Token Security for more details.

For example, a customer of a Provider may have an ID of 123. The Authority Service stores the public keys for this customer, along with his/her name, and a certificate signed by the customer’s Provider, which guarantees that said Provider confirms this information. Furthermore, each Provider would also have a certificate, signed by the Authority Service. Each party making any API call signs the data associated with that call using that party’s private key. They also pass along the certificate that associates their identity with their public keys. The recipient of the signed call can verify that the certificate is genuine via the digital signature of the authority service, and can then use the public keys in the certificate to verify the signature on the call. As a result, participants don’t need to know the public keys of all Providers in advance, they must only know and trust the Authority Service.

The Authority Service is critical in the Token payment system because it reduces the amount of trust that participants have to put on others, as well as the amount of assumed risk. For example, a Payer in an offline transaction cannot be sure of the reputation or identity of who he/she is paying, unless he/she is provided with a certificate signed by a Provider and the Authority Service.

The Authority Service can be run by the Federal Reserve, a partner Provider, current Certificate Authorities like Verisign, or another trusted third party institution.
Partner SDK - mobile & back-office

Token provides an SDK to Providers and other partners to assist them in integrating the TPS into their environment. The libraries will provide support for making Token API calls to the TPS, generating and managing private/public key pairs, and generating and verifying digital signatures.

The SDK:

- Enables Providers to integrate Token capabilities into their mobile apps and websites
- Enables partner websites and other applications to execute payments, request payment authorizations, etc.
- Enables third-party apps such as wallet providers, etc. to integrate Token functionality to support making payments from the apps.

The SDK includes:

- Mobile app libraries for iOS and Android that enables the partner’s mobile apps to integrate with Token. The libraries provide support for making Token API calls to the TPS, generating and managing private/public key pairs, and generating and verifying digital signatures.
- Back-office libraries for common programming environments such as Java and .NET that enables partner back-office software to integrate to Token Provider Software.

Token Currency Ledger (TCL)

Token Currency Ledgers (TCLs) are operated by the Central Bank (e.g. the Federal Reserve for US Dollars), or a designated party for a given currency. Each TCL supports Settlement among Providers hosting a ledger that is backed by funds reserved by the operator. The Provider receives a receipt for the transfer by a TCL, and this receipt is presented to the Provider to whom the funds were transferred as proof of that transaction.

The TCL:

- Provides an API to all member Providers to initiate funds transfers
- Accepts signed calls to transfer funds from one Provider to another
- Records all transactions in a distributed ledger or blockchain or other reliable ledger
- Provides a signed receipt of funds transfer to the requesting Provider
The TCLs do not need to be running Token TCL code so long as they provide the necessary functionality, i.e., the TCL can be a capable currency blockchain.

**Token Foreign Exchange Service (TFXS)**

The purpose of the FX service is to enable funds to be instantly moved across currencies. The FX provider is a Provider that has branches on multiple Central Bank rails.

Token supports any number of FX service providers. For example, large multi-national Providers can host their own FX service.

The FX service provider uses a simple API to move money on a foreign TCL. For example, Provider A can request (via IOU) the FX service provider move 100,000 EUR on the EUR TCL into Provider B’s account on that TCL, and return a receipt of that transaction to Provider A so it can present that receipt as proof of payment to Provider B.

**Smart Token Capability**

Tokenization is the process whereby sensitive information is replaced with a non-sensitive substitute, called a “token”. A token is a reference that maps back to the sensitive data through a tokenization system. Tokenization can be used effectively to safeguard any type of sensitive information such as medical records, driver’s licenses, personally identifiable information (PII) and much more.

Where it’s simply a matter of replacing sensitive information with a non-sensitive equivalent, a token is generated using **basic tokenization**.

The Token system provides an advanced capability called **smart tokenization** which supports the creation of tokens that include terms ruling access to the underlying asset.

<table>
<thead>
<tr>
<th></th>
<th>Basic tokenization</th>
<th>Smart tokenization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mask original asset address</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Set and enforce rules on access to the underlying asset</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Emulate multiple payment types</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Customer programmable</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Dynamic fields</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Like basic tokenization, smart tokenization masks the underlying assets identifier such as an account number, but it adds a key element — terms. Akin to “smart contracts” in the world of blockchain, smart tokens are programmable by defining terms (aka rules) that govern access to an asset, or simply adding contextual information. To maintain the integrity of smart tokens, terms cannot be altered. Recognizing that some terms may be dynamic (such as keeping track of a spending limit), smart tokens can also have a “state”.

Figure 2: A smart token created by a parent for her child in college.

In this example the token has been limited to $500/month and can only be used for expenses related to automobile, food, laundry and books. The token has an expiration date and a daily limit. The account owner is notified if the daily limit is reached and has the power to override.

Smart token terms can be defined arbitrarily and do not require specialized programming skills. The ability to specify the terms on smart tokens is integrated with customer tools such as mobile apps and ERP systems.

Smart tokens are secured by the most advanced cryptography available (Ed25519). When an End-user requests the creation of a smart token from their TPS, the terms specified for the token are signed using the End-user’s private key. The resulting signature ensures that the terms of the token cannot be modified after the fact, and it serves as the proof of authorization for future payments made using the token. No shared secrets such as usernames and passwords are used, eliminating issues associated with mass breaches. No personally identifiable information is ever revealed. See the Token Security section for more details.

In addition to being cryptographically signed by the End-user that creates the smart token, each smart token is typically tied to a specific Payee. For example, a token issued to pay for a monthly subscription service from a specific service provider cannot be redeemed by any other merchant.
Some examples of smart token terms include:

- The Payer’s account (Token Account Number) from which funds will be transferred.
- An effective date range, start date to end date. Redeem requests occurring outside this date range will be rejected.
- A “use count” - how many redeem requests can be made against this token. Typically, “single-use” or “unlimited”.
- A “lifetime amount cap”. Once the cap has been met, further redeem requests will be rejected.
- A per-request amount cap. A redeem request below this limit will be automatically approved. A redeem request above this limit will require the explicit approval of the Payer.
- A call-out mechanism to support making payment approval conditional on external factors, such as confirmation of shipment from a logistics provider. The callout specifies a URL and a certificate identifying a public key associated with the external service provider. The callout URL will be invoked with the terms of the payment request. The payment will be approved if the external service provider returns a response with a digital signature over the payment terms that is successfully verified against the public key.

Token Security

Introduction

Token relies on private/public key cryptography, digital signatures and certificates to ensure the security of the system. Token is implemented using Ed25519 as the cryptographic foundation for the signature scheme. Ed25519 provides cutting edge security, key sizes, and performance. Certificates are used to verify digital signatures, ensuring that entities are who they claim to be, and that they are reputable members, even in offline use cases.

Signatures

Every entity in the system is associated with one or more public keys, and handles corresponding private keys. When an entity makes an API call or a request to another party, the data being sent is signed by the former’s private key(s), proving that said entity initiated the request, locking the exact contents of the data against any tampering, and recording what time the data was sent. This results in a system in which data integrity and the sender identity are publicly verifiable via public keys, and attacks like forging requests, changing the request data, or changing the signer are impossible. If an entity discovers that a signature does not match the sender and data, the API call, payment, or request is rejected.
The result is that as long as private keys are kept secure, digital signatures can assure that every call can be verified to have been initiated by the correct entity. This tamper-proof authentication minimizes the risk of errors, failures, and fraud.

The securing of the private keys depends on the use case. For example:

- Enterprise entities such as Providers or merchants can store their private keys in hardware Trusted Execution Environments, and split their keys in different systems for additional security.

- Consumers can use an app that stores the private key, and may use additional private keys for greater security, for example one generated using a fingerprint, and another using a PIN code.

**Certificates and Identity**

Every request or message comes with an attached certificate. This certificate, signed by a higher authority, associates the sender of the request and the public key with an entity that is registered in the Token system. For example:

- A consumer’s Token-enabled mobile app receives a token request from a physical merchant such as Starbucks with public key ‘b67ac98’. The request is signed, so it’s known that the owner of this key initiated it. The certificate provides the additional mapping of the public key to the business name “Starbucks”. This certificate is issued and signed from Starbucks’ Provider, whose certificate is issued and signed by the Token Authority Service. This prevents a bad actor from masquerading as a legitimate merchant.

- Provider A sends a message to Provider B, signed using Provider A’s private key. Provider A attaches their certificate to the call providing proof of identity by linking their business name and ID to their public key, signed by the Authority Service. Provider B can then verify Provider A’s identity without having to have been in prior possession of Provider A’s public key or contacting some central “public key directory” service.

The certificate chain can be traced to the top, so that every request can be verified for/by any entity, without the need of an Internet connection, and only with the possession of The Authority Service’s public key. The Authority Service may be operated by trusted Providers, a Central Provider, or some other trusted third party. Its responsibility is to keep an up-to-date repository of trusted Providers and their public keys. See [Token Authority Service](#) for more details.

Furthermore, the certificates contain timestamps, so certificate aging policies can be established and enforced. Token does not define when a certificate becomes invalid, but participants in the system can choose how much risk they want to take on by rejecting older certificates.
Key Management
All entities in the Token ecosystem have a private key that they hold and an associated public key. For Providers, there is an approval process where the Provider’s public key is signed and added to CAs. For members such as consumer and businesses (clients of Providers), the public key is generated locally (e.g. on a mobile app on the consumer’s phone) and sent to the Provider in a secure fashion.

- Consumers will use their Provider’s mobile app to securely generate and transmit their key. Once a consumer logs in and agrees to enable Token on their app, a keypair is generated, and the public key is sent to the Provider. It is up to the Provider to enforce user identity authentication during this process, presumably using the same MFA methods the Provider uses to verify user identity for current financial transactions.

- Businesses generate their keys using their method of choice, and send their public key to the Provider via a process defined by the Provider. Against, the Provider is responsible for authenticating the End-user.

If a key is lost or stolen, it can be replaced. Certain keys have permissions to revoke or approve certain other keys. Approval and revocation rules are controlled by the TPS and the end users. If an end user has lost all of their keys, they must authenticate to their provider outside of the Token signature system. A consumer that lost his/her phone would have to log in to their Provider app or website, and provide authentication, in order to reset his/her keys.

Encryption and Openness
All data sent between entities in the Token system is encrypted using TLS. Personal Identifiable Information (PII) can be encrypted using a member’s public keys, so that it can only be accessed by that specific member, and not subject to mass breaches.

There are no shared secrets such as card numbers, account numbers, etc., meaning mass data breaches on Providers, merchants, or any entities will not reveal any useful information to attackers. Furthermore, since no secrets are shared, intercepted API calls, signature data and certificates, even in decrypted form, also provide no value to attackers. Since timestamps are included, replay attacks (re-sending a request twice) are impossible.

Since all Token API calls are fully authenticated and secure, and no shared secrets are used, the API at the TPS is completely open and accessible to anyone. This openness not only makes the system transparent and developer friendly, but also encourages best practices in security. Furthermore, this open API enables a wide variety of applications to be developed on top of the Token protocol, which all benefit from its security and simplicity.

Multi Factor Authentication
Multi-factor authentication is simple with this signature mechanism, since each factor is associated with one public/private key pair. Providers can enforce any level of desired security by requiring additional signatures on a request. A Provider may, for example, require three signatures from its members, by associating three public keys with each member. The three private keys of the member can be:

- (Have) Stored private key in any number of devices
- (Know) Private key generated from password, or PIN code + stored salt
- (Are) Private key generated from biometric like fingerprint or “eyeprint”, + stored salt

The system enables Providers to regulate how many signatures are required for an API call, and to set limits and rules for different devices and keys.

**Fraud**

With these security measures in place, as well as smart token capabilities, the potential for fraud is mostly eliminated.

1. **First party:** First party fraud is difficult to carry out in the Token system. For example, a Provider has the signature from a consumer, which proves that a transaction was made at a certain time and place, with the user’s phone and fingerprint.

2. **Second party:** Consumers can configure limits and restrictions on keys and/or tokens, thus making second party fraud difficult to accomplish. An end user may assign lower limits to their iPad, or children’s keys, while a business may assign restrictions on company voucher token, so that employees can only use the tokens for specific categories (e.g. meals and transportation).

3. **Third party:** Without the victim’s device private key, a fraudulent transaction is impossible. While an end user’s private key may be obtained by phone theft, hacking, etc., the end user is still protected through the use of multiple signatures and limits.

4. **Inducement:** Due to the certificate system, a Payer will always know who the true Payee is. Furthermore, all terms of a transaction or token are signed by the Payer, which makes deception very difficult. In a consumer use case, the transaction is confirmed by the user on a mobile app. In an enterprise use case, terms are verified and approved before any transaction is signed.

**Additional Notes on Security**

Apart from the security model outlined above, the TPS provides expected enterprise security features sufficient for a payment processor. These include services such as data breach
prevention and detection, full encryption, distributed databases, physical storage options for keys, detailed monitoring, high availability, disaster recovery plans, etc.

**Provider Mobile App Integration**

A common concern in the security of Token’s key system is how private keys are generated and associated to accounts at Providers. One of the possible ways this is done is through a trusted context in the Provider’s mobile app. If a Provider chooses to add Token capabilities to their iOS or Android app, an end user can enable Token from the app. This generates keys locally, and passes the public keys to the TPS. Then the Provider’s web server, as long as the user is authenticated, links the end user’s keys and IDs to the end user’s Provider accounts.

This is secure because the user must authenticate to the Provider in some way before enabling Token (password, MFA, etc.). Alternatively, end users can enable Token capabilities on the Provider's website, also authenticating before doing so. After this initial authentication to the Provider to link accounts, an end user will always authenticate using Token’s signature based security system, instead of through the traditional username and password systems.

![Diagram of Token user enablement](image)

**Figure 3**: Token user enablement. Note that while the TPS is usually run inside the Provider, in this case they are displayed separately to demonstrate that they are two different components (Provider web server and Token system)

**DETAILED DESCRIPTION OF PAYMENT PHASES**
This section will cover all the phases of a Token payment in detail. As has been discussed, Token supports two primary payment types: Direct Payment and Pre-authorized Payment.

A “Direct Payment” is a payment initiated by the Payer directly to a specified Payee account for a specific amount of money. The Token system supports near-real-time execution of payments between Token-enabled Providers, with a goal of providing funds availability to the Payee within milliseconds.

A “Pre-authorized Payment” is a payment or set of payments authorized by a Payer to a specific Payee. The payment is not executed immediately. Rather the payment authorization is recorded in the TPS at the Payer’s Provider in the form of a “smart token” with payment terms specified by the Payer and enforced by the TPS (see the Smart Token Capability section for details). The token ID is then given to the Payee who may, at some future time, request a payment by making a “redeem” API call to the Payer Provider’s TPS. The TPS will verify the Payee’s identity and validate the payment request terms against the authorization. If everything is valid, a payment will be executed. Note that this means that potentially many payments may result from a single payment authorization.

These two payment types differ in the Payment Initiation phase, so we will describe Initiation for each payment type separately. The payment phases after Initiation are the same for both payment types: Approval by Payer’s Provider, Clearing, Receipt, Settlement, Reconciliation. Each of those phases will be described in its own section.

**Direct Payment Initiation**

NOTE: Due to the design of the Token system the Initiation, Authentication and Payer Authorization phases as defined in the Solution Template are all accomplished simultaneously during payment initiation.

**Making a payment**

A Direct Payment is initiated via an API call to the TPS at a Provider by the End-user. The mandatory data elements of this call are:

- **Amount:** the amount of the payment specified as a number and a currency code
- **From account:** The Token Account Number (TAN) of the source account from which the payment will be made
- **Member ID:** The ID of the member who owns the source account
- **To account:** The Token account ID of the destination account
- **Description:** A string describing the purpose of the payment
Any Provider End-user can initiate or receive a payment via the Token system. Payment initiation and other payment-related operations are supported via the Token API provided by the Token Provider Software (TPS) running at each Provider. The “registered owner” End-user of an account can invoke this API through the Provider’s mobile app, the Provider web site and third-party apps and systems that have been authorized by the account owner. The API call must include a digital signature generated using a private key owned by the End-user.

**Detailed Example of Initiating a Direct Payment**

Alice, a customer of Provider A and using Provider A’s mobile app (as an example), wants to pay $10 to Bob, a customer of Provider B.

- Alice opens the “Initiate payment” screen in the app
- Alice enters:
  - Payer account: “Alice Checking” - one of her accounts at Provider A.
  - Payee account: The Token Account Number (TAN) for account “Bob Checking” at Provider B.
  - Amount: $10
  - Description: Lunch
- Alice is shown a confirmation screen with payment terms, including fee to be charged by Provider: $0.10.
- Alice confirms the payment
- The Provider’s mobile app makes a “transfer funds” API call to Token Provider Software (TPS) at Provider A (using the Token SDK), signing the call using the private key on the mobile device
- TPS at Provider A receives the API call, verifies Alice’s digital signature using the public key it has on file for Alice’s mobile device
- The TPS at Provider A proceeds to Payment Execution

**Pre-Authorized Payment**

The Token system also supports the execution of Pre-Authorized Payments. A pre-authorized payment uses a “smart token” to create an authorization for a specific Payee to request payments from the Payer’s account when specific terms defined by the Payer are met. This effectively provides a form of “pull payment”, a payment initiated by a Payee, but Token ensures that such payments are always under the control of the Payer. This general model supports many use cases across all use case categories.
The key concept behind a Token Pre-Authorized Payment is the creation of a “smart token” (see the Smart Token Capability section for details) by the TPS at the Payer’s Provider, specifying the terms for subsequent payment requests from a Payee. The smart token can be created directly by the Payer End-user, or can be created in response to a payment authorization request from a Payee. (e.g. A consumer service such as Spotify could request that its customer create a smart token that would allow it to receive the $10/month subscription fee directly via a payment from the customer’s bank account).

Once created, the ID of the token is given to the Payee. When the Payee wishes to initiate a payment from the Payer, it makes a “redeem” API call to the Payer’s TPS, providing the token ID and the terms of the requested payment. This call is signed using the private key of the Payee.

A redeem request contains the following fields:

- Token ID
- Payee member ID
- Amount
- Destination TAN

The TPS verifies the identity of the Payee using the digital signature, and verifies that the terms of the payment match the terms specified by the smart token. If verified, the payment will be executed in a similar fashion to a Direct Payment. If not verified, the redeem request is rejected.

The Payer may specify terms on the smart token that permit the Payee to make multiple redeem calls against the same token. In this sense, the token ID can be treated by the Payee in a similar fashion to a credit card on file. However, a persistent token is better than card on file in several ways:

- The token ID is not a “shared secret” like a credit card number, and therefore does not need to be kept secure. Tokens impose no “PCI compliance” issues on Payees.
- The Payer sets the terms for future payments, including restrictions on effective date range, number of uses, total funds cap, per-payment amount cap, etc. (See the Smart Token Capability section for more details.) This gives the Payer unprecedented control over recurring payments. Credit card and ACH payments provide no such controls.
- The Payer can revoke the token at any time, without requiring the cooperation of the Payee. Currently, recurring payments using credit cards or ACH credentials can only be revoked by making a request to the Payee.
Detailed Example of a Pre-Authorized Payment

This is an example of a pre-authorized payment for a recurring payment request:

- Acme, a corporate End-user, wants to set up a Pre-Authorized payment for a service provider “Ace Services” who bills Acme monthly for a variable amount that depends on services rendered, but is never to exceed $1,000 per month. Acme would make an API call (signed using Acme’s private key) to the TPS at their Provider (presumably from an internal financial system at the corporation) to create a smart token with the following terms:
  - Payer account: the TAN of one of Acme’s accounts at the Provider
  - Payee: The Token member ID of “Ace Services”
  - Recurrence: monthly
  - Payment limit: $1,000
  - Expiration date: 12/31/2016

- The TPS returns the token ID of this authorization to Acme, e.g. “t1”

- Acme provides the token ID to Ace

- Once per month Ace makes a “redeem” API call to the TPS at Acme’s Prover (presumably from a financial system at Ace) to request a payment. The call is signed using Ace’s private key. Sample payment request terms:
  - Token ID: t1
  - Amount: $850
  - Payee: Ace’s member ID
  - Payee account: the TAN of one of Ace’s accounts at their Provider

- The TPS at Acme’s Provider validates the payment request:
  - It verifies Ace’s digital signature on the call, ensuring that the request is actually being made by Ace
  - It looks up the terms on the smart token “t1” and verifies that the payment request matches the terms
    - Payee: Ace, which matches the Payee on the smart token
    - Amount: $800, which is under the per-payment limit of $1000
    - Date: 6/1/2016, which is before the expiration date
    - The last payment request against this token was received a month ago, which matches the recurrence limit
  - Once the payment terms have been verified, the payment is executed
Common Elements of Both Payment Types

**Authentication**
The Token solution is based on the use of cryptographically-secured identity for all parties involved in the payment process. When an End-User makes a Token API call to the TPS at their Provider, they generate a digital signature for that call using their private key and the data elements required for the API call. The TPS uses the associated public key that it has on file for the End-User to verify the signature.

Only the End-Users private key can generate a signature that can be verified with the corresponding public key. This ensures:

- **Identity:** That the API call could only have been initiated by that End-User
- **Non-repudiation:** The End-User cannot deny making the call
- **Reliability:** The terms of the payment have not been altered in any way in transit

If the signature cannot be verified, the payment request will be rejected.

Once the End-user identity has been verified by the TPS, the authorized operations can be carried out on the Provider accounts owned by the associated Provider customer.

**Platforms**
A payment can be initiated from any channel or device: a web page at the Provider, the Provider’s mobile app, any authorized third party app, at a retail Point of Sale terminal, etc. Token places no restrictions or requirements on the UI, sequence of steps, etc. All that is required is that the payment initiation platform be able to make an API call to the TPS at the Provider with the required data elements and signed using the private key of a party authorized to access the specified account. (Typically the End-user account owner or the Provider itself acting on behalf of the account owner.)

In this way Token is a true general-purpose platform for payments of all kinds. Token does not need to “own” the apps, sites, and user experiences in order to support payment being made. Token provides a multi-platform SDK to assist all parties and all platforms in making the API calls and generating the digital signatures.

**Account types**
Any type of account can be used as the source or destination of a payment as long as the Provider managing the account can credit and debit funds in the account “instantly”. In practice, there may be regulatory restrictions on the use of certain account types, such as “non-
transaction” accounts at Credit Unions. It is up to each Provider to determine which accounts can be involved in Token payments.

**Enrollment**
Providers can choose to Token-enable all accounts at the Provider or allow their customers to opt-in to “Token enabling” their accounts. An “enabled account” is assigned a Token Account Number, which is similar to the IBAN account number used in Europe: a single identifier that provides a direct mapping from that identifier to a specific account within a specific Provider. Note that Providers do not need to change the account numbering or identification scheme used in their back-office systems in order to deploy Token. Each Token-enabled account will be associated with a specific Token “member ID” associated with the Provider client who owns the account.

**Security**
All Token API calls must be digitally signed using a private key that is owned by and associated with the member who is authorized to control the account. In this way the TPS at the Provider can ensure that only authorized members have access to the account, and that all actions on the account are non-repudiable (i.e. could only have been executed by the owner of the account).

The release or sharing of a Token Account Number does not compromise security because possession of a TAN does not enable a bad actor to initiate or approve payments from that account; nor does it disclose any sensitive information about the account or account owner. Any operation on the account must be accompanied by a valid digital signature generated using a private key of the authorized account owner.

All calls are made via network connections secured using TLS. This end-to-end security prevents any third party from intercepting transmitted information about the payment.

**Privacy**
One benefit of the Token system is that no personal information need be exchanged between the parties of a payment. Token Account Numbers are abstract in that they don’t reveal the identity of the Provider customer or the underlying Provider account number. The use of a verifiable digital signature is the only proof that a Token party needs to provide in order to be Authenticated.

**Fees**
Fees charged at payment initiation (if any) are determined by the Provider deploying the solution. End-users must be informed of the fees to be charged in advance of payment initiation. The user interface of any consumer-facing payments service based on Token should present the
fee to the consumer prior to payment initiation. The fees charged to corporate customers should be agreed upon prior to the customer’s use of the Token system.

**Contextual data**
The initiator of a payment can provide additional contextual data that will travel with the payment. The contextual information can be based on an existing standard such as ISO 20022, or be structured in any form agreeable to the two parties.

**Payment Execution**
Once the payment has been initiated, all subsequent payment phases are the same for a Direct Payment and a Pre- Authorized Payment. For a Direct Payment these phases are triggered immediately upon payment initiation. For a Pre- Authorized Payment these phases will be triggered at the time of payment request from the Payee.

Token payments are executed via a “good funds” funds-transfer instruction from the Payer Provider to the Payee Provider. The Payer Provider first debits the funds from the Payer’s account (to ensure good funds) and then the Payer Provider sends a “digital IOU” to the Payee Provider, which is analogous to a “cashier’s check” in the paper-check world: a promise made from the Payer Provider to the Payee Provider that they will provide the specified funds in a future settlement operation. The Payee Provider will credit the funds to the Payee’s account upon receipt of the IOU.

**Approval by the Payer’s Provider**
Once the payment has been initiated, the TPS at the Payer Provider will engage the account management systems at the Provider to approve and process the payment. The TPS will access these existing Provider systems through a predefined Provider System interface that will be implemented as part of a Token integration at the Provider.

The TPS will verify that the source account specified by the Payer has sufficient funds to cover the payment amount. If not, the payment request will be rejected. The Provider’s account management system will also carry out any existing regulatory procedures needed to comply with AML and OFAC requirements. If the payment request violates any rules the payment will be rejected.

Once the account management system has verified funds and regulatory compliance, the TPS will direct the Provider account management system to debit the payment amount from End-user’s account into a “holding account” managed by the Provider. This ensures that all Token payments are “good funds”.
Once the funds have been reserved, the Payer Provider TPS creates a “Digital IOU” to the Provider that manages the specified Payee account. This Digital IOU is the basis for the Provider-to-Provider Clearing phase described in the next section. The Digital IOU has the following fields:

- Amount: the amount of the payment specified as a number and a currency code
- From Provider: the ID of the Provider initiating the payment
- To Provider: the ID of the Provider managing the account receiving the payment
- To account: the TAN of the account receiving the payment

The payment becomes final and irrevocable as of the creation of the IOU. The funds have been debited from the Payer’s account and it is now the responsibility of the TPS to ensure that the payment reaches the Payee.

This Provider Approval process will happen in “near real time”, limited only by the amount it takes to direct the Provider’s existing account management systems to debit the funds.

Clearing

Once Digital IOU has been created, the TPS at the Payer Provider initiates the transfer of the payment funds to the specified Payee account by sending the IOU to the TPS that manages that account via a Token API call. The call must be signed using the private key of the Payer Provider TPS.

All communication between Provider TPS instances is routed through and managed by the Token Hub. The Hub provides valuable convenience and security features, as well as services to help Providers manage their financial relationships with other Providers. See the sections on the Token Hub and Settlement for additional information.

The Token Hub receives the funds-transfer call and verifies the digital signature of the sending TPS. If the signature cannot be verified the payment is rejected. The Token Hub will adjust the net balance between the Payer Provider and the Payee Provider by the amount of the IOU.

The Token Hub forwards the IOU to the Payee Provider via an API call to the TPS, signed using the private key of the Token Hub.

The TPS at the Payee Provider receives the funds-transfer call and verifies the digital signatures of the Token Hub and the Payer Provider TPS. If the signatures cannot be verified the payment is rejected.
The TPS at the Payee Provider then engages with the account management system at the Payee provider to confirm that the Provider account associated with the TAN specified in the IOU is in “good standing” and is able to receive the payment funds. This can include regulatory compliance procedures such as AML and OFAC verification, etc. If there is a problem with the account, then the payment will be rejected. In this way the Payee Provider always has final control over whether a payment transaction is completed.

Receipt
Upon completion of the Clearing phase, the Payee Provider has assurance that the Payer Provider has guaranteed the funds for the payment will be delivered, and is therefore willing to make the funds available to the Payee. TPS at the Payee Provider will direct the account management system at the Provider to credit the payment amount to Payee account, transferring the funds from an internal “holding account”.

At this point the payment has been completed and the Payee has access to the funds.

Timing
Typically, a payment should be completed milliseconds after the payment call was originated by the Payer. The limiting factors are the speed and latency of the Internet connections between parties and the latency of the Providers’ account management systems.

Security and Fraud Prevention
The Token system uses digital signatures from end to end to verify Authentication and Authorization for all steps in the payment process, so it is extremely difficult for a bad actor to step in and spoof or subvert the payment process.

Both parties to a payment are “known customers” to their respective Providers, and all payments are ultimately transfers from one regulated Provider account to another. In this way the Token payment system leverages the existing KYC efforts of the Providers, as well as existing regulatory compliance processes for AML, OFAC, etc.

Payment Status
Provider End-users can make API calls to the TPS systems at their respective Providers to obtain the status of payments, including lists of all executed payment transactions, as well as details on any transaction including the contextual information for the payment. Given that Token payment transactions are near-real-time and always good-funds, typically the first opportunity for a Payee to obtain the status of a payment transaction is when payment has been received and funds made available.
Detailed Example of Payment Execution

In this case a payment of $10.00 has been initiated by Alice from her “Alice Checking” account at Provider A to account “Bob Checking” at Provider B.

- TPS at Provider A prepares to execute payment
  - Verifies funds availability in “Alice Checking”
  - Debits $10 from “Alice Checking” into cash holding account - description: “Payment to Bob’s account for ‘lunch’”

- TPS at Provider A creates a “digital IOU” to Provider B for the funds transfer IOU terms:
  - From: Provider A
  - To: Provider B
  - Amount: $10
  - Destination account: Token Account Number of “Bob Checking” account
  - Description: “lunch”

- At this point the payment is “good funds” and irrevocable by the Payee

- TPS at Provider A makes a “transfer funds” API call to Token Hub, signing the call using Provider A’s private key.

- Token Hub receives the API call, verifies the digital signature of Provider A

- Token Hub adjusts the “net balance” between Provider A and Provider B by $10 - Provider A owes Provider B an additional $10

- Token Hub annotates the “transfer funds” message, adding the current net balance amount

- Token Hub forwards “transfer funds” API call to Provider B, signing the call using Token Hub’s private key and passing along the digital signature and certificate from Provider A

- TPS at Provider B Receives API call, verifies digital signature of Token Hub and Provider A.

- TPS at Provider B verifies that net balance with Provider A is under the credit limit it is willing to extend to Provider A
  - If not, the IOU from Provider A is rejected and the payment is not processed

- TPS at Provider B completes the payment
  - Credits $10 to account “Bob Checking”

- At this point the payment is complete and Payee has access to the funds
Settlement

A Payee Provider will typically credit their End-user’s account upon receipt of an IOU from the Payer Provider in the Clearing phase, as the IOU is the digital analog of a “cashier’s check”, backed by the financial resources of the Payer Provider, not the Payer. When the Payee Provider credits funds to the End-user account, they are advancing the funds in the expectation that the “debt” from the Payer Provider will be settled between the institutions at some future time. Token provides a “periodic net settlement” mechanism between Providers to support this.

The Token Hub maintains a record of the “net balance” between any two Providers. This net balance is the difference between the sum of the amounts of all IOUs accepted by each Provider from the other at any time. As payments flow between Providers over time this net balance is adjusted.

Each Provider can specify a maximum “credit limit” that they are willing to extend to any other Provider. If at any time the net balance between the two Providers exceeds this limit (that is, the amount “owed” to Provider A by the partner Provider B exceeds the limit), Provider B must “pay down” the difference by transferring funds to Provider A.

The Token system supports this inter-Provider funds transfer via the Token Currency Ledger (TCL). This component is installed and operated by the Central Bank and provides an API to Providers that will transfer funds from the Provider’s account in the Central Bank to some specified other Provider’s account. The TCL will provide a receipt of the funds transfer. Any such transfer is “irrevocable good-funds” certified by the Central Bank, so the presentation of the receipt from one Provider to another will be accepted as proof of settlement of the amount of funds transferred.

A typical settlement flow:

- Provider A and Provider B are exchanging Digital IOUs to execute payments on behalf of their customers
- Provider A has established a “credit limit” for Provider B of $10,000
- The Token Hub shows that the net balance between Provider A and Provider B is “$9,500 owed by B to A”
- Provider B is processing payment of $1,000 to an account at Provider A
- Provider B recognizes that sending the $1,000 digital IOU to Provider A will exceed the limit set by A
● Provider B will make a “funds transfer” API call to the TCL, signed using Provider B’s private key
  ○ Amount: $5,000
  ○ From: Provider B
  ○ To: Provider A

● The TCL will verify the digital signature of Provider B. If the signature cannot be verified, the funds-transfer request will be rejected.

● The TCL will direct the account management systems at the Central Bank to transfer funds from the Central Bank account Provider B to the account of Provider A

● The TCL will return a receipt for the transfer to Provider B, signed with the private key of the TCL

● Provider B will send the funds-transfer receipt to Provider A via the Token Hub

● The Token Hub will verify the TCL signature on the receipt and adjust the net balance between Provider B and Provider A by the amount of the funds transfer. The new balance is $4,500.

● The Token Hub will send the receipt to Provider A

● Provider A will note that Provider B has reduced its “outstanding debt” by $5,000

● Provider B will send the Digital IOU for $1,000 to Provider A

● The new outstanding balance at the Token Hub will be $5,500

Reconciliation

Both the Payer Provider’s and Payee Provider’s TPS systems maintain a record of every transaction. The Payer Provider has a record of the Payer End-user’s authorization of the payment, including the digital signature that can only have been generated by the Payer End-user. Both Providers have a record of the Provider-to-Provider payment execution in the form of the Digital IOU. The IOUs each have the digital signature of the Provider that initiated the payment.

For a Pre-Authorized payment, the Payer Provider’s TPS has a record of the payment authorization, including the digital signature of the End-user on the smart token. The Payer Provider also has a record of the payment request(s), signed by the End-user that requested the payment against the token. Thus all payment transactions can be tied to specific approvals and actions of the parties involved.
The processes and timeframes for handling unauthorized, fraudulent, erroneous, or otherwise disputed payments, and the rules for allocation of liability among, and substantive liability limits for, all parties involved in the payment will be addressed during the creation of a Rulebook for Token Payments. As a technology provider, Token is reaching out to partners to assist in this process. As of the time of submission of this proposal NACHA has agreed to work with Token to establish the rules and policies.

Payment Process Flow Diagrams

**Direct Payment**

Alice pays $10 to Bob by sending a Direct Payment from her account to TAN123, Bob’s account

Initiation → Receipt

![Diagram of Direct Payment](image)

**Pre-Authorized Payment Initiation & Redemption**

Alice issues a smart token to merchant “Ace” that allows Ace to request payments up to $100

Initiation → Receipt
Figure 5: Pre-authorized payment with a token

Settlement
Provider A transfers $10,000 to Provider B to settle outstanding IOUs

Figure 6: Token settlement
Multi-currency & cross-border

Foreign exchange (FX) is essentially handled the same way that domestic transactions are handled using the Token Hub, with the addition of an FX service provider.

When two Providers in different countries using different currencies perform transactions, the Token Hub keeps track of relative balances using two counters (one for each currency).

Each Hub transaction thread between two parties has three elements:

1. A sequence number
2. The transaction
3. The current net relative balance after the transaction is posted

Three kinds of transactions (item #2) can be posted to a thread:

1. Signed IOU of $xx from party A to party B per transactionID y
2. Offer to exchange, e.g., swap 1100 USD for 1000 EURO
3. Payment (the party who is in debt presents a distributed ledger receipt signed within the last 1 hour indicating a payment associated with this thread; whether it was initiated by Provider A or by the FX provider on behalf of the debt on this particular thread)

The Token Hub calculates the net balance between the parties based on the evidence presented, so there is continuous reconciliation with digital proof.

Each Provider tracks the total IOU balance of the counterparty (adds the net balance in all of the threads).

A Provider can “pay down” the IOU balance via an FX service provider (which can be a large global Provider operating in a large number of countries).

The payment transaction to the credit Provider on the TCL that is done by the FX service contains the following:

1. The debtor Provider (since a third Provider may be paying for the debtor Provider) and
2. The threadID of the conversation (to prevent a payment from being posted to >1 thread)

For example:
1. Provider A operates in USD; Provider B operates in EUR

2. When Provider A sends money to Provider B, Provider A writes an IOU for 20 EUR. Similarly, when Provider B wants to send money to Provider A, Provider B writes an IOU in USD.

3. When Provider A’s IOU credit limit is overdrawn, Provider A sends an IOU in USD to the FX service provider in USD. The FX service provider makes the DL transfer to Provider B (making sure to note in the payment that this is a payment made for Provider A/ threadID) and hands the signed receipt to Provider A, so Provider A can post it as a payment on the relevant thread.

**Part A, Section 2: Use Case Description**

In this section the stakeholders are defined as:

End user: Payer and Payee
Tech provider: Token
Processor: Payer and Payee Providers

**Business to Business (B2B)**

In a B2B application such as Business A paying an invoice from Business B, the payment may be initiated from an ERP system. The ERP system provider will have integrated Token as a payment mechanism and calls the Token API at the Payer’s Provider (direct payment) or sends the Payer a smart token (pre-authorized payment) for later redemption.

So for the B2B use case, both Token payment types apply. See [Direct Payment](#) and [Pre-Authorized Payment](#) for detailed flow.

<table>
<thead>
<tr>
<th>Direct payment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initiation</strong></td>
</tr>
<tr>
<td>Payer’s Provider</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>Clearing</td>
</tr>
<tr>
<td>Receipt</td>
</tr>
<tr>
<td>Settlement</td>
</tr>
<tr>
<td>Reconciliation</td>
</tr>
</tbody>
</table>

### Pre-authorized payment

<table>
<thead>
<tr>
<th></th>
<th>End users</th>
<th>Technology providers</th>
<th>Processors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>Payer specifies terms of smart token and submits TPS at Payer Provider. Payer gives token ID to Payee</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redeem request</td>
<td>Payee submits request for payment according to smart token to TPS at Payer Provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approval by the Payer’s Provider</td>
<td></td>
<td></td>
<td>Debit funds from Payer’s account after regulatory compliance check passes</td>
</tr>
<tr>
<td>Clearing</td>
<td></td>
<td>Send digital IOU to</td>
<td>Credit funds to</td>
</tr>
</tbody>
</table>

© 2016 Token, Inc.
<table>
<thead>
<tr>
<th></th>
<th>Payee Provider</th>
<th>Payee’s account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receipt</td>
<td>Receipt info available to all parties</td>
<td>Account ledgers update</td>
</tr>
<tr>
<td>Settlement</td>
<td>Monitor Payer Provider’s credit exposure</td>
<td>Send funds to Feds as needed</td>
</tr>
<tr>
<td>Reconciliation</td>
<td>Initiation request incl. digital signature of Payer and Payee, Digital IOUs</td>
<td></td>
</tr>
</tbody>
</table>

As a high-level example, a third party developer could build a corporate application using pre-authorized payments to handle cash sweeping for treasury departments:

- The corporate financial system is granted access to multiple accounts at multiple Providers using tokens
- The system can make real-time calls to the TPS systems at the Providers to get balances and transfer funds
- “Access tiers” can be controlled through separate tokens. E.g. a “read-only token” grants balance and transaction history; a “standard token” adds the right to initiate payments up to $1,000; a “restricted token” allows movement of large sums but requires multiple signatures.

**Business to Person (B2P)**

In a B2P application such as Business A making a salary payment to its employees, the payment may be initiated from an HR system. The HR system provider will have integrated Token as a payment mechanism and calls the Token API at the Payer’s Provider (direct payment) to initiate the payments.

For the B2P use case, the Token direct payment type applies. See Direct Payment for detailed flow.
### Direct payment

| Initiation | Payer specifies terms of payment and submits to TPS at Payer Provider |
| Approval by the Payer’s Provider | Debit funds from Payer’s account after regulatory compliance check passes |
| Clearing | Send digital IOU to Payee Provider | Credit funds to Payee’s account |
| Receipt | Receipt info available to all parties | Account ledgers update |
| Settlement | Monitor Payer Provider’s credit exposure | Send funds to Feds as needed |
| Reconciliation | Initiation request incl. digital signature of Payer and Payee, Digital IOUs |

**Person to Business (P2B)**

In a P2B application such as a Consumer paying online at an online e-commerce vendor, the payment may be initiated from the Payer’s mobile device. Direct payment is the most likely payment type to be used, although the pre-authorized payment type is also an option. In a direct payment, the Payer initiates the payment from her mobile device and submits to her Provider for further processing.

So for the P2B use case, both Token payment types apply. See Direct Payment and Pre-Authorized Payment for detailed flow.
<table>
<thead>
<tr>
<th></th>
<th>Payer Provider</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval by the Payer’s Provider</td>
<td></td>
<td>Debit funds from Payer’s account after regulatory compliance check passes</td>
</tr>
<tr>
<td>Clearing</td>
<td></td>
<td>Send digital IOU to Payee Provider</td>
</tr>
<tr>
<td>Receipt</td>
<td></td>
<td>Receipt info available to all parties</td>
</tr>
<tr>
<td>Settlement</td>
<td></td>
<td>Monitor Payer Provider’s credit exposure</td>
</tr>
<tr>
<td>Reconciliation</td>
<td></td>
<td>Initiation request incl. digital signature of Payer and Payee, Digital IOUs</td>
</tr>
</tbody>
</table>

### Pre-authorized payment

<table>
<thead>
<tr>
<th></th>
<th>End users</th>
<th>Technology providers</th>
<th>Processors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>Payer specifies terms of smart token and submits TPS at Payer Provider. Payer gives token ID to Payee</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redeem request</td>
<td>Payee submits request for payment according to smart token to TPS at Payer Provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approval by the Payer’s Provider</td>
<td></td>
<td></td>
<td>Debit funds from Payer’s account after regulatory compliance check</td>
</tr>
</tbody>
</table>
Person to Person (P2P)
In a P2P application such as a Venmo-like mobile app, the payment is initiated from the Payer’s mobile device and the Payee is notified of funds available on her mobile device.

For the P2P use case, the Token direct payment type applies. See [Direct Payment](#) for detailed flow.

<table>
<thead>
<tr>
<th>Direct payment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>End users</strong></td>
</tr>
<tr>
<td>Initiation</td>
</tr>
<tr>
<td>Approval by the Payer’s Provider</td>
</tr>
<tr>
<td>Clearing</td>
</tr>
<tr>
<td>Receipt</td>
</tr>
</tbody>
</table>
As an example, a third party app vendor could quickly build a Venmo-like mobile app using the Token API to facilitate P2P payments. The vendor would just need to set up a directory service mapping publicly-know “friendly names” of users to Token account numbers. The app would then use the Token SDK to make API calls to the TSP at a user’s Provider and “register itself” by associating a private/public key pair generated by the app with the user’s account at the provider.

- The payment app vendor would create a directory service that would allow people to register a public “friendly name” identifier such as their mobile number and link it to a Token Account Number
- To send a payment to another party, the app user would enter the Payee’s “friendly name” into the app and specify the amount of money to send
- The app would look up the friendly name in the directory and get back the TAN
- The app would make an API call to the TPS at the user’s Provider to initiate a Direct Payment to the Payee’s TAN, signed by the private key in the app
- The TPS would verify the signature and execute the payment
- The app would report success or failure of the payment to the user immediately

### Part A, Section 3: Use Case by Effectiveness Criteria

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>U.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>-------</td>
<td>-----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
</tr>
<tr>
<td></td>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.6</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>E.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>U.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.10</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Payer Authorization</strong></td>
<td>U.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Approval by the Payer’s Provider</strong></td>
<td>S.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>F.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>F.5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Clearing</strong></td>
<td>E.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Receipt</strong></td>
<td>U.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>--------</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td></td>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.6</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Settlement</td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>F.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>F.5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Settlement</td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>F.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Reconciliation</td>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>E.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.6</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
PART B: BUSINESS CONSIDERATIONS

1. Implementation Timeline

Development timeline

The Token system is currently under development and is expected to be completed by the end of 2016. Token uses agile software development methods and practices. Since all four use cases are supported through the same open API, they are all supported in the first release.

![Figure 7: Implementation Timeline]

Typical customer engagement plan

Since Token is still in a development phase, thus the customer engagement plan is an estimate based on industry experience.
Market ubiquity plan

Token’s plan for reaching market ubiquity is to first focus on the 10 largest Providers in the market. They represent roughly 2/3 of the total market. Using strategic partnerships, we estimate it will take approximately 24 months to reach this point.

The long tail of the Provider market will be reached in an additional 3 years.

Interoperability with existing solutions

While the Token system is designed and built from a clean sheet and utilizes state-of-the-art technologies to achieve a fast and secure payments, interoperability with legacy systems has been a key design aspect. The Token system integrates with a Provider’s existing account management system and until ubiquity has been reached, the Token system can interact with other, non real-time payment rails.

Initial and subsequent features

The functionality outlined in this proposal will be available at the time of product release at the end of 2016.
Future product releases will focus on extended capabilities, such as the creation of key dependencies and risks

The key dependency for Token to deliver the proposed system by the end of 2016 rests in its ability to hire and retain key development staff in a highly competitive labor market. Token is planning to raise capital in the second half of 2016 to fund the continuous development of the solution and the appropriate sales, marketing and technical support efforts.

2. Value Proposition and Competition

Fees are defined by the Providers and the rate schedule must be publically available. Token recommends a pricing model that is transparent and based on a fee representing a percentage of the transaction value. Variations of the pricing model may exist to address the various use cases. Revenue from fees is shared between Token (technology provider) and the Providers (processors) participating in the transaction. Each of the revenue share partners may share their revenue further with additional service providers.

The Token system is based on an open, secure API allowing third party developers to build innovative applications directly on top of the Token payment rail. All features and functionality are available to all developers. This creates a competitive app ecosystem similar to those of Apple and Google. Apps using the Token development platform and payment rail are in general offered for free, but may incur API access charges.

Business to Business (B2B)

<table>
<thead>
<tr>
<th></th>
<th>End users</th>
<th>Technology providers</th>
<th>Processors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>Payer: 1) Granular control of payment instructions. 2) Low risk of security exposure.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td>Certainty of authorization</td>
<td>Payer Provider: Certainty of authorization</td>
</tr>
<tr>
<td>Payer Authorization</td>
<td>Payee: Certainty of good funds.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approval by the Payer’s Provider</td>
<td></td>
<td></td>
<td>Payer account debited before IOU created</td>
</tr>
<tr>
<td>Clearing</td>
<td>Payee: 1) Certainty of funds received. 2) Instant transfer</td>
<td>Revenue</td>
<td>Revenue</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Receipt</td>
<td>Knowledge of transaction status at any point during transaction lifecycle (if exposed)</td>
<td>Knowledge of transaction status at any point during transaction lifecycle</td>
<td>Knowledge of transaction status at any point during transaction lifecycle</td>
</tr>
<tr>
<td>Settlement</td>
<td></td>
<td></td>
<td>Credit exposure monitoring</td>
</tr>
<tr>
<td>Reconciliation</td>
<td></td>
<td></td>
<td>Full trace of all transactions and fully non-repudiated</td>
</tr>
</tbody>
</table>

**Business to Person (B2P)**

<table>
<thead>
<tr>
<th></th>
<th>End users</th>
<th>Technology providers</th>
<th>Processors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>Payer: 1) Granular control of payment instructions. 2) Low risk of security exposure.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td>Certainty of authorization</td>
<td>Payer Provider: Certainty of authorization</td>
</tr>
<tr>
<td>Payer Authorization</td>
<td>Payee: Certainty of good funds.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approval by the Payer’s Provider</td>
<td></td>
<td></td>
<td>Payer account debited before IOU created</td>
</tr>
<tr>
<td>Clearing</td>
<td>Payee: 1) Certainty of funds received. 2) Instant transfer</td>
<td>Revenue</td>
<td>Revenue</td>
</tr>
<tr>
<td>Receipt</td>
<td>Knowledge of transaction status at any point during</td>
<td>Knowledge of transaction status at any point during</td>
<td>Knowledge of transaction status at any point during</td>
</tr>
</tbody>
</table>
### Person to Business (P2B)

<table>
<thead>
<tr>
<th></th>
<th>End users</th>
<th>Technology providers</th>
<th>Processors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initiation</strong></td>
<td>Payer: 1) Granular control of payment instructions. 2) Low risk of security exposure.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
<td>Certainty of authorization</td>
<td>Payer Provider: Certainty of authorization</td>
</tr>
<tr>
<td><strong>Payer Authorization</strong></td>
<td>Payee: Certainty of good funds.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Approval by the Payer’s Provider</strong></td>
<td></td>
<td></td>
<td>Payer account debited before IOU created</td>
</tr>
<tr>
<td><strong>Clearing</strong></td>
<td>Payee: 1) Certainty of funds received. 2) Instant transfer</td>
<td>Revenue</td>
<td>Revenue</td>
</tr>
<tr>
<td><strong>Receipt</strong></td>
<td>Knowledge of transaction status at any point during transaction lifecycle (if exposed)</td>
<td>Knowledge of transaction status at any point during transaction lifecycle</td>
<td>Knowledge of transaction status at any point during transaction lifecycle</td>
</tr>
<tr>
<td><strong>Settlement</strong></td>
<td></td>
<td></td>
<td>Credit exposure monitoring</td>
</tr>
<tr>
<td><strong>Reconciliation</strong></td>
<td></td>
<td></td>
<td>Full trace of all transactions and fully non-repudiated</td>
</tr>
</tbody>
</table>
Person to Person (P2P)

<table>
<thead>
<tr>
<th></th>
<th>End users</th>
<th>Technology providers</th>
<th>Processors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>Payer: 1) Granular control of payment instructions. 2) Low risk of security exposure.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td>Certainty of authorization</td>
<td>Payer Provider: Certainty of authorization</td>
</tr>
<tr>
<td>Payer Authorization</td>
<td>Payee: Certainty of good funds.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approval by the Payer’s Provider</td>
<td></td>
<td></td>
<td>Payer account debited before IOU created</td>
</tr>
<tr>
<td>Clearing</td>
<td>Payee: 1) Certainty of funds received. 2) Instant transfer</td>
<td>Revenue</td>
<td>Revenue</td>
</tr>
<tr>
<td>Receipt</td>
<td>Knowledge of transaction status at any point during transaction lifecycle (if exposed)</td>
<td>Knowledge of transaction status at any point during transaction lifecycle</td>
<td>Knowledge of transaction status at any point during transaction lifecycle</td>
</tr>
<tr>
<td>Settlement</td>
<td></td>
<td></td>
<td>Credit exposure monitoring</td>
</tr>
<tr>
<td>Reconciliation</td>
<td></td>
<td></td>
<td>Full trace of all transactions and fully non-repudiated</td>
</tr>
</tbody>
</table>

non-repudiated
3. Integration Effort

None of the estimates below include time for testing and verification.

Business to Business (B2B)

End-users
Payee and Payer (in case of pre-authorized payment) applications integrate the Token solution using the provided SDKs (available for popular programming languages).

Time estimate: 10 days.

New functionality released approximately 4x/year. Continuous hot fixes.

Technology Provider
No incremental effort to support a new use case and a new customer.

Processor
Unless Token was already implemented to support any of the other user cases (in which case no incremental effort is required), Providers must integrate the Token system with their account management system. There are four basic calls: get account information, get account balance, get account history, transfer funds.

Time estimate: 2 - 12 weeks.

Payer’s Provider must integrate Token SDK in Provider’s mobile app.

Time estimate: 4 weeks.

New functionality released approximately 4x/year. Continuous hot fixes.

Business to Person (B2P)

End-users
Payee applications integrate the Token solution using the provided SDKs (available for popular programming languages).

Time estimate: 10 days.

New functionality released approximately 4x/year. Continuous hot fixes.

Technology Provider
No incremental effort to support a new use case and a new customer.

**Processor**

Unless Token was already implemented to support any of the other user cases (in which case no incremental effort is required), Providers must integrate the Token system with their account management system. There are four basic calls: get account information, get account balance, get account history, make transfer.

Time estimate: 2 - 12 weeks.

New functionality released approximately 4x/year. Continuous hot fixes.

**Person to Business (P2B)**

**End-users**

Payee and Payer applications integrate the Token solution using the provided SDKs (available for popular programming languages).

Time estimate: 10 days.

New functionality released approximately 4x/year. Continuous hot fixes.

**Technology Provider**

No incremental effort to support a new use case and a new customer.

**Processor**

Unless Token was already implemented to support any of the other user cases (in which case no incremental effort is required), Providers must integrate the Token system with their account management system. There are four basic calls: get account information, get account balance, get account history, make transfer.

Time estimate: 1 - 12 weeks.

New functionality released approximately 4x/year. Continuous hot fixes.

**Person to Person (P2P)**

**End-users**

Payee and Payer applications integrate the Token solution using the provided SDKs (available for popular programming languages).

Time estimate: 10 days.
New functionality released approximately 4x/year. Continuous hot fixes.

**Technology Provider**

No incremental effort to support a new use case and a new customer.

**Processor**

Unless Token was already implemented to support any of the other user cases (in which case no incremental effort is required), Providers must integrate the Token system with their account management system. There are four basic calls: get account information, get account balance, get account history, make transfer.

Time estimate: 1 - 12 weeks.

New functionality released approximately 4x/year. Continuous hot fixes.
PART C: SELF-ASSESSMENT AGAINST EFFECTIVENESS CRITERIA

1. Ubiquity

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>#</td>
<td>Consideration Name</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.1</td>
<td>Accessibility</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.2</td>
<td>Usability</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.3</td>
<td>Predictability</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.4</td>
<td>Contextual data capability</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.5</td>
<td>Cross-border functionality</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.6</td>
<td>Applicability to multiple use cases</td>
</tr>
</tbody>
</table>

**Justification for U.1:**

U.1.1: All types of payment to/from Accounts based in the U.S. held at all Depository Institutions are facilitated since they happen instantly through IOUs using Token Hub and the settlements at the Token Central Provider Software. Regulated Non-Provider Account Providers are able to continue their intra-Provider operations normally, and any inter-Provider transaction would be facilitated as well. See Payment Execution for more details.

U.1.2: All Entities and Payees are, to some extent, associated with a Depository Institution. Thus, in any transaction between Providers, we follow the Payment Execution flow detailed above. All intra-Provider transactions can also be immediately settled by crediting and debiting the accounts of the Payer and Payee, respectively. Consequently, the payments of all Entities can reach any and all Payees.

U.1.3: Token supports multi-currency operations using the [Token Foreign Exchange Service](#).
U.1.4: The ability to make payments to/from Regulated Non-Provider Account Providers is supported.

U.1.5: The Token Solution provides a Token Provider Software (TPS) which creates a narrow communication to the Provider’s existing infrastructure. This means the Providers don’t need to replace their current system, but instead simply add another layer on top of their software. In addition, the Solution provides a simple and developer-friendly SDK to our RESTful API which greatly facilitates implementation by Regulated non-Provider Account Providers and Third-party service providers. Furthermore, Token has an adoption plan which involves integrating Token features into the mobile apps of Providers, in order to more easily on-board customers.

U.1.6: The Interoperability aspects of the Token Solution is the communication between the Token Provider Software and the Core Provider Software, which is part of the Token layering design on top of Providers’ current system, and the communication between Token and Providers, which is done through the RESTful API. All other communications are part of the Token software. Thus, all entities are connected and get send a receive payments to each other.

**Justification for U.2:**

By creating a simple and flexible solution that can be used for Providers when building their applications, the solutions fully satisfies all usability criteria.

U.2.1: The Solution is available to End Users in a variety of circumstances. Since Providers can use the Token SDK to call the RESTful API and build applications through it, the Token Solution can be used to move money for any application. This would include payments through mobile device, online, on a laptop, on a tablet, offline (Bluetooth), etc. This would also include use cases such as bill pay, merchant online checkout, salary payments, in-store checkout, rent payments, spit restaurant bill, in-app purchases, etc.

U.2.2: Application developers can create their service in such a way that it maps user’s Token Account Number (TAN) with any sort of alias (e.g. with a name, email address, and/or phone number), so consumers would never need to remember or enter their TAN. The system might require more information (e.g. biometrics, second authorization from another person) depending on the preferences defined by the user (e.g. “ask for my fingerprint if I’m making a purchase over $1000).

U.2.3: The Solution is indeed accessible to End Users on a 24x7x365 basis.

U.2.4: Since applications are build using the Solution as a foundation to move money, it is the responsibility of the application developers to make their products easy to use. With that said, there is nothing on the Solution side that would make it any difficult for that to happen, and if
anything the simplicity of the SDK makes it extremely easy for Providers to build user friendly applications that accommodate varying levels of End-User technological proficiency.

**Justification for U.3:**

Token provides consistency and predictability for its users, partners, and customers. This includes User experience, sign up, features, and agreements.

U.3.1: This is ensured by the design, since the protocols and infrastructure have been defined and all that is needed for implementation is the integration between the Token Software and the Provider’s account management system.

U.3.2: The baseline features are defined, documented and communicated. The Providers have part of the responsibility in communicating payment details to the End User, which they are required to do to be compliant.

U.3.3: The Solution uses standard messaging protocols, like email, text, push notifications, etc. It also makes it flexible by allowing the Providers to choose their messaging protocols with their user.

U.3.4: Token API does not discriminate in any way, and all features are offered to Providers who use the Token software.

U.3.5: The error resolution protections, rights, and liabilities for end users have not yet been defined.

U.3.6: The Solution can be described as “smart token”, which can be commonly understood and distinguishable from other payment methods. Throughout this document we have been describing the various parts of the system by using the “Token” brand (e.g. Token Bank Software (TBS)), but that is not a requirement of the Solution.

**Justification for U.4:**

The smart token capability creates an ideal environment for the integrations and transferring of contextual Data of any type.

U.4.1: The smart token can be arbitrarily complex with a set of rules and descriptions for each payment authorization, which allows all contextual Data to be attached to a given payment.

U.4.2: The contextual Data can be easily extracted by the Providers from the smart token.

U.4.3: Flexibility/adaptability is at the core of the smart token design, allowing Data to be associated with a given payment.
**Justification for U.5:**

U.5.1: Cross-border transactions function very much the same way as domestic transaction. The security mechanisms are the same.

U.5.2: The Token system is fully interoperable with other payment systems such as FPS in the UK and SEPA in the EEA.

U.5.3: Token provides full transparency regarding any fees associated with any payment, whether domestic or cross-border involving FX, or not.

U.5.4: This is handled by the Token Foreign Exchange Service (TFXS).

U.5.5: Cross-border functionality is planned for the initial implementation.

**Justification for U.6:**

The Token Solution initially supports a large number of use cases. The combination of the versatile smart token capability (which allows rules and data to be attached to any payment), the instant transactions (which happen through RESTful API commands) and high level of security (which uses digital signatures, no shared secrets, and multiple levels of authentication), the Solution is able to support all targeted use cases mentioned (B2B - ad hoc low value, B2P - ad hoc high value, B2P - ad hoc low value, and P2B ad hoc real time). Moreover, the Solution remains flexible so other use cases can also fit the scheme.

**2. Efficiency**

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>#</td>
<td>Consideration Name</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.1</td>
<td>Enables competition</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.2</td>
<td>Capability to enable value-added services</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.3</td>
<td>Implementation timeline</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.4</td>
<td>Payment format standards</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.5</td>
<td>Comprehensiveness</td>
</tr>
<tr>
<td>------------</td>
<td>-----</td>
<td>------------------</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.6</td>
<td>Scalability and adaptability</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.7</td>
<td>Exceptions and investigations process</td>
</tr>
</tbody>
</table>

**Justification for E.1:**

Since Token is a payment system layer on top of banks that can be accessed and used by Providers, it is very effective at enabling competition.

E.1.1: Providers can use the Token SDK to access the RESTful API and build their applications and platforms on top of our payment system. The Solution is not tied to any providers and thus allows the choice of Provider(s) based on factors including, but not limited to, services and price.

E.1.2: Providers can use the Token SDK to access the RESTful API and build their applications and platforms on top of our payment system. The Solution is not tied to any providers and thus allows the easy switch among Provider and/or use of multiple providers.

E.1.3: The Provider that uses our service has the responsibility of setting their fees and communicating to the End User the total cost associated with a given payment and/or service.

E.1.4: The Solution allows Providers, regardless of their size or incumbency, to provide services as long as the Providers meet participation requirements.

**Justification for E.2:**

E.2.1: Providers can use the Token SDK to access the RESTful API and build their applications and platforms on top of our payment system, allowing them to offer value-added services to any Entity.

E.2.2: The Solution allows Providers, regardless of their size or incumbency, to provide value-added features as long as the Providers meet participation requirements.

E.2.3: The Provider that uses our service has the responsibility of setting their fees and communicating to the End User the optionality of a given value-added service.

**Justification for E.3:**
E.3.1: Token is a startup organization and as such there is no comparable historical data from within the organization. However, Token has 100% confidence in its ability to execute the plan. Token’s senior staff has an exceptionally successful track record in delivering technology solutions to the financial market.

**Justification for E.4:**

The Token Solution messaging is a combination of accepting format standards such as ISO 20022, while also creating a new, flexible API with its own data formats.

E.4.1: Yes. For instance, accept "contextual information" for a payment using ISO 20022

E.4.2: Cross-border interoperability in the message format is supported through ISO 20022. Support for other message formats can be added.

E.4.3: The Token Solution accepts ISO 20022, but it is mostly a newly defined, developer-friendly, API with its own data formats, which encapsulates user auth, account link, unlink, etc. Based on its design, this API should be easy, practical, and cost effective to adopt.

E.4.4: The API message format is extremely flexible, since it allows for arbitrarily complex rules for each smart token, and also easy to update from a developer perspective. Consequently, it facilitates innovation.

E.4.5: The Token API is extremely transparent and well documented for any developers interested in using the solution.

**Justification for E.5:**

The Token solution encapsulates all relevant aspects of the end-to-end payment process with a technical design that support its features in several different criteria.

E.5.1: The Solution enables all relevant aspects of the end-to-end payment process. See Token Payments for more details.

E.5.2: The technical design of the Solution adequately supports all of its features, as explained in PART A of this document.

**Justification for E.6:**

The strong technical design of the Token Solution supports the projected use cases, was being scalable and adaptable.
E.6.1: The technical design supports projected use cases.

E.6.2: The Token system is designed for elastic scalability, meaning the ability to scale horizontally and vertically with demand. Each individual TPS instance can be configured to handle the anticipated payments volume of the given Provider. The central Token components, such as the Token hub are deployed within top-tier infrastructure providers such as IBM SoftLayer and Amazon AWS. The Token components are designed to be deployed using Docker containers, thus providing a highly flexible operating environment.

The most CPU intensive operation in the Token system is signature verification. In preliminary tests, the Token system verifies over 5,000 signatures per second per CPU.

E.6.3: By creating a flexible RESTful API, and a compatible SDK to it, the technical design is readily adaptable to ongoing developments.

**Justification for E.7:**

E.7.1: The Solution notifies Providers of details of the transaction, and any potential exceptions that occur. The Provider can then package such information and showcase it to the user the best way it judges to be fit given the situation (e.g. email, text, push notification, screen in app flow, etc.).

E.7.2: The Solution creates, records, and retains information, making it easy to trace back previously originated payments.

E.7.3: The detailed transaction logging data maintained by the Token solution can be used as the foundation for pattern analysis and other forms of exception detection and management.

### 3. Safety and Security

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Safety and Security</th>
<th>Effectiveness Criteria Self-Assessment</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>S.1</td>
<td>Consideration Name: Risk management</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.2</td>
<td>Payer authorization</td>
<td>X</td>
</tr>
<tr>
<td>---------------------</td>
<td>------</td>
<td>---------------------</td>
<td>----</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.3</td>
<td>Payment finality</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.4</td>
<td>Settlement approach</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.5</td>
<td>Handling disputed payments</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.6</td>
<td>Fraud information sharing</td>
<td>N/A</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.7</td>
<td>Security controls</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.8</td>
<td>Resiliency</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.9</td>
<td>End-user data protection</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.10</td>
<td>End-user /provider authentication</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.11</td>
<td>Participation requirements</td>
<td>X</td>
</tr>
</tbody>
</table>

**Justification for S.1**

S.1.1: As stated in self-assessment section G - Governance, these policies have not yet been fully developed. Token and NACHA will collaborate on providing effective, transparent governance in time for the product release.

S.1.2: The Token system mitigates Settlement risk by allowing all Providers to determine their “exposure” relative to any other Provider. If the amount owed to a Provider by another exceeds its specified limits it can refuse to process additional IOUs from the other Provider until a settlement payment has been made through the TCL.

S.1.3: Due to the Token system being highly automated, resilience to operational errors is very high. Manual and human intervention is kept at a minimum. Some risks involve incorrect storage of private keys, loss/theft of keys, account recovery without keys, and bugs or unavailability of legacy software rails.
S.1.4: Risks of fraudulent or erroneous transactions is minimal and related costs are low. This is due to the signature and certificate security model, as well as tight controls on user authentication and user intent for transactions. Smart token features enable end users and Providers to set limits on untrusted devices, untrusted merchants, or certain keys. See Token Security section.

S.1.5: As stated in self-assessment section G - Governance, these policies have not yet been fully developed. Token and NACHA will collaborate on providing effective, transparent governance in time for the product release.

S.1.6: The risk framework will be reviewed and updated frequently, as well as analyzed upon key events such as changes in laws, regulations, adoption, software updates, etc.

**Justification for S.2:**

S.2.1: Both types of payments, direct, and pre-authorized payments, are subject to the Payer authenticating to his/her Provider. On direct payments, API calls from the Payer to the Provider are signed using all required keys. On pre-authorized payments, the Payer signs the Token payload, and it must be verified by the Payer’s provider for authorization before the transaction goes through. The only difference in these two cases is the order in which the data flows (see Payment Flows).

S.2.2: The Payer can create a token with any of the smart token capabilities, which define Payee, source account, limits, times, etc. Token creation is signed by the Payer and verified by the Payer’s Provider. The token terms are available to both the Payer’s and Payee’s Providers, and can be accessed by both end users (with signatures). The Payee will be able to redeem the token if it is made out to them.

S.2.3: Token terms and parameters can be changed at any time by the Payer (creator of the token). Token revocation and suspension are also available. Both of these are simple signed API calls from the Payer to the Payer’s Provider.

**Justification for S.3:**

S.3.1: The Payer’s Provider checks for good funds on each payment and decides whether or not to approve it. Every transaction goes through and must be approved by both the Payer and Payee’s Providers. See Payment Flows for more details.

S.3.2: The stage where a payment is irrevocable is well defined. Specifically, this is at the time when the Payer’s Provider approves the payment and creates an IOU. At this time, this specific payment cannot be reversed, and it is made clear to the Payer. (Through chargeback, end users can retrieve their money, but through a new transaction, the old one cannot be reversed).

S.3.3: The mechanism in the Token system for compensating a Payer in case of a payment dispute is for the Payee to initiate a new payment (direct payment, or pre-authorized payment) to
the Payer (the Payer/Payee roles switch), referencing the dispute, or original payment transaction. Token requires that Providers comply with relevant consumer protection laws. If deemed required during the development of the governance framework, additional rules will be defined to comply with appropriate consumer protection rules and regulations.

**Justification for S.4:**

S.4.1: The decision and rule-making processes have not yet been defined. Token and NACHA will collaborate on providing effective, transparent governance.

S.4.2: The decision and rule-making processes have not yet been defined. Token and NACHA will collaborate on providing effective, transparent governance.

S.4.3: The Token system provides a mechanism for inter-Provider Settlement using the services of a trusted central authority such as the Central Bank for a given currency. In that case, inter-provider Settlements would be conducted in central bank money.

**Justification for S.5:**

S.5.1: Both the Payer and Payee’s Providers must review a transaction before it is finalized. Token provides the tools and framework necessary to decide whether transactions are fraudulent, erroneous, etc. Providers using the Token software are responsible for deciding which transactions to accept disputes for.

S.5.2: Providers are responsible for complying with all regulations (including consumer protection laws), when using Token’s software. Although fraud and unauthorized payments will be low due to the security of the Token system, Providers are be able to provide refunds to end users for unauthorized transactions.

S.5.3: An API call is provided by Token to request money or a refund from a Payee. Although transactions are irrevocable, the Payee can choose to voluntarily return the funds, (by sending a new transaction). In cases where the Payee is legally required to return the funds, the Payee’s Provider can create the transaction from the Payee’s account.

S.5.4: As stated in self-assessment section G - Governance, these policies have not yet been fully developed. Token and NACHA will collaborate on providing effective, transparent governance in time for the product release.

S.5.5: As stated in self-assessment section G - Governance, these policies have not yet been fully developed. Token and NACHA will collaborate on providing effective, transparent governance in time for the product release.

**Justification for S.6:**
Token does not provide any fraud information sharing features. Providers can use and retrieve data from the Token software, and use their own fraud information sharing systems. However, as described in Token Security, fraud will not be a huge concern due to the signature authentication system.

**Justification for S.7:**

S.7.1: All Token APIs are open, and secured by the latest digital signature algorithms and open web standards. Encryption, privacy, and security are some of the most important concerns of the Token system. See Token Security section for more details.

S.7.2: Token provides all the operational components and processes required to secure a global payments system. This includes infrastructure for testing, denial of service protection, emergency response and recovery, encryption between hosts, data privacy, monitoring systems for all services, backups, high availability, internal and external firewalls, etc. Although each Provider will have different security architectures, Token will work with each one to ensure the TPS is correctly and securely integrated into each architecture, and will require that Providers maintain secure systems. See Token Security section for more details.

S.7.3: Token has policies for evaluating risk and ensuring that the systems are compatible and adaptable to enterprise architectures and systems. Token uses the latest enterprise security practices, and will work with Providers to comply will all risk related requirements.

**Justification for S.8:**

S.8.1: Token will strive for extremely high availability in production. The system Components have been designed for high availability and scalability, including the use of horizontal scaling techniques. The Token system is a large-scale distributed system, with instances of components installed and operated at individual Provider institutions. The exact availability metrics and plans for meeting them will need to be determined and met in conjunction with the Providers.

S.8.2: Business continuity planning will be done in conjunction with Providers that deploy the Token Components.

S.8.3: The Token system is deployed in a highly-distributed fashion with individual instances of the TPS running at various Providers. It is very unlikely that any single issue can cause a systematic failure. The central Components of the system, such as the Token Hub, have been designed to run in a high-availability, redundant environment, minimizing risk to the system.

S.8.4: Token will work with Provider partners, operational partners and regulators to determine the level of resources required to operate the system reliably.
S.8.5: Contingency planning will have to be carried out in partnership with the Providers and other parties.

**Justification for S.9:**

S.9.1: Everything in the Token system is encrypted with the latest technologies both in requests and at rest. Sensitive payment information is never transmitted over the Internet, only public keys and signed certificates are. Furthermore, Token's SDKs provide robust security mechanisms and procedures necessary to ensure that end user data is not revealed to unauthorized parties.

S.9.2: All private keys are stored locally, and there is no central repository of private keys. No sensitive payment information such as account numbers, card numbers or private keys needs to be revealed in order to make transactions, only public signatures. Other parties in a transaction will not be able to see any of sensitive information.

S.9.3: Since Token does not rely on transmitting any sensitive information for sending or receiving payments, there is no risk. Token member IDs and account IDs reveal nothing about the underlying Provider accounts.

**Justification for S.10:**

S.10.1: Authentication of end users, Providers, and other parties in the Token network is all done securely using digital signatures and certificates. With this model, a recipient of a message can always be sure that the sender of the message is who they claim. See Token Security for details.

S.10.2: TPS at the Providers and the Token Hub explicitly requires that transactions are only processed if the Provider owning the Payee’s account approves and signs them. Certificates are attached with each API call providing cryptographic proof of the Payee’s name/domain, and that they own their account. Also, calls can be made to the authority server by any entity in the system to verify the identity of another member.

S.10.3: The solution is compatible with U.S. regulatory guidance, as well as European regulations (including the new Payment Services Directive 2) with regards to user authentication. Furthermore, Token is compatible with best practices and standards for user authentication in the payments industry.

S.10.4: Token has a very flexible and secure user authentication scheme, where multiple key signatures can be requested by the components in the system. Every transaction must be signed, and Providers can require as much security as necessary by increasing the number and types of signatures needed for API calls. For instance, high-value payments may require multiple signatures and multi-factor authentication (MFA) whereas a low-value payment can be completed with a single signature. More detail in the Token Security section.
S.10.5: End user enrollment is performed in a secure context where the end user is already authenticated to their Provider. For example, a user can enable Token while logged in to their bank’s website, or their bank’s mobile app. At that time, the end user obtains an identity with the Solution (at their Provider’s TPS), in a secure manner. Providers may require high authentication levels such as their own MFA before creating a Token identity for their users. Providers can re-authenticate end users based on their own custom limits per token, per account, or per user, and tokens themselves can contain rules for authentication levels required to be redeemed.

S.10.6: Token uses Ed25519 signatures, but this security scheme is arbitrary and can be changed in future implementations of the Token Components, and a new security scheme can be specified in the authorization header (which is provided on every API call). Providers can tweak their authentication settings based on their own risk/user experience tradeoff, by changing limits or requiring more or less MFA/signatures.

**Justification for S.11:**

S.11.1: Providers are required to comply with all AML, KYC and other federal and state regulations in order to use the TPS. Such mechanisms are not included in the TPS itself, but rather Providers must use their existing compliance solutions. Data handled by the TPS will be encrypted and securely transmitted and stored. Providers will also be required to demonstrate an ability to store system level keys and other sensitive data in compliance with industry level security standards.

S.11.2: One of the main design principles of the Token system is that it would allow Providers to easily integrate TPS with other systems such as financial, legal, and technical solutions. During onboarding, Providers must demonstrate compliance with the then current federal and state rules and regulations; and show that they are capable of fulfilling all required obligations to participate in the Token network.

S.11.3: Token (And the Token Hub) monitors balances and payments between Providers to ensure that all Providers are compliant with the transaction time and settlement requirements. Providers that aren’t compliant with the requirements will be restricted or removed.

### 4. Speed (Fast)

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>Consideration Name</td>
<td>VE</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>Fast approval</td>
<td></td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.2</td>
<td>Fast clearing</td>
</tr>
<tr>
<td>-------------</td>
<td>-----</td>
<td>---------------</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.3</td>
<td>Fast availability of good funds to Payee</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.4</td>
<td>Fast settlement among depository institutions and regulated non-Provider account providers</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.5</td>
<td>Prompt visibility of payment status</td>
</tr>
</tbody>
</table>

**Justification for F.1:**

Token is a real-time payment system. Token processes its requests at millisecond speed. Latency is largely defined by external dependencies such as Internet packet routing latency and in the case of providing Good Funds assurance, latency depends on how long it takes the Payer Provider to return a Good Funds response.

**Justification for F.2:**

Clearing occurs immediately after approval by the Payer’s Provider. Payer’s Provider notifies Payee’s Provider, who then credits the Payee’s account.

**Justification for F.3:**

Token at the Payee’s Provider processes the request from the Payer’s Provider instantly. Availability of funds to Payee depends largely on the speed at which the Payee’s Provider is able to make the funds available to the Payee.

**Justification for F.4:**

Settlement using the Token Solution is fast, secure, and handles edge cases such as different Provider time-outs and transaction lags.

F.4.1: Might need more stuff The Solution manages credit and liquidity risk exposures arising from any lag between transaction Finality by creating a system where Providers have a credit limit with each other. This means that, as long as within the credit limit, the Provider for the
Payee will credit the money to the Payee’s account instantaneously, which will be settled later. Otherwise, the settlement happens using the Token Currency Ledger, between the Depository Institutions associated with each Provider. The settlement process takes a fraction of a second.

F.4.2: The real-time payment system is independent of time zones and will be recorded in the local time of each Depository Institution or Regulated Non-bank Account Provider.

F.4.3: Providers decide how often they want to perform settlement. By defining a credit limit, a Provider indicates credit risk vis a vis another Provider. A credit limit of 0 (zero) indicates that a Provider accepts no credit risk and that the opposing Provider must provide the funds instantly. The credit risk is expressed on a Provider pair basis (Provider A may accept a $X credit risk related to Provider B, but a $Y credit risk related to Provider C). Consequently, the settlement is usually done instantaneously, but the Providers have the flexibility to determine an alternative timing of settlement dependent of the credit limit they give each other.

**Justification for F.5:**

F.5.1, F.5.2: At every completed step of the payment lifecycle, Token generates a status message. Token immediately distributes status messages as desired by the parties relevant to the particular transaction and the specific lifecycle step. The respective Providers are able to notify the user using their chosen means of contact (e.g. text, push notification, email, etc).

### 5. Legal Framework

NOTE: Effectiveness Criteria with unchecked self-assessment means that this part of the solution has not yet been developed.

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria Name</strong></td>
<td><strong>Consideration Name</strong></td>
<td><strong>VE</strong></td>
</tr>
<tr>
<td>Legal Framework L.1</td>
<td>Legal framework</td>
<td>X</td>
</tr>
<tr>
<td>Legal Framework L.2</td>
<td>Payment system rules</td>
<td>X</td>
</tr>
<tr>
<td>Legal Framework L.3</td>
<td>Consumer protections</td>
<td></td>
</tr>
<tr>
<td>Legal Framework L.4</td>
<td>Data privacy</td>
<td></td>
</tr>
</tbody>
</table>
Legal Framework

Justification for L.1:
Token runs at the Provider, accessing end user accounts held at the Provider. In doing so, Token relies on the regulatory compliance in place by the Provider including OFAC, AML/BSA and UIGEA. No additional compliance rules are required for running Token.

L.1.1: Since Token relies on regulatory compliance upheld by the Providers, there are currently no known rulings, court decisions, etc. that need to be further identified. If and when gaps are identified, they will be addressed promptly.

L.1.2: There are currently no known legal gaps. If and when gaps are identified, they will be addressed promptly.

L.1.3: All Entities in the Token system are existing customers of one or more Providers. Such Entities are already subject to regulatory KYC, OFAC, AML/BSA, etc. Therefore, payments in the Token system are legally bound within the legal framework.

L.1.4: All Entities in the Token system are existing customers of one or more Providers. Such Entities are already subject to regulatory KYC, OFAC, AML/BSA, etc. Therefore, payments in the Token system are legally bound within the legal framework.

L.1.5: Currently, no known unique legal provisions are required.

Justification for L.2:
L.2.x: This part of the Legal Framework has not yet been developed.

Justification for L.3:
L.3.x: This part of the Legal Framework has not yet been developed.

Justification for L.4:
L.4.x: This part of the Legal Framework has not yet been developed.

Justification for L.5:
Each participating Provider agrees to the Token license agreement (TLA), which indemnifies the Provider from third-party rights related to patents, trademarks, copyrights, and trade secrets.
6. Governance

NOTE: Effectiveness Criteria with unchecked self-assessment means that this part of the solution has not yet been developed.

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>#</td>
<td>Consideration Name</td>
</tr>
<tr>
<td>Governance G.1</td>
<td></td>
<td>Effective governance</td>
</tr>
<tr>
<td>Governance G.2</td>
<td></td>
<td>Inclusive governance</td>
</tr>
</tbody>
</table>

**Justification for G.1:**
The decision and rule-making processes have not yet been defined. Token and NACHA will collaborate on providing effective, transparent governance.

G.1.1: Token’s governance arrangements will ensure efficient decision making and rule making, including the establishing of clear lines of responsibility for all decision makers or decision-making bodies.

G.1.2: Token’s governance arrangements will be publicly disclosed.

G.1.3: Token’s governance arrangements will provide a process to handle appeals related to specific decisions or implementation thereof.

G.1.4: Token’s governance arrangements will be independently validated for compliance with its rules, compliance with applicable law, and achievement of the Token system’s objectives and public policy objectives.

**Justification for G.2:**
G.2.1: The establishment of, and revisions of Token’s governance arrangements will include consideration of the public interest.

G.2.2: Token is collaborating with NACHA to ensure that all stakeholders can provide input and feedback to the governance arrangements.

G.2.3: Token is collaborating with NACHA and other interest groups.
G.2.4: Token will ensure that specific stakeholders or stakeholder groups are proportionately represented.

G.2.5: Token will ensure that actual, perceived, or potential conflicts of interest are addressed and managed appropriately.
Faster Payments QIAT

PRELIMINARY ASSESSMENT

Proposer: Token, Inc.

APPENDIX A: QUESTIONS BACK TO PROPOSER

Ubiquity

U.1.2: How does Token interact with non-real-time payment systems before ubiquity is reached?

TOKEN: Smart tokens include transfer instructions that specifies the payment rail to be used. For example, transfer instructions to a Provider that is not using Token but can be reached through ACH would look something like:

```
transfer: {
  method: ACH,
  from: Token Account,
  to: ["routing number": 1234, "account number": 8768767]
}
```

The sending Provider uses the transfer instructions to initiate the payment through the alternative rail.

U.1.3: How does the Token FX Service operate in terms of funding? What is its revenue model and its exchange transaction model?

TOKEN: The operator will charge a small fee per transaction proportional to the amount of the transaction in much the same way that bitcoin exchanges like Coinbase charge. This is a proven model.

U.1.4: Will non-FIs /non-regulated entities be allowed to join the Solution as providers? How does the Solution plan to bring non-banking providers on board as participants in Token?

TOKEN: Yes, the whole idea behind token is that it is an open protocol for value exchange. Anyone can join as a value provider, just like anyone can put a web server up on the Internet. It’s up to the clients whether they want to use those services. Token plans to provide online documentation demonstrating the ease of joining the Token network. Token will reach out to major value providers to have them join the network.

U.1.5: What are some specific examples of provider adoption and integration? Please clarify the value proposition to providers to motivate adoption.

TOKEN: A specific example of adoption and integration is Fidor Bank in Germany. By integrating Token’s system with Fidor’s basic bank API calls, Token was able to get the system running in one day even though we had to develop a wrapper around the available OAuth2-based. Had Fidor provided the 9 API calls required by Token, the integration would have taken even less time.
European banks are required to comply with a regulation called PSD2, which requires all banks to have an open API accessible by Third Party Providers (TPP) by January 2018. This regulatory pressure, combined with advantages outlined in the paragraph below, jumpstarts Provider adoption (first in Europe, then in the rest of the world).

From a revenue perspective, the Provider can charge for each API call. From an ecosystem perspective, having a simple, secure, open, flexible, and powerful payments API allows more applications to be created, which results in an increase in transactions (and thus revenue for the Provider).

From a speed perspective, transactions are now essentially instant (microseconds), instead of taking days to be completed (which has positive revenue and user experience impacts for the Provider).

From a cost perspective, Token’s proposal reduces overhead, fraud, and fees costs for the Provider.

From a brand perspective, the Provider’s brand is now in the forefront of every transaction.

From a security perspective, the Provider can now use digital signatures, Ed25519, and smart tokens -- which have a much lower risk profile than legacy security standards (such as OAuth2).

From an opportunity perspective, the smart tokens allow for complex rules and constraints surrounding a given asset, and this flexibility opens up the creation of entirely new business models.

U.2.3: What will be the minimum requirements, if any, to providers for the user interface and experience?

TOKEN: On the user interface (UI) and user experience (UX) sides, the minimum requirement is that a Provider has a signup form on their website that allows the user to create a Token member by choosing an alias (i.e. username), and storing the private key on a device. To limit the amount of effort on the Provider’s side, Token recommends adding an “Enable Token” button that calls a Token-hosted iFrame, which then handles the member creation.

U.3.2: How will Token enforce providers’ compliance with the communication of baseline features to end users? Please share the participation requirements (as stated in the Rulebook or elsewhere) that address this criterion

TOKEN: Token plans to qualify merchants into one, maybe two categories. The identification of the merchant category and a hyperlink to the terms and conditions for the merchants in that category will be available to the user on the checkout popup screen to avoid ambiguity.

U.3.3: What are the standard communication and messaging protocols used between the Solution and Providers?

TOKEN: REST protocols, but the specific API calls are unique to Token.

U.3.5: What will be the error resolution protections, right, and liabilities between payer and payee?
TOKEN: That will be specific to the merchant category, and the rules for each category will be defined in the rulebook. It will likely be similar to Visa’s protection or the Faster Payment protection depending on merchant class. See U.3.2.

U.4.1: What message format does Token use? If two parties need to always negotiate on what message format to use, how is this scalable?

TOKEN: There is a specific RESTful API that all parties use to communicate. There is no negotiation. The payment API calls use ISO 20022 to specify the parameters of the payment.

U.4.2: Please describe how contextual data in a direct payment and a smart token (a pre-authorized payment) would be integrated with interfacing business and personal finance systems

TOKEN: Smart tokens lock down the payment terms between the payer and bank. The contextual data will be in ISO 20022.

U.4.3: How will Token standardize and customize contextual data to ensure adoption by use case (taking into account the varying contextual data needs by use case – e.g., B2B, POS?)

TOKEN: By adopting ISO 20022 and extending it if required. One of Token’s first customers is a large ERP company in the UK and we’ll be working out any exceptions with their input.

U.5.1: How will Token handle any special cross-border considerations (e.g., different regulations, message formats)?

TOKEN: The software is licensed to banks to run in their countries. To account for differences in different counties, we modularize these sections so that the bank can deploy with the appropriate in-country plug-in modules.

U.5.2: How will the Solution ensure interoperability with FPS in the UK or SEPA in Singapore?

TOKEN: Singapore uses FAST. Both FAST and FPS (in the UK) are supplied by VocaLink and the systems do not interoperate. In such cases, a solution is to use Token Instant between banks. Token Instant uses a global ledger run by a large global entity (which may not yet be named) that allows for instant cross border payments.

U.5.3: How will Token work with providers to ensure upfront transparency to end users on cross-border payment fees, exchange rates, and other costs?

TOKEN: First, Token will work with the Providers to ensure fee structures are known to users prior to placing an order. Further, fees and exchange rates will be presented to the end user prior to the transaction being completed. End users will be able to accept, or decline any such charges prior to executing the cross-border payment.

U.5.5: What is the implementation plan for achieving cross-border payments, including the timeline for implementation and how this addresses the other sub-criteria?

TOKEN: Multi-currency, and cross-border payments will be available with the initial release. The cross-border functionality takes advantage of the Provider-to-Provider communication enabled by
the Token network and will work much like normal transactions -- with the exception of multi-currency transactions, where an FX service is also involved. See more details about this on the “Multi-currency & cross-border” section of our submission.

**Efficiency**

E.1.2: How would the step by step process work for an end user to switch Providers and still use Token as well as use multiple Providers through Token?

**TOKEN:** To switch Providers, the end user should disable her Token account with the old Provider (in mobile app or in the browser), and enable Token at the new Provider’s website, using her Token alias (i.e. username). To use multiple Providers with Token, the user simply enables Token at each Provider by entering her Token alias (i.e. username). To enable Token at a Provider’s website, the ideal user experience is: click “enable Token” button inside Provider’s website → enter alias (e.g. “jsmith”) → confirm pairing on mobile app through push notification.

E.2.1. Does the Digital IOU have contextual data fields (examples are largely related to text messages between two parties but do push payments and smart tokens enable more structured data such as invoice numbers? How is the contextual information structured? What flexibility is allowed and how does it maps to ISO20022? How does it travel ‘with’ the payment?

**TOKEN:** The Digital IOU does have a Description field (see Detailed Example of Payment Execution), as well as an Amount, From Provider, To Provider, and To Account fields. However, most contextual data field and structured data will be found in the rules of the smart token being redeemed. A smart token has key-value pairs that are flexible -- as long as the TPS or another entity the Provider trusts is able to interpret them. ISO 20022 is compatible with the Token system as it is yet another field of a smart token. The only part that “travels” is the smart token ID (tokenID). Each tokenID has a unique identifier. Authorized parties may lookup the rules associated with a smart token.

E.3.1: Please provide more detail regarding plans for funding and partnerships, as well as growth projections.

**TOKEN:** Token is currently in the process of raising a $12M Series A. 3 VCs are currently doing due diligence on the deal, and 8 other VC firms have expressed interest as co-investors. Four large EU banks want to participate in the round. Token expects to grow to slightly over 50 employees by the end of 2017. Token is striking partnerships with major IT players in the EU marketplace: IBM, CGI, Capgemini, VirtusaPolaris, Accenture, SIA, Almaviva and more.

E.3.1: How will the Solution develop a settlement system through the Token Currency Ledger and what is the timeline?

**TOKEN:** Token expects to have the TCL live in 2017 for testing and operational in 2018. The technology is straightforward. One of the world’s largest banks is interested in operating the TLC. The TLC could also be operated by organizations such as SWIFT and/or TCH.

E.4.1: What message format will be used and when for push and pre-authorized payments?

**TOKEN:** The message format is proprietary and JSON-like. The ISO 20022 (or any other message format) is supported by embedding as a term in the smart token.
E.4.3: How will Token ensure interoperability between standard formats and the proprietary format in its API?

TOKEN: Standard formats (such as ISO 20022) can be encapsulated within the terms of a token, thus ensuring interoperability.

E.4.3: How cost-effective is Token’s proprietary data format to adopt compared to existing standard formats?

TOKEN: Very cost-effective. Token components encapsulates any complexity, including having open standard fields (e.g., ISO-20022) within the token body. Consequently, this means minimum (if not zero) extra work for adoption.

E.4.5: What plan is there to have the message formats developed and/or published by a recognized standards development organization?

TOKEN: Token’s message formats are built to be flexible and compatible with other standards. The data format is transparent and well documented. There are no immediate plans to get it published and recognized by a standards development organization. This may change, but with the caveat that token terms should remain flexible and easily updateable, so increasingly more payment rules can be added to it.

E.6.2: What projected volumes and values, including heightened transaction volumes and values during peak times or periods of stress, can Token handle? What capacity does Token have to handle the projected volume? Does any of this capacity need to come from external providers? Any sources/partners identified?

TOKEN: A Token server can confidently handle at least 10,000 transactions per second (TPS). Projected volume is of several trillions of dollars and hundreds of millions of transactions daily once the system is in place worldwide. Achieving such performance comes from a combination of building scalable software and partnering with cloud service providers (such as IBM, a current partner) to host and run the software, as well as having the Token system hosted and run by Providers.

E.7.1 and E.7.2: What tools are provided for exceptions and investigations?

TOKEN: Token’s philosophy is to provide Providers with programmatic access to all relevant data for further processing in external systems. This reduces operational cost and increases efficiencies for the Provider. Providers will have access to APIs to extract all relevant information from the Token system for processing in external systems. Such systems may be a Provider’s existing case management system, or will be created by Token if desired by the Provider.

E.7.1: What information will the Solution actually see in a transaction (e.g., a smart token) that will enable it to address exceptions or create tools to do so?

TOKEN: A smart token goes through a lifecycle (issue->endorse->redeem->Expire/Revoke/End. Each step can be queried. Some examples:
Issued smart token:
{
"scheme": "pay/1.0",
"issuer": "HSBC",
"payer": "d1922087f7/Alexey Kalinichenko",
"redeemer": "9ec142ad8492/Steve Kirsch",
"created_at": "2016-07-04T16:54:58Z",
"description": "Some description",
"transfer": {
"method": "FPS",
"from_account": "hsbc:54645454545/checking",
"to_account": "db:23423434/savings"
},
"currency": "EUR",
"amount": 10000
}

Endorsed smart token:
{
"id": "470c2ca159de43342afe",
"payment": { },
"endorsements": [ {
"signature": "c587d222470c2ca159de4..."
"member": "d1922087f7",
"timestamp": "2016-07-05T16:54:58Z",
}, {
"signature": "930e21ffe30282151db9d..."
"member": "wf",
"timestamp": "2016-07-05T16:54:58Z",
}, ]
}

E.7.3: What will the Solution provide around aggregating exceptions data to spot patterns at the network level?

TOKEN: This hasn’t been specified yet. Token will hire data scientists to analyze transaction data.

Safety and Security

S.1.1: Please provide more detail on the Token-NACHA collaboration including the scope and timing. What is NACHA’s commitment to developing the rules? What is the intended approach for the definition of the risk management framework?

TOKEN: The CEO of NACHA has offered to partner with Token to devise the rules for the US marketplace. Scope and timing is not available at this time.

S.1.2: How will the Solution manage the large number of multilateral limits set by participating providers? What is the mechanism for governing settlement limits between banks? How does Token plan to scale this?
TOKEN: Token provides the ledger software to the operator (large global bank) that operates the network. The software enables the operator to set the credit limits for each participant. The limits are not set multilaterally; it is a hub-spoke model for risk so it’s all between each participant bank and the operator.

S.1.3 and S.1.4: How will Token address the remaining operational and fraudulent or erroneous payment risks?

TOKEN: The banks operate the Token system. Token expects the banks to use their existing frameworks for this area. It’s impractical for a solution provider to provide this worldwide.

S.3.3: What recourse will a Payer have if the Payee refuses to initiate a new payment when there is a dispute?

TOKEN: The process for recourse will be defined in the upcoming Rulebook. At a high level, the Payer would instruct its Provider to request the payment according to the dispute from the Payee’s Provider. The Payee’s Provider would validate the reason for the dispute and the terms (according to the Rulebook) and return the funds to the Payer’s bank.

S.4: Please explain step by step how the settlement process works and what new systems need to be developed versus what existing infrastructure is used.

TOKEN: It’s a shared ledger run by an operator (large global bank). It’s conceptually like every bank opens an account at the Operator and money is moved between the accounts on the ledger. At any time, any bank can move money from the central bank rail to/from their account at the Operator. This is done via a public crypto secure operated by the Operator. Token may use IBM’s Hyperledger for this service (IBM is a partner). A bank makes a signed request to the ledger to move funds. The shared ledger returns a signed receipt of the transfer. The sending bank hands the receipt to the receiving bank. The receiving bank has two ways to verify that “money is in the bank”: 1) check the signature of the Operator on the transaction; or 2) goes directly to the ledger and requests the transaction. At that point the Token software at the receiving bank tells the core banking system to debit an FBO account and credit the receiving customer’s account. The opposite happens at the sending bank (debit the sending customer’s account, credit the FBO account in the core banking system).

S.4.1: Are the Token Currency Ledger (TCL) and the system where providers set credit limits for each other the same settlement system?

TOKEN: Yes, see answer in S.1.2.

S.4.1: Because the settlement service will be new for the Federal Reserve, please describe the specific responsibilities for the Federal Reserve.

TOKEN: Involvement by the Fed is optional. Token wants the Fed to have a crypto secure Fedwire operating 24x7. Token can supply the software for this or the Fed could. This enables banks to adjust their position with the Token Global Ledger on a straight through processing basis 24x7. On request by the Bank of England (BoE), Token has proposed BoE a pilot project for this. The Fed could run the same system.
S.4.2: What steps does the Solution take to proactively manage inter-provider credit and liquidity risk exposures aside from the credit limits each provider sets?

TOKEN: See S.1.2 answer.

S.4.2: How will the Solution manage the large number of multilateral limits set by participating providers? What is the mechanism for governing settlement limits between banks? How does Token plan to scale this?

TOKEN: See S.1.2 answer.

S.5.1: What tools does Token provide to decide whether transactions are fraudulent or erroneous (as referenced on pg. 61)?

TOKEN: Token tracks suspicious fraudulent members of the system and provides a lookup function to identify such members and warn Payers and Providers. As with all Token services, this can be accessed through an API.

S.6.: Token provides supplemental information

TOKEN: S.6: Token wants to further clarify: As mentioned in the response to S.5.1, Token will track suspicious fraudulent members and provide a centralized lookup function to access this information. This can be accessible to Providers (API) and externally to the Token ecosystem if desired.

S.7.2, S.7.3: Please provide more detail on the elements within S.7.2 and S.7.3.

TOKEN: Token components operating in the cloud comply with all the standard security measures such as SOC1/2/3, FISMA, etc. Communication between all services is encrypted with TLS. Data retention and disposal policies comply (at a minimum) with those required by the Providers. These policies have not yet been finalized, but will be completed and reviewed by external experts prior to general availability of the Token solution. Incident reporting will follow standard enterprise incident reporting procedures with multiple levels of severity and associated committed response times.

Managerial policies and oversight need additional information on all four components, including how the system will integrate with existing processes, a description of how it is adaptable to enterprise-level security architectures, etc. (S.7.3).

Token is committed to integration with existing tools and processes through APIs.

S.8: Please provide any further support for addressing the Resiliency criteria.

TOKEN: All Token cloud components run in a cluster, distributed geographically. Should a service component fail it can instantly be taken offline and a new instance can be operational within seconds. At a Provider’s location, Token runs in a high-availability cluster with failover support.
S.9.1: How will Token ensure the securing of private keys for Providers, merchants and consumers?

TOKEN: For Providers, the private keys will be stored in a hardware security module (HSM). For merchants, they are able to secure their private keys as desired, whether using HSMs or storing it in a cloud service. For consumers, the private key will be secured inside their mobile app. No sensitive information is ever transmitted, and there is no central repository of private keys. On top of this, the system does continuous key rotation of all keys, in order to protect Token members from potential attacks.

S.10.1: How will Token ensure minimum enrollment authentication standards are met by Providers?

TOKEN: If a Provider does not use digital signature and certificates when confirming authorizations and transactions, the given authorization/transaction will fail, since the Token Hub will not be able to verify and accept them. Thus, Providers have big incentives to meet authentication expectations. Moreover, the Token Provider Software, which will be hosted and run by the Providers, has all the logic needed to ensure authentication standards are met, so there is minimum effort required from a Provider’s perspective.

S.10.2: How will the Solution enforce security requirements for the local storage of private keys?

TOKEN: Refer to answer to S.9.1, which details how Token will ensure the securing of private keys.

**Speed (Fast)**

F.1: How will Token ensure approval occurs within 2 seconds? How is this monitored and enforced? What are the consequences for exceeding this time?

TOKEN: When a transaction hits the Token system to be processed, it only touches the code to complete except at the very end where a message is sent to the core banking system to credit the account. The operations are simple and the databases used are very fast. It’s all about latency. Token reduces the number of systems and round trips to complete a transaction to keep the elapsed time to a minimum. Also, most banks will likely run Token in the cloud. This greatly minimizes latency.

F.3: How will Token ensure a maximum delay for Providers to make funds available to Payees?

TOKEN: It’s part of the software itself, so unless the Provider modifies the Token source code, it will happen. If Token hears reports of non-compliance, the license agreement may be revoked.

F.3: Will Token set a maximum time period within which the payee’s provider must make the funds available to the Payee (e.g., within one minute)? If so, how is this monitored and enforced? What are the consequences for exceeding this time?
TOKEN: Yes, Token requires the Provider to credit the account when the software makes the call to the core banking system. This will be monitored by creating test accounts at each licensee Provider so it can be monitored and enforced.

F.4: Please explain step by step how the settlement process works and what new systems need to be developed, versus what existing infrastructure is used.

TOKEN: See S.4 answer.

Legal

L.2: Please provide a plan or timeline for how and when the Payment System Rules will be developed.

TOKEN: The Payment System Rules will be developed together with industry partners and legal experts in the field. Token expects to have this completed by June/2017.

L.3: Please provide a plan or timeline for how and when the Legal Framework addressing consumer protection will be developed.

TOKEN: The Legal Framework addressing consumer protection will be developed together with industry partners and legal experts in the field. Token expects to have this completed by June/2017.

L.4: Please provide a plan or timeline for how and when the Legal Framework addressing data privacy will be developed.

TOKEN: The Legal Framework addressing data privacy will be developed together with industry partners and legal experts in the field. Token expects to have this completed by June/2017.

L.5.1: Please describe Token’s approach to a due diligence review of potentially applicable intellectual property rights, and other measures it will undertake to address any risks in this regard.

TOKEN: Prior to general availability (GA) of the Solution, Token will perform a GA legal review related to patents, trademarks, copyrights, and trade secrets to ensure Token is clear of any infringements in those areas. The results of this review will be shared with Providers using the Token Solution. While this truly is an ongoing process, Token is committed to provide Providers with updates should the status change.

Under certain circumstances, Token may allow Providers to access sources in order to conduct their own due diligence in those areas.

Governance

G.1, G.2: Please provide a plan or timeline for how and when governance will be developed.

TOKEN: Token anticipates a Scheme Management Board (“SMB”) responsible for performing the functions of management and evolution of the Token Scheme. Token will consult with industry and legal experts in the field to develop governance as part of the Rulebook. Token expects to have this completed by June/2017.
Faster Payments QIAT

DRAFT ASSESSMENT

Proposer: Token, Inc.

Summary Description of Solution:
Token is a set of software and service components that enable payers to make direct push and pre-authorized pull payments through digital tokens. Providers (depository institutions and non-regulated account providers), merchants and other entities install the Token Provider Software (TPS) which supports their participation in the Token system. A “token” is a reference or identifier that maps back to an individual’s sensitive data (e.g., account information, Personally Identifiable Information (PII)) but that protects that data by having no meaning other than as a reference. The Token system provides an advanced capability called smart tokenization which supports the creation of tokens that include terms ruling access to the underlying asset. For pre-authorized payments, payees use these “smart” tokens to access funds in the payer’s account under terms that the payer has previously set. The network uses digital signatures to authenticate payers and payees and authorize payments.

Payers and payees access Token through an Application Program Interface (API) where third-party developers create and provide applications. Participating providers have the TPS to send and receive payments through the Token System, and the Token Hub routes messages based on these tokens between providers. The Token Authority Service (TAS), which would be the Federal Reserve or another trusted third-party, manages the mapping between end user data and their tokens as well as the end users’ and providers’ digitally signed certificates. Finally, settlement is conducted through a shared ledger run by the operator (a large global bank). Providers move money into accounts at the operator to enable immediate settlement. The Token Foreign Exchange Service allows funds to be moved instantly across different currencies. Token supports quotes and rates possibly coming from multiple foreign exchange service providers.

Executive Summary of the Proposal

Major strengths
- Token uses innovative and leading-edge security and end user data protection by using digital signatures and certificates to authenticate and authorize every payment. Every entity in the system is associated with one or more public keys, and handles corresponding private keys. As long as private keys are kept secure, digital signatures assure every API call or request to a third party can be verified to have been initiated by the right entity, which reduces risk of errors, failures, fraud
- Smart tokens are an innovative way to provide Payer control and flexibility over pre-authorized pull payments. They allow programmable payments by defining terms that govern access to an assets or adding contextual information, are secured by advanced cryptography, and tied to a specific Payee
- Token runs on top of the existing account management systems at providers and does not replace core banking systems

Areas for improvement and enhancement
- The proposal indicates that a large global bank will be the operator of the solution. Participating banks will open an account at the operator and settlement will happen through those accounts. This creates the need for significant risk management of the single large global bank
The overall implementation plan does not currently address adoption by billers, merchants, and end users. In addition, the value proposition for providers to adopt and make the solution available to end users need further support.

The solution has not yet developed rules, governance, legal framework, and in particular, how to handle disputes, error resolution, and consumer protection.

**Use cases addressed**


**Proposer’s overall ability to deliver proposed solution**

- The solution is based on innovative technologies and approaches, which are still in early stages of developments with expected completion of development by the end of 2016.

- The proposal does not describe any live pilots in market and no track record is provided for similar developments or implementations in the past.
**Ubiquity**

**U.1 Accessibility**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution facilitates payments to and from all types of payment accounts (as determined by the individual provider) at both Depository Institutions and Non-Regulated Account Providers (U.1.1). Token also supports multi-currency through the Token Foreign Exchange Services, which has providers with accounts in multiple countries (U.1.3). Token demonstrates that the solution is technically feasible for providers to adopt, and indicates that the motivation for providers to adopt Token is regulatory pressure (PSD2 in Europe), improved security, reduced cost, and the opportunity for new business models (U.1.5).

However, the solution needs to describe how payers can ensure that their payments can reach all Payees, even those with providers that are not part of the Token network (U.1.2). For example, more detail would be helpful regarding how it will authenticate and enroll first-time end-users who use a provider not yet on the Token network.

**U.2 Usability**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Token supports usability but is dependent on providers for the end user experience. Token is available through any channel including mobile, online, offline, but ultimately depends on the providers using the Token SDK to build applications across channels (U.2.1)

Token enables initiation of payment with limited information. The Payer needs to know the Token Account Number (TAN) of the Payee, but application developers can create a service that maps a user’s TAN with an alias such as email and phone (U.2.2)

The solution itself is available 24/7/365 but is dependent on providers to make it accessible to end users 24/7/365 (U.2.3). In addition, providers are responsible for accommodating varying levels of end-user technology proficiency and usability needs. The proposal does not indicate baseline operating rules or guidelines to ensure a minimum user experience, though reference is made to a Rulebook (U.2.4).

**U.3 Predictability**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Token’s design ensures reliable delivery of its baseline core features within its network and across channels, particularly regarding the digital signatures and the payment process (U.3.1, U.3.2). The solution uses REST protocols as its standard communication and messaging protocols with providers (U.3.3). The solution is described as “smart token” to distinguish it from other payment methods (U.3.6).
However, the proposal does not address the error resolution protections, rights, and liabilities of the payer and payee (U.3.5). The solution relies on providers to communicate the baseline features of the payment experience to the End Users (U.3.2, U.3.4) without operating rules or guidelines to ensure this happens.

**U.4 Contextual data capability**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale**

The solution indicates that contextual data will be in ISO20022 or structured in any form agreeable to two parties (U.4.1). For instance, the smart token for pre-authorized payments is complex and includes contextual data that is attached to the payment.

Although the capability for contextual data exists, more details are needed about how the solution will enable easy integration with business and personal finance systems (U.4.2). More details are also needed on how Token’s approach will balance the need for flexibility with the need for standards. Token is in process of working with a large ERP company that will help inform further contextual data needs (U.4.3).

**U.5 Cross-border functionality**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The proposal does not currently have cross-border functionality, but it is planned for the initial implementation. Given that current faster payment schemes do not yet interoperate, the solution allows for Interoperability with similar Payment Systems in other countries through “Token Instant” where banks across countries will share a global ledger if on the Token Network (U.5.2). The solution does require providers to make advance disclosure of fees, exchange rates, costs (U.5.3), and the solution allows conversion of currency through an FX service provider (U.5.4).

More information would be helpful on how different regulations, settlement would be handled (U.5.1). In addition, more detail would be helpful on the implementation timeline including adoption plan for providers in other countries to join the global ledger (U.5.5).

**U.6 Applicability to multiple use cases**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

**Efficiency**

**E.1 Enables competition**

![Very Effective] Effective Somewhat Effective Not Effective

**Rationale:**
Token’s API-based system and the Software Development Kit (SDK) encourages providers and application developers to create value-added services, and promotes competition (E.1.1, E.1.4).

The solution also allows entities to choose a provider, switch providers, or use multiple providers. The end user can disable a Token account with one provider and enable the same Token account at the new provider’s website. Multiple providers can be used by enabling Token at each Provider using the end user’s Token alias (E.1.2). More detail would be helpful on how end users can choose which payment account to use if an alias is associated with multiple providers. The solution relies on third parties to develop the mapping between personal and account IDs which is needed for portability and easy switching of providers.

**E.2 Capability to enable value-added services**

![Very Effective] Effective Somewhat Effective Not Effective

**Rationale:**
Token allows all Providers and third parties to integrate, build applications, and create value-added services with the API and Token’s Software Development Kit (E.2.1). Contextual data resides in the smart tokens. The Token system is compatible with ISO20022 as fields in the smart token.

Providers are responsible for setting fees for value-added services and disclosing that these fees are optional to end users. However, it is unclear what requirements the solution sets (if any) for providers around disclosure (E.2.3)

**E.3 Implementation timeline**

![Very Effective] Effective Somewhat Effective Not Effective

**Rationale:**
The Token solution is still under development and expects to be completed by end of 2016. The implementation timeline starts with reaching market ubiquity through the 10 largest providers over a 24-month period using strategic partnerships with the long tail being reached in three years. The key dependency cited is hiring and retaining key talent and Token indicates it will raise capital in the second half of 2016. The solution will be funded through venture capital money: the proposal states that Token is in process of raising a $12M Series A, with interest from 11 VCs and 4 EU banks.

The implementation plan would benefit from more detail on how it will achieve ubiquity with not just providers but the businesses, billers and merchants where Token plans to use smart tokens, the implementation and ubiquity hurdles beyond talent and plans to overcome those hurdles.
E.4 Payment format standards

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token accepts format standards such as ISO 20022 but focuses on the new proprietary data formats in its flexible API (E.4.1, E.4.2). These proprietary formats are flexible and able to accommodate complex rules within smart tokens (E.4.4).

However, the solution has not committed to having the proprietary formats developed and/or published by a recognized standards development organization (E.4.5). In addition, more clarity is needed on how ISO20022 can be embedded in the smart token while still ensuring the integrity of any translation required between the proprietary format and ISO20022 (E.4.1, E.4.3).

E.5 Comprehensive

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token provides the technical design and support for all aspects of the end-to-end of the payment process in combination with providers (E.5.1, E.5.2).

E.6 Scalability and adaptability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token’s technical design is readily adaptable (i.e., the flexible API) and supports the solution’s projected use cases (E.6.1, E.6.3). The server can handle at least 10,000 transactions per second based on scalable software and partnership with cloud service providers (E.6.2).

E.7 Exceptions and investigations process

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token gives providers the details of all transactions, including any exceptions (E.7.1). It also ensures that transaction data is created, recorded, and then retained appropriately for post-transaction evaluation (E.7.2).

However, it does not provide any tools, messages, alerts, notifications and related protocols for supporting the ability to address exceptions in a reasonable timeframe (E.7.1). It also does not provide any case management tools for post-transaction evaluation (E.7.2), nor does the solution commit to exceptions data aggregation to spot patterns above the level of an individual provider (E.7.3).
Safety and Security

S.1 Risk management

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
Token has not yet developed a risk management and legal framework, although it notes a collaboration with NACHA to develop policies and governance in time for the product release (S.1.1, S.1.5).

The operator of the Token network is a large global bank that will use the Token ledger software. Each participant bank sets credit limits for settlement with the operator (S.1.2). More detail on risk management at the operator level would be helpful.

The proposal also indicates that there is a low likelihood of operational risk and unauthorized, fraudulent, or erroneous payments given the automation of the system and the security of user authentication. However, the solution does not indicate how it will address the remaining risks such as incorrect storage, loss, or theft of private keys, or account takeover, other than to state that those are the providers’ responsibility (S.1.3, S.1.4).

S.2 Payer authorization

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The solution requires that the payer authorizes to their provider with each payment, and the system uses the keys of both the Payer and the Payee’s provider (S.2.1). On pre-authorized payments with “smart tokens,” the payer can specify a number of parameters, which they can revoke or change at any time (S.2.2, S.2.3).

S.3 Payment finality

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
Token requires the Payer’s provider to approve each payment following initiation to ensure Good Funds (S.3.1). The payment becomes irrevocable when the Payer’s provider approves the payment and creates an IOU to the Payee’s provider (S.3.2). In the event of a disputed payment, a payee can compensate a payer by initiating a new payment that returns the money to the Payer through a second transaction.

However, the solution does not yet include “mechanisms and processes to protect or compensate the payer in the event that the payment is disputed – this is to be defined in the upcoming Rulebook (S.3.3).”

S.4 Settlement approach

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>
Rationale:
The solution settles in commercial bank money – a large global bank is the operator that runs a shared ledger. Participating banks move money from existing Fed-operated clearing and settlement systems to an account at the Operator. The Operator then settles between accounts at the Operator. The proposal envisions optional participation by the Fed – Token would want the Fed to operate 24/7 and provide a direct connection with the Token Global Ledger to enable account settlement in real-time.

More details on the settlement approach would be helpful: in particular, the rules and timing of settlement (S.4.1) as well as most critically, the management of operator risk given that the settlement approach is dependent on a single global bank for a payment system of national scale (S.4.2).

S.5 Handling disputed payments

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th><strong>Somewhat Effective</strong></th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
Any party in the transaction can request prompt voluntary return of funds from the Payee in a disputed payment through an API call that Token provides (S.5.3). However, the solution’s rules for handling disputed payments do not include “requirements, processes, and timeframes” for handling disputed payments as well as mechanisms to hold rule violators accountable (S.5.1). Providers decide which transactions they will accept disputes for.

In addition, Token has not yet developed an approach including the “delineation of roles, responsibilities and liability allocation” which reasonably protects business, government and consumer payers against losses from fraud or errors (S.5.4, S.5.5), although it indicates a collaboration with NACHA to develop policies and governance in time for the product release.

S.6 Fraud information sharing -

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th><strong>Somewhat Effective</strong></th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
Token tracks suspicious fraudulent members of the system and provides a lookup function to identify such members and provide alerts to providers through an API (S.6.3).

However, Token does not require information sharing among providers to facilitate managing and monitoring fraud (S.6.1). Providers are expected to use and retrieve data from the Token software and use their own fraud information sharing systems (S.6.2, S.6.4-S.6.7). The proposal focuses on preventive measures in the Token system to limit the amount of fraud.

S.7 Security controls

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th><strong>Somewhat Effective</strong></th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The solution provides details around its technical access components and controls (S.7.1).
However, more detail is required on the operational and procedural components and controls (e.g., data retention and disposal controls, physical security, operations security, monitoring, and incident response) (S.7.2). The proposal notes that these have not yet been finalized but will be completed prior to general availability of the solution. Managerial policies and oversight need additional information on all four components, including how the system will integrate with existing processes, a description of how it is adaptable to enterprise-level security architectures, etc. (S.7.3).

S.8 Resiliency

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The proposal states that the solution has high availability, but it is not able to provide target availability metrics and plans for meeting them at this time (S.8.1); instead, it will do so in the future in collaboration with providers. The proposal states that the Token cloud components can be taken offline and a new instance can be operational within seconds.

Business continuity planning, disaster recovery plans, resourcing and contingency testing planning will be done at a later time with providers (S.8.2, S.8.4, S.8.5).

S.9 End-user data protection

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Token has controls and mechanisms that protect end-user data throughout the end-to-end payment process – all data is encrypted in transit and at rest (S.9.1). Token’s SDK’s provide security mechanisms and procedures to ensure end user data is protected and not revealed to unauthorized parties.

PII is protected from unnecessary disclosure and all operators and providers must have robust mechanisms for protecting sensitive information. The Payer and Payee need to know only the Token Account Number to initiate and receive payments, rather than any sensitive information (S.9.2, S.9.3).

However, the greatest security risk for end-user data is the theft of end-user private keys. Enterprise entities can store private keys in hardware trusted execution environments while consumers can use an app that stores the private key. The system does continuous key rotation of all keys as a security measure.

S.10 End-user/provider authentication

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Token requires authentication of end users, providers and other parties to be done through the use of the digital signatures and certificates (S.10.1). These ensure that payments reach the intended payee at the intended payee account. Certificates are attached with each API call.
providing cryptographic proof of the Payee’s name and that they own the account (S.10.2). Providers can increase the number and types of signatures needed for API calls based on the risk-weighting of the transaction (S.10.4). Providers can also re-authenticate users based on their own custom limits per token, per account or per user and smart tokens can include rules for authentication levels to be redeemed (S.10.5).

However, the solution is dependent on providers for enrollment and if the authentication of end user is breached at time of enrollment, then the Token system will have fraudulent payments. More clarity would be helpful on the requirements for identification and verification for enrolling end users (S.10.1).

S.11 Participation requirements

Very Effective  Effective  Somewhat Effective  Not Effective

**Rationale:**

While Participant rules are not yet developed, Token provides detail on the elements of participation requirements. The solution has put in place participation requirements for providers that are relevant to the providers’ role within Token. It requires that data handled by the TPS be encrypted and securely transmitted and stored. Providers must also demonstrate their ability to store system-level keys and other sensitive data in ways that meet industry-level security standards (S.11.1).

When providers join Token, they must show that they are compliant with regulations and that they can fulfill all the operational, financial and legal obligations of participating in the Token network (S.11.2).

Finally, Token monitors balances and payments between providers to ensure that all providers comply with transaction time and settlement requirements. If providers do not comply, they are restricted or removed (S.11.3).

Speed (Fast)

F.1 Fast approval

Very Effective  Effective  Somewhat Effective  Not Effective

**Rationale:**

The solution processes payment requests in milliseconds. However, the proposal notes that “latency depends on how long it takes the Payer provider to return a Good Funds response.” The proposal states that it will reduce the number of systems and round trips to complete a transaction to keep the elapsed time to a minimum.

F.2 Fast clearing

Very Effective  Effective  Somewhat Effective  Not Effective
**Rationale:**
Clearing occurs immediately after approval in the solution. Assuming approval is real-time, so it clearing.

**F.3 Fast availability of good funds to payee**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
This criterion covers the completion of payment initiation to the point when funds can be withdrawn or transferred by the payee. Token processes the request from the payer’s provider instantly at the payee’s provider. However, the availability of the funds to the payee depends largely on how quickly the payee’s provider can make them available. Token will require the provider to credit the account within a maximum time frame and enforce through licenses that are monitored. The QIAT has interpreted this to mean that availability of funds will be within one minute.

**F.4 Fast settlement among depository institutions and regulated non-bank account providers**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution settles in commercial bank money. The operator is a large global bank, which runs a shared ledger. Participating banks move money from the existing Fed-operated clearing and settlement systems to an account at the Operator. The Operator then settles between accounts at the Operator. The proposal envisions optional participation by the Fed – Token would want the Fed to operate 24/7 and provide a direct connection with the Token Global Ledger to enable account settlement in real-time.

While the settlement of accounts at the operator can be fast, the solution does not fully satisfy the criteria for fast settlement as there is not enough clarity on the approach to managing the risk exposure of the large global bank acting as the operator.

**F.5 Prompt visibility of payment status**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token sends a status message to providers within five seconds of each stage of payment process, although the provider is responsible for notifying the End User.
Legal

L.1 Legal framework

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution works with providers and entities that comply with current regulations and laws (KYC, OFAC, AML/BSA), and believes that this compliance provides the oversight necessary to implement Token. It recognizes that these will evolve over time and that it depends on participant compliance. Token expects to have the legal framework developed by June 2017. As such, the proposal acknowledges a need for a Legal Framework and sets out a path to complete it, but it is not yet complete and more detail is not provided on the outlines of a framework. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

L.2 Payment system rules

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token has not yet developed the payment system rules, which include “requirements, standards/protocols, and procedures that govern the rights and obligations of all end users, providers, payers, and payees (L.2).” Token expects to have the payment system rules developed by June 2017. The proposal acknowledges a need for Payment System Rules and sets out a path to complete it, but it is not yet complete and more detail is not provided on the outlines of a framework. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

L.3 Consumer protections

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token has not yet developed a legal framework around consumer protections, which require that it “has a legal framework and procedures that allocate legal responsibilities, allocate financial responsibility, and support error resolution for payments made to or from natural persons for personal, family, or household purposes (L.3).”
The proposal acknowledges a need for a legal framework addressing consumer protection and sets out a path to complete it, but it is not yet complete and more detail is not provided on the outlines of a framework. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”
L.4  Data privacy

Rationale:
Token has not yet developed a legal framework around data privacy, which requires that it “has 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. It should also have an approach to secure information that should not be disclosed (L.4).”

The proposal acknowledges a need for a legal framework addressing data privacy and sets out a path to complete it, but it is not yet complete and more detail is not provided on the outlines of a framework. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

L.5  Intellectual property

Rationale:
The solution’s approach to intellectual property relies on the Token License Agreement (TLA) that each provider signs. This TLA indemnifies the provider from third-party rights related to patents, trademarks, copyrights, and trade secrets. Prior to general availability of the solution, Token will conduct a legal review to ensure Token is clear of any intellectual property infringements.

Governance

G.1  Effective governance

Rationale:
The solution has not yet developed governance, which requires that it “should have decision and rule-making processes that are transparent and support both the solution’s objectives and public policy objectives (G.1).” It plans to collaborate with NACHA on this in the future. Token also anticipates a Scheme Management Board to manage and evolve the Token Scheme and will develop governance in concert with industry and legal experts by June 2017.

As such, the proposal acknowledges a need for effective governance and sets out a path to complete it, but it is not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

G.2  Inclusive governance
Rationale:

The solution has not yet developed inclusive governance, which requires that it “should allow for input and representation from diverse stakeholders (e.g., end users, operators, providers, and regulators) and support the public interest (G.2).” It plans to collaborate with NACHA on this in the future. Token also anticipates a Scheme Management Board to manage and evolve the Token Scheme and will develop governance in concert with industry and legal experts by June 2017.

As such, the proposal acknowledges a need for effective governance and sets out a path to complete it, but it is not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”
## APPENDIX A: ASSESSMENT SUMMARY

**UBIQUITY**

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.1: Accessibility</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.2: Usability</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.3: Predictability</td>
<td>○</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>U.4: Contextual data capability</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.5: Cross-border functionality</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.6: Multiple use case applicability</td>
<td>○</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

**EFFICIENCY**

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.1: Enables competition</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.2: Capability to add value-added services</td>
<td>○</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>E.3: Implementation timeline</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.4: Payment format standards</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.5: Comprehensive</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.6: Scalability and adaptability</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.7: Exceptions and investigations process</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SAFETY AND SECURITY**

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.1: Risk management</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.2: Payer authorization</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.3: Payment finality</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.4: Settlement approach</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.5: Handling disputed payments</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.6: Fraud information sharing</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

✓ = QIAT Assessment  ○ = Proposer Self-Assessment
<table>
<thead>
<tr>
<th><strong>SAFETY AND SECURITY (cont’d)</strong></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.7: Security controls</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.8: Resiliency</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.9: End-user data protection</td>
<td>○✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.10: End-user/provider authentication</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.11: Participation requirements</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SPEED (FAST)</strong></td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
<td>Not Effective</td>
</tr>
<tr>
<td>F.1: Fast approval</td>
<td>○✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.2: Fast clearing</td>
<td>○✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.3: Fast availability of good funds to payee</td>
<td>○✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4: Fast settlement</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.5: Prompt visibility of payment status</td>
<td>○✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>LEGAL</strong></td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
<td>Not Effective</td>
</tr>
<tr>
<td>L.1: Legal framework</td>
<td>○✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.2: Payment system rules</td>
<td>○✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.3: Consumer protections</td>
<td>○✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.4: Data privacy</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.5: Intellectual property</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>GOVERNANCE</strong></td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
<td>Not Effective</td>
</tr>
<tr>
<td>G.1: Effective governance</td>
<td>○✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G.2: Inclusive governance</td>
<td>○✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX B: PROPOSER RESPONSE TO QIAT ASSESSMENT

Token is a startup company with a groundbreaking solution for how to securely move value instantly across the world. The solution is optimized for where the market is heading, rather than for where it is today. We’ve designed, and are now implementing what we believe to be the payments infrastructure for the next 100 years.

As such, some of the interim solutions may appear sub-optimal for today’s needs. For example, relying on large banks for the Currency Ledger, is an interim solution until Central Banks run the Token Ledger, or any other modern Ledger that supports crypto-signed requests and responses and 2-phase commits across currency ledgers.

In our proposal we have focused on the core functions of the solution. Auxiliary functions and processes (nevertheless critical for a payments system in production) such as fraud management, error resolution, liabilities, governance, consumer protection, data privacy, rule book, operations, etc. need further development and will, no doubt, be resolved in due course. We expect to achieve “Very Effective” in all those areas by the time the solution is ready for production deployment.

Token is looking forward to collaborating with the payments industry to resolve those critical functions and processes in order to bring to market a complete solution that addresses the Feds current and future requirements.

Specific evaluation criteria comment:

S.10: QIAT says “if the authentication of end user is breached at time of enrollment, then the Token system will have fraudulent payments.” That is true but the payments are limited only to that one bank. A token identity is created on the mobile device. That identity is then linked to each bank by the user after he logs into that bank. If a particular bank has inadequate security, an attacker could only make fraudulent payments only at that one bank. Those payments would still be limited in amount by the bank. There is always a tradeoff between security and ease of use. This is an economic decision which can only be assessed once the system is in operation. In cases where fraud rises to unacceptable levels, it is appropriate to take additional steps to reduce the fraud. The system we describe is a base level implementation which is an extremely secure approach for the amount of friction it produces.
TOKEN PROPOSAL

TASK FORCE ASSESSMENT COMMENTS

Please share your concerns about this proposal’s assessment against the Effectiveness Criteria.

I do not believe that the settlement proposal is effective. The use of a single global bank and a 24x7x365 Fed is feasible.

Smart Tokens an interesting solution with multi-level security—account & payment authorization, restricted access using smart contracts/tokens, DDOS and intrusion detection.

Solution still in development—dependent upon 3rd party developers to create new apps. Solution does not address how the adoption between key participants in ecosystem—billers, merchants, and end-users—will take place. No guidance on rules, governance, legal framework, dispute resolution, errors and consumer protection.

Some big names backing the solution in pilot - will be interesting to see how it comes to 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 did not answer all sections of the template and 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 did not include the unbanked. The solution is still in development. There is no risk management or legal framework. The solution did not include L.3, L.4, L.5, G.1, and G.2.

Please submit any comments about this proposal’s assessment against the Effectiveness Criteria.

The legal and governance frameworks are works-in-process. I disagree with the arbitrary QIAT ratings for L1, L2, L3, L4, G1 and G2.

Agree as assessed. Solution proposal is very light on details of key criteria elements and many components of the Legal and Governance criteria are still under construction.
The ratings are adequate—several Somewhat Effective in the Legal area, and my interpretation of the proposal agrees with this.

Need development of legal and governance criteria, as noted by QIAT.

Token involves some very creative technology but offers nothing in the way of legal structure, governance or operational rules. If there were a rating between Agree and Disagree, I would score the assessment that way.

Rules and Governance are not explained.

Innovative technology does not need to replace core banking system technology.

This proposal appears to be flexible and complementary, and does address B2B.

Is an interesting concept, but not sure how widely this Tokenization concept could be adopted, as there must also be a tokenization module running inside each bank, through Token Provider Software (TPS) and for faster payments it would be a challenge.

Providing a modernized solution to the outdated rails based on the “smart tokenization” model with a power set of rules which will solve the two problems of “now global standard open API and no global standard for moving money.” Token requires a central bank to maintain accounts – a large global bank is central to the proposal.

Contextual data capability appears to be rated too highly because the solution is described as being able to “hold” data, but not how various participants would know exactly what data is expected to be transmitted or what would be received. Descriptions of value-add services (and ability to support amongst various participants) in order to support the given rating. Rules and governance are too highly rated, as there are not specifics provided.

This may be overly positive depending on the participant who would implement using this technology. Without the pilot or testing references to scaling, this is an area of concern. The areas of Legal and Governance could easily be enhanced through partnership or handled by the implementing entity of the technology, should it prove to scale.

Disguises user’s identity through the use of tokens. Secured with cryptography. Lacking governance. Dependent on single large bank as operator. Technology still being built. Proposed pricing as a percentage of principal. Dependency on a single bank seems to block adoption. Doesn’t address adoption by merchants, billers, etc. Does not appear to be a complete solution.

Agree: I believe the assessment was correct. I like how it can be integrated with existing core processing systems. Relies on one large FI or central bank to be operator. Areas were not fully addressed such as the rules, legal, and governance areas.

Proposer’s solution is more conceptual in its offering of a payment solution. It is relying a lot on future innovation and technologies to meet established criteria.
TASK FORCE SOLUTION-ENRICHING COMMENTS

Ubiquity

Solution does not offer cross-border functionality which limits opportunity to provide to users who need this option. Timeline of cross-border implementation was not clear.

Thank you for this innovative proposal. The use of tokens for transactions allows for a more secure structure for faster payments.

I would have liked to see more details regarding the value proposition for financial institution participation. Additionally, currently, a few core service providers control a lot of what products small and medium financial institutions are able to provide. In order to be successful, Token will need to sell the solution to many of these providers. 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.

The overall solution could be enriched by describing how the Providers (financial institutions and non-regulated account providers) make the Token application available to their end-users through APIs developed by third party developers.

Additionally, the solution could be enriched by including a plan to reach ubiquity and interoperability with other faster payment systems.

Proposal should describe more fully how capabilities of the solution or adoption will enable the ability to have the surety to reach any bank account in the US.

It seems as though this solution allows for not only banks to provide accounts but also non-regulated financial institutions. It would be helpful to have some additional detail regarding how non-regulated financial institutions would gain access to the system. This proposal was also lacking details on how this would reach all users which includes those that are underbanked or unbanked. After reading the proposal I was struck by the lack of explanation about a value proposition for end-users. As an end-user, and more specifically a government end-user, I didn't understand why we would accept this as a payment alternative.

(1) Technology conceptual, beta (2) pricing as % of principal (3) settlement not clear (4) not really end to end.

Just here that it sounds like Token, Inc. has a good framework on what they want to do but are still working and under development with other aspects of their proposal. My concern here is if their timeframe, from an internal aspect of their company, will actually meet the target guidelines.
It would be helpful to better understand how cross-border payments would function. There was insufficient detail in the proposal as to the role and detailed responsibilities of the additional party.

Not at all ubiquitous. Only addresses B2B.

**Efficiency**

Implementation is vague for the timeline in which to have solution available. More clarity in who will have access to payment data for disputes and other research needs.

The use of a large bank as the sole provider for settlement services would limit competition. While contemplated, the solution should further explain and pursue the Federal Reserve to provide the settlement services needed.

Describe more fully how contextual data that can be held within in the Token is understood (and supported) by all participants that need to deliver or accept that data.

**Safety and Security**

Reliance on others to develop the risk management and legal framework. Address of loss, theft, etc., was not included in how these situations would be handled. Expectation on FRB operating under a 24/7 schedule is unrealistic. What other option would be available to have the solution viable? The idea of the fraud monitoring system was agreeable but who is allowed access to the information and why can’t trends of fraud be provided to others?

The solution could be enriched by further describing the risk and liquidity associated with settlement being conducted through a shared ledger which is run and managed by a large global bank.

Quite simply, I see a number of tests on Safety & Security here. Although interesting, can a vulnerability testing phase show enough information to validate security?

Too much is left up to the providers—basic requirements should be listed.

Use of latest encryption technologies for all data elements, as well as the policy of never transmitting any sensitive payment information over the internet, likely provides a high level of data protection. The solution also calls for the local storage of keys, preventing the consolidation of valuable information in a single repository. Based on the assertion that the solution complies with PSD2, I assume that means it leverages multi-factor authentication, which is a good thing.

**Speed (Fast)**
Reliance on FRB 24/7 availability is only mechanism to have solution be offered as real-time. As this is not a likely option, at least in the near future, then reliance on FED windows for payment transfers is required. This limits payment timeframes, particularly for West Coast users based on timeframes.

Legal

As stated in the QIAT assessment, this area requires development in order to be considered effective.

I would have liked to see some suggested implementations for participation agreements and legal framework, particularly in light of the need to ensure that all financial institutions have equal access to a faster payments system.

The solution could be enriched by providing insight into the payment system Rules and legal framework. Additionally, the solution could be enriched to further explain The Token Foreign Exchange Service and the associated Rule and legal framework associated with the service.

Describe rules more fully so that participants understand their various roles and responsibilities.

This area could easily be enhanced through partnership or handled by the implementing entity of the technology.

Needs development in this area—relies on current regulations/laws without providing any requirements/baselines.

Governance

I would have liked to see some suggested implementations for participation agreements, legal, and governance framework, particularly in light of the need to ensure that all financial institutions have equal access to a faster payments system.

The solution could be enriched by providing insight into the governance and how disputes, error resolution, and consumer protection would be handled within the Token system.

The use of NACHA as a governance body perpetuates the lack of inclusion and transparency as only FIs are allowed to vote and the vote is not disclosed publicly. Token should consider a governance model similar to the US Payment forum in which equal representation and voting rights are given to all stakeholders.

Describe governance more fully.

This area could easily be enhanced through partnership or handled by the implementing entity of the technology.

As the governance structure has yet to be established, it needs to include end-users to help make this a viable system and to voice their unique perspective.
Needs development in this area.

1) There is a lot of risk in having a single operator, unless that operator is chosen wisely (e.g., independent, non-competitive position, etc.). Otherwise they may gain a monopolistic position, among other benefits. Suggest adding basic recommended criteria for the position this operator should be in the industry (e.g. government vs. non-government, bank vs. non-bank, etc.).

2) It seems unwise to leave pricing up to the providers. This could lead to confusion and risk of gouging. Suggest changing this or providing additional context on controls that would serve to protect the public and the system.

3) The minimal rules provided thus far seem inconsistent. There is mention of payments being irrevocable after submission but then later stating the payment could fail or be rejected for some reason.

Token’s response to G.2.4 states that it will ensure that specific stakeholders and stakeholder groups are proportionately represented. It’s unclear (1) what “specific” groups are being referred to and (2) in what capacity they will be represented. If the representation is on the governing body and the “specific” groups include all relevant stakeholder groups, this is a strong response.

G.1 Effective governance & G.2 Inclusive governance: SOMEWHAT EFFECTIVE, but it will be difficult to achieve such a governance structure.

There was no governance provided in the executive summary. However, in the Q&A “Token anticipates a Scheme Management Board (SMB) responsible for performing the functions of management and evolution of the Token Scheme. Token will consult with industry and legal experts in the field to develop governance as part of the Rulebook. Token expects to have this completed by June 2017.”
Proposer responses to the Task Force comments were optional and not all proposers chose to respond
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: Token, Inc.

Summary Description of Solution:

Token is a set of software and service components that enables payers to make direct push and pre-authorized pull payments using digital tokens. Providers (depository institutions and non-regulated account providers), merchants, and other entities install the Token Provider Software (TPS), which supports their participation in the Token system. A “token” is a unique digital reference or identifier that maps back to an individual’s sensitive data (e.g., account information, personally identifiable information or “PII”) but has no meaning on its own, other than as a reference. The Token system enables an advanced capability called “smart tokenization,” which involves the creation of tokens that include terms dictating access to the token’s underlying asset. For pre-authorized payments, payees use these “smart” tokens to access funds in the payer’s account under terms that the payer has previously set. The network uses digital signatures to authenticate payers and payees and to authorize payments.

Payers and payees access Token through an application program interface (API), which allows third-party developers to build and integrate applications onto the Token platform. Participating providers use the TPS to send and receive payments through the Token system, and the Token Hub routes messages that are based on the tokens between providers. A trusted third party—such as the Federal Reserve—would serve as the system’s Token Authority Service (TAS). The TAS manages the mapping between end-user data and their tokens, as well as end-users’ and providers’ digitally signed certificates.

Settlement is conducted through a shared ledger run by the operator (a large global bank). Providers move money into accounts at the operator to enable immediate settlement. The Token Foreign Exchange Service allows funds to be moved instantly across different currencies. Token supports quotes and rates from multiple foreign exchange service providers.

Executive Summary of the Proposal

Major strengths

- Token uses innovative, leading-edge security. The solution protects end-user data and mitigates risk by using digital signatures and certificates to authenticate and authorize every payment. Every entity in the system is associated with one or more public keys, with corresponding private keys. As long as private keys are kept secure, digital signatures verify that every API call or request to a third party has been initiated by the right entity, thereby reducing the risk of errors, failures, and fraud.

- Smart tokens allow payers to have more control and flexibility with their pre-authorized pull payments. The tokens enable programmable payments by defining the terms that govern access to an asset or by adding contextual information. They are secured by advanced cryptography and tied to a specific payee.

- The Token solution is layered onto providers’ existing account management systems and does not replace core banking systems.

Areas for improvement and enhancement

- The proposal indicates that a large global bank will be the operator of the solution. Participating banks will open accounts at the operator, and Token payments will be settled through those accounts. This model poses significant risk to the global bank.
– The overall implementation plan does not currently address adoption by billers, merchants, or end-users. In addition, the value proposition for providers to adopt the solution and make it available to end-users needs strengthening.

– The solution has not yet developed rules, governance, or legal framework; in particular, it lacks process for handling disputes, error resolution, and consumer protection.

■ **Use cases addressed**

– The solution addresses all four major use cases: P2P, P2B, B2P, and B2B.

■ **Proposer’s overall ability to deliver proposed solution**

– The solution is based on innovative technologies and approaches that are still in the early stages of development, with expected completion by the end of 2016.

– The proposal does not describe any live pilots in market, nor is there a track record for similar developments or implementations in the past.
**Ubiquity**

**U.1 Accessibility**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution facilitates payments to and from all types of payment accounts (as determined by the individual provider) at both depository institutions and non-regulated account providers (U.1.1). Token also supports multi-currency payments through Token Foreign Exchange Services, which has providers with accounts in multiple countries (U.1.3). The proposal demonstrates that Token is technically feasible for providers to adopt and cites regulatory pressure (PSD2 in Europe), improved security, reduced costs, and the opportunity for new business models as the primary motivators for providers to adopt the solution (U.1.5).

However, the proposal needs to describe how payers can be sure that their payments can reach all payees, even those with providers that are not part of the Token network (U.1.2). For example, more detail would be helpful regarding how the solution will authenticate and enroll first-time end-users who use a provider that is not yet on the Token network.

**U.2 Usability**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token supports usability but depends on providers for the end-user experience. Token is available through any channel, including mobile, online, and offline channels, but it ultimately depends on providers’ using the Token SDK (software development kit) to build applications across channels (U.2.1).

Token enables initiation of payment with limited information. The payer needs to know the payee’s Token Account Number (TAN), but application developers can create a service that maps a user’s TAN with an alias such as email address or phone number (U.2.2).

The solution itself is available 24x7x365 but depends on providers to make it continuously accessible to end-users (U.2.3). In addition, providers are responsible for accommodating varying levels of technology proficiency and usability needs among end-users. The proposal does not articulate baseline operating rules or guidelines to ensure a minimum user experience, though it does refer to a “Rulebook” (p. 32) (U.2.4).

**U.3 Predictability**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token’s design ensures reliable delivery of its baseline core features—particularly the digital signatures and payment process—within its network and across channels (U.3.1-2). The solution uses REST protocols as its standard communication and messaging protocols with providers (U.3.3). The solution is described as “smart token” to distinguish it from other payment methods (U.3.6).
The proposal does not address the error resolution protections, rights, and liabilities of the payer and payee (U.3.5). The solution relies on providers to communicate the baseline features of the payment experience to end-users (U.3.2, U.3.4) without operating rules or guidelines to ensure that this happens.

U.4 Contextual data capability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale**

The proposal indicates that contextual data will be provided in the ISO 20022 standard messaging format or structured in any form agreeable to two parties (U.4.1). The smart token for pre-authorized payments is complex and includes contextual data with the payment.

Although the capability for contextual data exists, more details are needed about how the solution will enable easy integration with business and personal finance systems (U.4.2). More details are also needed on how Token’s approach will balance the need for flexibility with the need for standards. Token is in process of working with a large ERP company that will help inform further contextual data needs (U.4.3).

U.5 Cross-border functionality

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The proposal does not currently have cross-border functionality, but this functionality is planned for the initial implementation. Given that current faster payment schemes do not yet interoperate, the solution allows for interoperability with similar payment systems in other countries through “Token Instant,” which enables banks across countries to share a global ledger if they are on the Token Network (U.5.2). The solution does require providers to make advance disclosure of fees, exchange rates, and costs (U.5.3), and the solution supports conversion of currency through an FX service provider (U.5.4).

More information would be helpful on how the solution would accommodate the varying regulations among countries and how it would handle settlement (U.5.1). In addition, more detail would be helpful on the implementation timeline, including the adoption plan for providers in other countries to join the global ledger (U.5.5).

U.6 Applicability to multiple use cases

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution addresses all four major use cases: P2P, P2B, B2P, and B2B.
Efficiency

E.1 Enables competition

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Token’s API-based system and the SDK promote competition and encourage providers and application developers to create value-added services (E.1.1, E.1.4).

The solution also allows entities to choose among providers, switch providers, or use multiple providers. The end-user can disable a Token account with one provider and enable the same Token account at a new provider’s website. Multiple providers can be used by enabling Token at each provider using the end-user’s Token alias (E.1.2). The proposal can be strengthened by explaining in detail how end-users can choose the payment account to use if an alias is associated with multiple providers. The solution relies on third parties to develop the mapping between personal and account IDs, which is needed for portability and easy switching of providers.

E.2 Capability to enable value-added services

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Token allows all providers and third parties to integrate, build applications, and create value-added services with the API and SDK (E.2.1). Contextual data resides in the smart tokens. The Token system uses ISO 20022 for data fields in the smart token.

Providers are responsible for setting fees for value-added services and disclosing that these fees are optional to end-users. However, it is unclear what requirements the solution imposes (if any) on providers regarding disclosure (E.2.3)

E.3 Implementation timeline

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The Token solution is still under development and was expected to be complete by the end of 2016. The implementation timeline assumes that the solution will achieve market ubiquity through strategic partnerships with the ten largest providers over a 24-month period. Reaching “the long tail of the provider market” will take an additional: three years (p. 45).

To achieve its objective, Token needs to hire and retain key talent; the proposer expected to raise the capital to do so in the second half of 2016. The solution will be funded through venture capital money; the proposal states that Token is in process of raising a $12M Series A, with interest from eleven VCs and four EU banks.

The implementation plan would benefit from more detail on how it will achieve ubiquity with not just providers but also with the businesses, billers, and merchants where Token plans to use smart tokens. Further, the plan needs to address expected implementation and ubiquity hurdles (beyond the need to hire talent) and to articulate strategies for overcoming those hurdles.
**E.4 Payment format standards**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token supports standard messaging formats like ISO 20022 but focuses on new, proprietary data formats in its flexible API (E.4.1-2). These proprietary formats are flexible and able to accommodate complex rules within smart tokens (E.4.4).

However, the solution has not committed to having the proprietary formats developed and/or published by a recognized standards development organization (E.4.5). In addition, more clarity is needed as to how ISO 20022 can be embedded in the smart token while still ensuring the integrity of any translation required between the proprietary format and ISO 20022 (E.4.1, E.4.3).

**E.5 Comprehensive**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
In concert with providers, Token provides the technical design and support needed for all aspects of the end-to-end payment process (E.5.1-2).

**E.6 Scalability and adaptability**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Thanks to the flexible API, Token’s technical design is readily adaptable and supports the solution’s projected use cases (E.6.1, E.6.3). The server can handle at least 10,000 transactions per second based on scalable software and partnership with cloud service providers (E.6.2).

**E.7 Exceptions and investigations process**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token gives providers the details of all transactions, including any exceptions (E.7.1). It also ensures that transaction data is created, recorded, and then retained appropriately for post-transaction evaluation (E.7.2).

The solution does not provide any tools, messages, alerts, notifications, or related protocols to support the ability to address exceptions in a reasonable timeframe (E.7.1). It does not provide any case management tools for post-transaction evaluation (E.7.2), nor can it aggregate exceptions data to spot patterns beyond the individual-provider level (E.7.3).
Safety and Security

S.1 Risk management

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token has not yet developed a risk management and legal framework, although the proposal does mention a collaboration with NACHA to develop policies and governance in time for the product release (S.1.1, S.1.5).

The operator of the Token network is a large global bank that will use the Token ledger software. Each participant bank will set credit limits for settlement with the operator (S.1.2). More detail on risk management at the operator level would be helpful.

The proposal also indicates that the likelihood of operational risk and unauthorized, fraudulent, or erroneous payments is low, given the automation of the system and the security of user authentication. But the proposal does not explain how Token will address any remaining risks, such as the risk arising from incorrect storage, loss, or theft of private keys or from account takeover. The proposal simply states that these risks are the providers’ responsibility (S.1.3-4).

S.2 Payer authorization

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution requires payers to authorize each payment with their providers; the system then uses the keys of both the payer and the payee’s provider to execute payment (S.2.1). For pre-authorized payments with “smart tokens,” the payer can specify a number of parameters, which the payer can revoke or change at any time (S.2.2-3).

S.3 Payment finality

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token requires the payer’s provider to approve each payment following initiation to ensure good funds (S.3.1). The payment becomes irrevocable when the payer’s provider approves the payment and creates an IOU to the payee’s provider (S.3.2). In the event of a disputed payment, a payee can compensate a payer by initiating a new payment that returns the money to the payer through a second transaction.

The solution does not yet include mechanisms and processes to protect or compensate the payer in the event that the payment is disputed; these mechanisms and processes will be defined in the upcoming Rulebook (S.3.3).
### S.4 Settlement approach

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution settles in commercial bank money; the operator, a large global bank, runs a shared ledger. Participating banks move money from existing Fed-operated clearing and settlement systems to their accounts at the operator, which then settles between these accounts. The proposal envisions optional participation by the Fed; Token would like the Fed to operate 24x7 and to provide a direct connection with the Token Global Ledger to enable account settlement in real time.

More details on the settlement approach would be helpful. In particular, the proposal would be strengthened by articulating the rules and timing of settlement (S.4.1) and, most critically, by explaining how operator risk will be managed, given that the settlement approach depends on a single global bank for a payment system of national scale (S.4.2).

### S.5 Handling disputed payments

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Any party in the transaction can request prompt, voluntary return of funds from the payee in a disputed payment through an API call that Token provides (S.5.3). However, the solution’s rules for handling disputed payments do not include “requirements, processes, and timeframes” for handling disputed payments or mechanisms to hold rule violators accountable. (S.5.1).

Providers determine the transactions for which they will accept disputes.

Token has not yet developed an approach—including the “delineation of roles, responsibilities and liability allocation”—that reasonably protects business, government, and consumer payers against losses from fraud or errors (S.5.4-.5). The proposal does, however, allude to a collaboration with NACHA to develop policies and governance in time for the product release.

### S.6 Fraud information sharing

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Token tracks suspicious or fraudulent members of the system. It provides a look-up function to identify such members and to send alerts to providers through an API (S.6.3).

Token does not require fraud information-sharing among providers to facilitate the management and monitoring of fraud (S.6.1). Providers are expected to use and retrieve data from the Token software and then to use their own fraud information-sharing systems (S.6.2, S.6.4-.7). The proposal focuses on preventive measures in the Token system to limit the instance of fraud.

### S.7 Security controls

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>
Rationale:
The solution provides details around its technical access components and controls (S.7.1). More detail is needed, however, on the solution’s operational and procedural components and controls (e.g., data retention and disposal controls, physical security, operations security, monitoring, and incident response capabilities) (S.7.2). The proposal notes that these elements have not yet been finalized but will be completed prior to the solution’s becoming generally available. The proposal could be strengthened further by providing more information on managerial policies and oversight. Specifically, the proposal should explain how the system will integrate with existing processes, as well as how it can adapt to enterprise-level security architectures (S.7.3).

S.8 Resiliency

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The proposal states that the solution has high availability, but it is not yet able to provide target availability metrics or plans for meeting those targets (S.8.1). Token will provide these metrics and plans later, in collaboration with providers. The proposal states that the Token cloud components can be taken offline, and a new instance can be operational within seconds. Business continuity planning, disaster recovery plans, resourcing, and contingency testing planning will likewise be completed at a later time with providers (S.8.2, S.8.4-5).

S.9 End-user data protection

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
Token has controls and mechanisms that protect end-user data throughout the end-to-end payment process. All data is encrypted in transit and at rest (S.9.1). Token’s SDKs provide security mechanisms and procedures to ensure that end-user data is protected and not revealed to unauthorized parties.

PII is protected from unnecessary disclosure, and all operators and providers must have robust mechanisms for protecting sensitive information. The payer and payee need to know only the TAN to initiate and receive payments (S.9.2-3).

The greatest security risk for end-user data, however, is the potential theft of end-user private keys. Enterprise entities can store private keys in hardware-trusted execution environments, while consumers can use an app that stores the private key. The system continuously rotates all keys as a security measure.

S.10 End-user/provider authentication

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
Token requires authentication of end-users, providers, and other parties through the use of the digital signatures and certificates (S.10.1). These ensure that payments reach the intended payee
at the intended payee’s account. Certificates are attached to each API call, providing cryptographic proof of the payee’s name and ownership of the account (S.10.2). Providers can increase the number and types of signatures needed for API calls based on the risk-weighting of the transaction (S.10.4). Providers can also re-authenticate users based on their own custom limits per token, per account, or per user, and smart tokens can include rules for authentication levels to be redeemed (S.10.5).

The solution depends on providers for enrollment, and if the authentication of the end-user is breached at the time of enrollment, the Token system will generate fraudulent payments. More clarity would be helpful on the requirements for identifying and verifying end-users at the time of enrollment (S.10.1).

S.11 Participation requirements

Very Effective  Effectivem  Somewhat Effective  Not Effective

Rationale:

While participant rules are not yet developed, Token provides detail on some elements of its participation requirements. The solution’s participation requirements for providers are relevant to the providers’ role within Token. Token requires that data handled by the TPS be encrypted and securely transmitted and stored. Providers must also demonstrate their ability to store system-level keys and other sensitive data in ways that meet industry-level security standards (S.11.1).

When providers join Token, they must show that they are compliant with regulations and that they can fulfill all the operational, financial, and legal obligations applicable to participating in the Token network (S.11.2).

Token monitors balances and payments between providers to ensure that all providers comply with transaction time and settlement requirements. If providers do not comply, they are restricted or removed from the network (S.11.3).

Speed (Fast)

F.1 Fast approval

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:

The solution processes payment requests in milliseconds. However, the proposal notes that “latency depends on how long it takes the payer provider to return a good-funds response.” The proposal states that it will reduce the number of systems and round trips needed to complete a transaction in order to keep the elapsed time to a minimum.

F.2 Fast clearing

Very Effective  Effective  Somewhat Effective  Not Effective
**Rationale:**
Clearing occurs immediately after payment approval in the solution. If approval indeed is real-time, so is clearing.

**F.3 Fast availability of good funds to payee**

<table>
<thead>
<tr>
<th>Effectiveness</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
This criterion covers the completion of payment initiation to the point when funds can be withdrawn or transferred by the payee. Token processes the request from the payer’s provider instantly at the payee’s provider. However, the availability of the funds to the payee depends largely on how quickly the payee’s provider can make them available. Token will require the provider to credit the account within a maximum time frame and enforce this requirement through monitored licenses. The QIAT has interpreted this to mean that funds will be available within one minute.

**F.4 Fast settlement among depository institutions and regulated non-bank account providers**

<table>
<thead>
<tr>
<th>Effectiveness</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale**
The solution settles in commercial bank money. The operator is a large global bank, which runs a shared ledger. Participating banks move money from the existing, Fed-operated clearing and settlement systems to an account at the operator. The operator then settles between accounts at the operator. The proposal envisions optional participation by the Fed; Token would like the Fed to operate 24x7 and to provide a direct connection with the Token Global Ledger to enable account settlement in real time.

While the settlement of accounts at the operator can be fast, the solution does not fully satisfy the criteria for fast settlement, as the proposal does not clearly articulate the approach to managing the large global bank’s risk exposure in its role as the operator.

**F.5 Prompt visibility of payment status**

<table>
<thead>
<tr>
<th>Effectiveness</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token sends a status message to providers within five seconds of each stage of the payment process, although the provider is responsible for notifying the end-user.
Legal

L.1 Legal framework

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution works with providers and entities that comply with current regulations and laws (KYC, OFAC, and AML/BSA) and believes that this compliance provides the oversight necessary to implement Token. It recognizes that these regulations and laws will evolve over time and that the solution depends on participant compliance. Token expects to have the legal framework developed by June 2017.

The proposal thus acknowledges a need for a legal framework and sets out a path to complete it, but it is not yet complete, and sufficient detail on a basic framework is not provided. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

L.2 Payment system rules

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token has not yet developed the payment system rules, which include “requirements, standards/protocols, and procedures that govern the rights and obligations of all end-users, providers, payers, and payees (L.2).” Token expects to have the payment system rules developed by June 2017.

The proposal acknowledges a need for payment system rules and sets out a path to complete them, but they are not yet complete, and sufficient detail on a basic framework is not provided. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

L.3 Consumer protections

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Token has not yet developed a legal framework around consumer protections, which require “a legal framework and procedures that allocate legal responsibilities, allocate financial responsibility, and support error resolution for payments made to or from natural persons for personal, family, or household purposes” (L.3).

The proposal acknowledges a need for a legal framework that addresses consumer protection and sets out a path to complete it, but it is not yet complete. Moreover, the proposal does not provide sufficient detail on a basic framework for protections. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”
L.4 Data privacy

**Very Effective**  Effective  **Somewhat Effective**  Not Effective

**Rationale:**
Token has not yet developed a legal framework around data privacy, which requires that it have “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. It should also have an approach to secure information that should not be disclosed” (L.4).

The proposal acknowledges a need for a legal framework addressing data privacy and sets out a path to complete it, but it is not yet complete and more detail is not provided on the outlines of a framework. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

L.5 Intellectual property

**Very Effective**  **Effective**  Somewhat Effective  Not Effective

**Rationale:**
The solution’s approach to intellectual property relies on the Token License Agreement (TLA) that each provider signs. This TLA indemnifies the provider from third-party rights related to patents, trademarks, copyrights, and trade secrets. Prior to the solution’s becoming generally available, Token will conduct a legal review to ensure that Token is clear of any intellectual property infringements.

Governance

G.1 Effective governance

**Very Effective**  Effective  **Somewhat Effective**  Not Effective

**Rationale:**
The solution has not yet developed a governance model, which requires “decision and rule-making processes that are transparent and support both the solution’s objectives and public policy objectives” (G.1). Token plans to collaborate with NACHA on governance in the future. Token also anticipates creating a Scheme Management Board to manage and evolve the Token Scheme and will develop governance in concert with industry and legal experts by June 2017.

The proposal thus acknowledges a need for effective governance and sets out a path to complete it, but it is not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

G.2 Inclusive governance

**Very Effective**  Effective  **Somewhat Effective**  Not Effective
**Rationale:**

The solution has not yet developed inclusive governance, which requires that it “allow for input and representation from diverse stakeholders (e.g., end-users, operators, providers, and regulators) and support the public interest” (G.2). Token plans to collaborate with NACHA on governance in the future. Token also anticipates creating a Scheme Management Board to manage and evolve the Token Scheme and will develop governance in concert with industry and legal experts by June 2017.

The proposal thus acknowledges a need for effective governance and sets out a path to complete it, but it is not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”