Trust Framework Development Guidance

Draft Version 1.0

Table of Contents

This page is intentionally left blank.

Trust Framework Development Guidance

1 Introduction

The secure identity and access management credential market today can be compared to the bank card industry forty-five years ago. At that time, there were several credit card systems. MasterCard and Visa, for example, served their own member issuers and participating acquirers (relying parties) to provide transaction services for credit cards at the point of sale (POS). Similarly, in the early ATM days, banks serviced only their own customers through proprietary ATM networks. Several decades later, all MasterCard and Visa customers (as well as other providers) can now perform transactions at the same retail POS terminals at retailers nationwide. Likewise, debit card holders from most financial institutions can use virtually all ATMs to withdraw cash, regardless of which banks operate them. Furthermore, cardholders can use both their debit and credit cards in ATMs and POS terminals. In essence, each card federation created a “federation of federations” whereby individual card domains have normalized to achieve super-interoperability.

Over the last decade, government and various companies have implemented identity and access management credential schemes for secure access to their applications. In the past, identity federations such as TSCP established and followed rules and specifications that permitted interoperability, trust and governance within a particular community of interest or domain. More recently, they are starting to set up identity federations in order to facilitate the exchange of credentials across sector communities. A key NSTIC objective is to facilitate interoperability across such communities that use secure credentials and promote their usage when conducting commercial transactions over the Internet; in fact, interoperability is one of the four NSTIC Guiding Principles. In addition to interoperability, the NSTIC strategy also requires the introduction of controls that implement the other three Guiding Principles: privacy-enhancing (and voluntary); secure and resilient; and, cost-effective and easy to use.

As governments and TSCP member companies continue to require highly secure transactions at LOA 4 for Defense and certain other applications, they now also need to be able to authenticate at lower levels of assurance in a federated manner for both government and commercial applications to accommodate participants who conduct less sensitive transactions. In addition, these communities are looking to ensure that their trust frameworks incorporate the types of protections inherent in the NSTIC principles for individuals using business credentials for commercial use.

TSCP has developed a trust governance framework to combine both categories of credentials that will leverage common functions and requirements. This guidance document provides a basis for developing a trust framework that meets the NSTIC goals and provides a common, well-understood basis for trust. Using TSCP’s trust framework as a foundation, this *Trust Framework Development Guidance*, is intended to serve as guidance on developing a trust framework through the example of TSCP’s expansion of its trust framework to include the:

- Extension of the Trust Framework (TF) from serving largely Level of Assurance (LOA) 3/4 PKI users, credentials and transactions to include Levels 1-3 (non-PKI);
- Extension of the TF to harmonize its components and encompass a broad range of practices and requirements accepted across participant categories and industry sectors; and,
- Alignment of the TF with government guidance on secure Internet transactions by incorporating the NSTIC guiding principles.

Sample trust framework documents are provided in the appendices.

1.1 Governance Goal: TSCP Trust Framework Expansion

The majority of existing TFs and federations are based on interoperability standards and governance within a community of interest. The members made a decision to “intra-federate” and follow their rules and governance scheme, for example, TSCP for the Aerospace & Defense community and InCommon for the education community. Within a community, the federation may limit itself to certain types of credentials and transactions, for example, the defense IT community historically has limited itself to the use of highly secure PKI (LOA4) credentials. Many trust framework providers (TFPs) and federations also have opted to interoperate with the Federal government and its partners by aligning to the Federal Identity, Credentialing and Access Management (FICAM) framework and/or achieving a bi-lateral trust with the DoD PKI system. In a move to increase their functionality and value, TFPs and federations are looking to extend their footprints by expanding participation within and beyond their existing communities and increasing the range of credentials accepted.

Thus, the expectation is that federations will look to authenticate between and across communities - inter-federation - in order to minimize the number and types of credentials a user will have to procure and maintain. In addition, in an effort to align with the Federal government’s initiative to promote the usage of secure credentials for routine Internet commercial transactions, they are looking to enable their user bases to use the credentials already issued to them by their employers for commercial Internet transactions. Much like the super-interoperability achieved between the bank card federations, in order to be successful, a trust governance framework is required to provide a common basis for federated identities.

The objective of this document is to produce a “framework-of-frameworks” for potential use by the NSTIC Identity Ecosystem Steering Group (IDESG) that incorporates the NSTIC Guiding Principles using a set of common governance documents. The TSCP Team has taken TSCP’s existing framework as a baseline and is updating it to include the expansion objectives outlined in the Introduction as well as incorporating the NSTIC Guiding Principles and shared lessons learned from the various NSTIC pilots into the new reference governance documents. This*Trust Framework Document Guidance (TFDG) V.1* is available to serve as a resource for governance and to provide a basis for establishing a trusted identity framework that will integrate seamlessly into the identity and access management space. Two subsequent updates will be made to this version.

The TSCP community and its TF provide an ideal test bed for the development of a framework-of-frameworks model. TSCP has served as a federation within its own community domain for LOA 4 PIV-I credentials for many years. It established a bridge service that makes use of specifications and rules that enable its members to issue, accept, and conduct secure authentication and access management in transactions with PIV-I cards through its PKI infrastructure, which is cross-certified to the Federal PKI Bridge and the DoD PKI system. For the NSTIC pilot, TSCP is producing governance documents that will enable interoperability across multiple frameworks, using identities that can be federated across sectors.

1.2 Operational Goal: Federated Bridge for Secure Credentials

As governments and member companies continue to require highly secure transactions (LOA 4) for Defense and other privileged applications, more recently they also have identified applications for which they need to be able to authenticate at lower levels of assurance in a federated manner (for both government and commercial applications). The trust framework laid out in this document addresses assurance levels 1-4 to leverage common functions and requirements across identity and access management credentials.

There are several organizations that have established and operate trust frameworks, i.e., trust framework providers (TFPs). They have set up frameworks and processes by which participants agree to trust and exchange credentials within their community of interest; entities that agree to participate in the framework are trust framework adopters. Exactly how the participants implement and technically interoperate is up to the participants and can be formalized through bilateral agreements.

An operational federation goes a step further. In addition to a trust framework, an operational federation sets up a bridge/hub and infrastructure and establishes technical specifications and rules to support the exchange of credentials, secure authentication and access management. A federation may operate a bridge service for LOA 3-4 PKI credentials and/or a hub/exchange for LOA 2-3 non-PKI credentials. Today, these two services (LOA 3-4 PKI vs. LOA2-3 non-PKI) are typically designed and operated separately with redundant and overlapping functions and separate infrastructures. The trust framework presented in this document is intended to combine both in order to avoid the redundancies and overlaps.

1.3 Approach

Using a combination of pilot results and consultation with industry experts, the TSCP Team will produce a set of reference documents (Appendix A-I) that, along with this TFDG, will help others who may want to establish an open community TF. Through the pilots, the TSCP Team will extend secure credential usage from a closed community to an open community; TSCP members, including both industry and government counterparts will test the use of company and government-issued credentials in the financial services community. In other words, the pilot TSCP member companies and government participants will use their PIV, PIV-I and CAC cards, as well as LOA 2-3 credentials, to access their accounts at Financial Institutions, thereby extending corporate and government credentials into the retail sector, establishing secure Internet transactions within a limited but new segment of the Identity Ecosystem.

The specific tasks that will lead to the revised governance structure and related documents are as follows and illustrated in Figure 1:

1. ***Conduct Pilot.*** The TSCP NSTIC team is conducting a pilot in which users will test the technology and process for using PIV/PIV-I/CAC cards and LOA 2-3 credentials to access their Financial Institution accounts. In addition to technical testing, the TSCP NSTIC team is working with Financial Institutions to explore privacy, business, and liability/legal requirements that need were incorporated into the framework to account for NSTIC principles and marketplace considerations

2. ***Extend Credentials to LOA 2-3.*** Through the Trust Framework Provider Adoption Process (TFPAP), TSCP will extend its credential issuance and usage to accommodate Level 2-3 credentials in accordance with FICAM (i.e., PKI and non-PKI). TSCP will facilitate the normalization of common requirements and processes between the PKI and non-PKI (TFPAP) model.

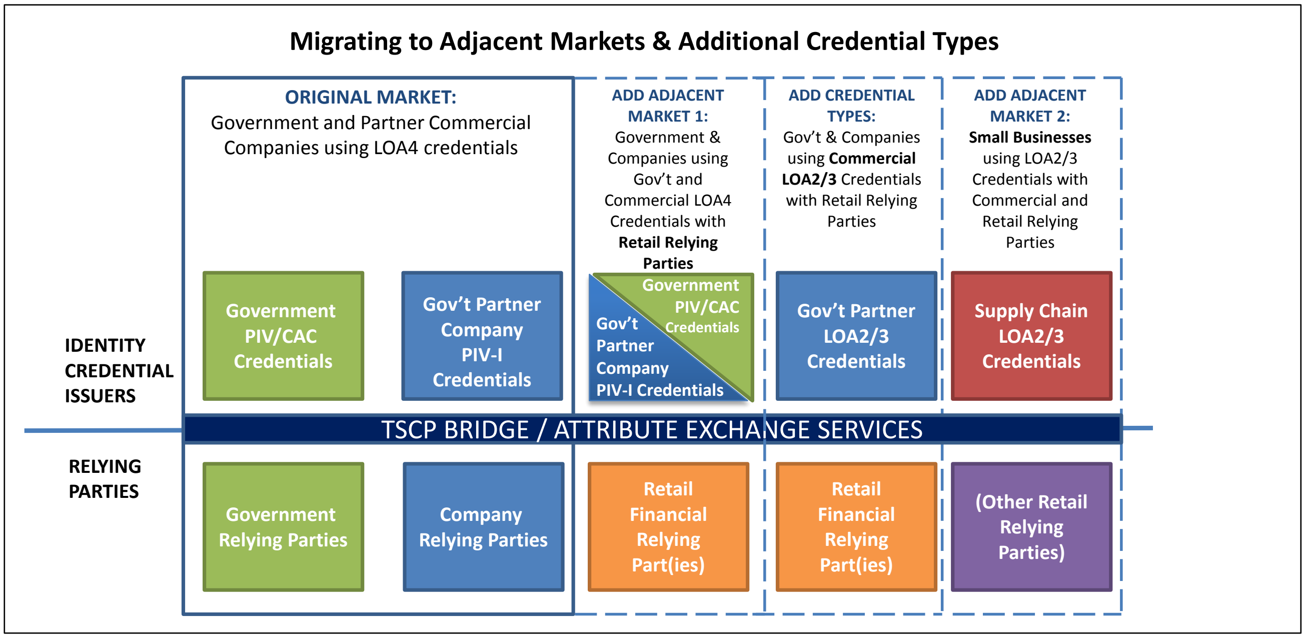
Migrating to Adjacent Markets & Additional Credential Types
ORIGINAL MARKET:
Government and Partner Commercial Companies using LOA4 credentials
ADD ADJACENT MARKET 1:
Government & Companies using Gov't and Commercial LOA4 Credentials with Retail Relying Parties
ADD CREDENTIAL TYPES:
Gov't & Companies using Commercial LOA2/3 Credentials with Retail Relying Parties
ADD ADJACENT MARKET 2:
Small Businesses using LOA2/3 Credentials with Commercial and Retail Relying Parties
IDENTITY CREDENTIAL ISSUERS
Government PIV/CAC Credentials
Gov't Partner Company PIV-I Credentials
Government PIV/CAC Credentials
Gov't Partner Company PIV-I Credentials
Gov't Partner LOA2/3 Credentials
Supply Chain LOA2/3 Credentials
TSCP BRIDGE / ATTRIBUTE EXCHANGE SERVICES
RELYING PARTIES
Government Relying Parties
Company Relying Parties
Retail Financial Relying Part(ies)
Retail Financial Relying Part(ies)
(Other Retail Relying Parties)

Figure 1: Migrating to Adjacent Markets & Additional Credential Types

3. ***Incorporate NSTIC Guiding Principles.*** Using the elements in FIPS, FISMA, the PEM and the NSTIC Guiding Principles, particularly those related to privacy, TSCP will incorporate related controls into its policies, specifications, rules, and reference documentation.

4. ***Develop Accreditation Process.*** TSCP will extend its existing certification, accreditation, and audit checklist to develop an accreditation process that encompasses the new requirements, including levels of assurance 2-4.

5. ***Develop Legal/Business Model.*** In conjunction with its pilot business partners, TSCP will develop a business model that its members use today, and that can be implemented by others to go into

full production in the future. The model includes the framework for determining fees, liability, and legal considerations.

6. ***Revise Governance and Operational Documents.*** TSCP will incorporate the revisions into its governance and operational documents, e.g., CP/CPS, COR and membership agreements. It also will develop a set of reference documents, based upon its published CP and COR, to provide a basis for others to develop federated identities that will be trusted in the federation-of-federations.

2 Trust Framework Development Guidance

Federation governance leads to the expectation and, ultimately, the requirement that the participants will follow the certain minimum processes and procedures when validating identities and attributes, and issuing credentials for enabling access decisions. While the infrastructure and technical standards and specifications are critical to the foundation of these systems, federation schemes cannot be successful without supporting governance structures memorialized in a series of governance documents. The sections that follow describe:

- The Trust Framework
- Services under the Trust Framework
- Federation Operator/Trust Framework Provider Roles & Responsibilities
- Member/Participant Roles & Responsibilities
- Business & Legal Governance Structure

2.1 The Trust Framework

In the broadest sense, the TF for a federation is composed of the participants, their interactions and infrastructure, and the governance structure that binds the federation together to ensure it operates according to its mission or purpose, and a common set of minimum requirements as illustrated in Figure 2.

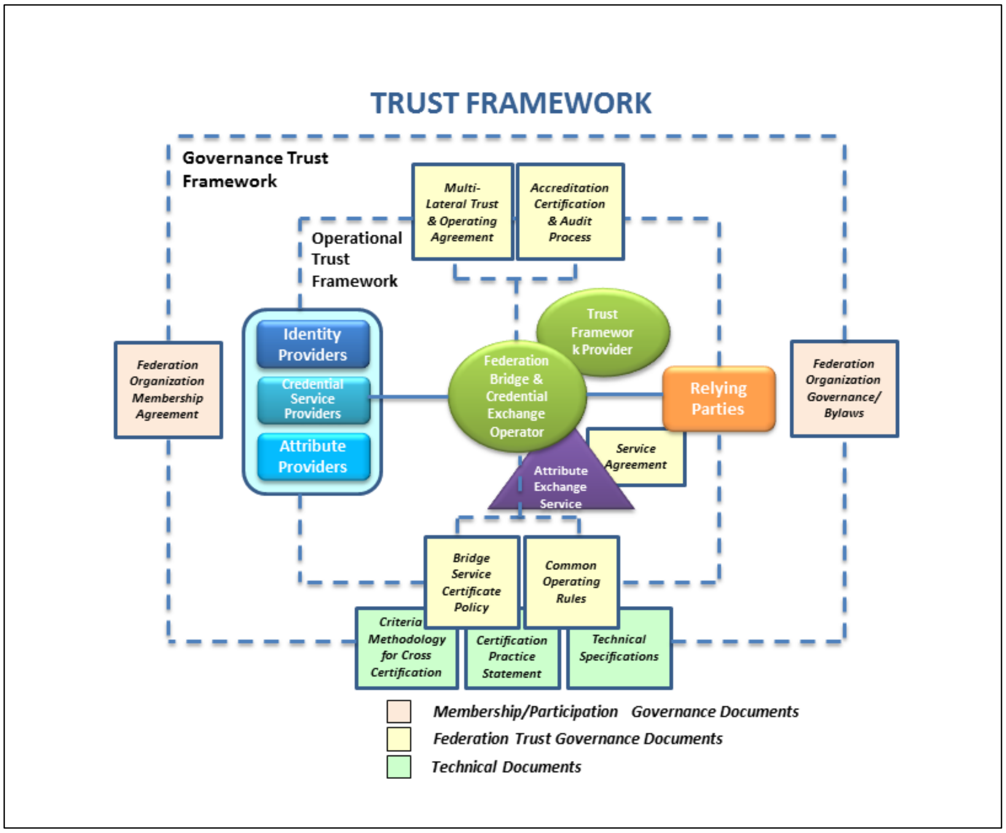
TRUST FRAMEWORK
Governance Trust Framework
Operational Trust Framework
Multi-Lateral Trust & Operating Agreement
Accreditation Certification & Audit Process
Trust Framewor k Provider
Federation Organization Membership Agreement
Identity Providers
Credential Service Providers
Attribute Providers
Federation Bridge & Credential Exchange Operator
Relying Parties
Federation Organization Governance/ Bylaws
Service Agreement
Attribute Exchange Service
Bridge Service Certificate Policy
Common Operating Rules
Criteria Methodology for Cross Certification
Certification Practice Statement
Technical Specifications
Membership/Participation Governance Documents
Federation Trust Governance Documents
Technical Documents

Figure 2: The Federation Trust Framework

The participants in the TF are the Federation Operator/TFP, Identity Providers (IdPs), Credential Service Providers (CSPs), Attribute Providers (APs) and Relying Parties (RPs). (See Section 2.4 for descriptions of these participants and their roles and responsibilities.) The participants are bound to their roles and responsibilities first by the organizational governance component of the trust framework illustrated in the graphic and described in Section 2.4.3, and second, by the operational components of the trust framework, which consists of several operational governance documents described in Section 2.7.

For situations where attributes are used, a Federation Operator can stand up its own attribute exchange service or it may contract with an attribute exchange service (or use some combination of both) to support its exchange and authentication for LOA2/3 (non-PKI) credentials.

2.2 Incorporating NSTIC Principles into the Trust Framework

NSTIC envisions the Identity Ecosystem as one where individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation. In order to realize the vision, the NSTIC Strategy calls out four Guiding Principles to which the Identity Ecosystem should adhere. The principles specify that identity solutions will be:

1. privacy-enhancing and voluntary
2. secure and resilient
3. interoperable
4. cost-effective and easy to use

Each principle has implications for the trust framework. In other words, each principle can be translated into a list of Trust Framework policies and requirements. These polices and requirements are then implemented by entities operating under the Trust Framework in the federation's system design, technologies, operations, processes and/or governance with related implications for the system participants. In order to enforce the principles and related policies, requirements must be incorporated into the federation governance documents to impose compliance. The table below lays out these requirements according to categories related to a federation's credential issuance acceptance process, solution and system design, operations and business policies and references the governance documents that are likely to be impacted.

For existing federations, particularly those that align with FICAM for LOA3 (non-PKI) and LOA4, many of the requirements are already incorporated into their TFs. In the table below, these requirements are italicized.

Table 1:
NSTIC PRINCIPLES INCORPORATED INTO TRUST FRAMEWORK

CATEGORY	REQUIREMENT	NSTIC PRINCIPLE	IMPACTED FRAMEWORK/ GOVERNANCE DOCUMENTS
Credential Issuance/ Acceptance	**Issue/accept credentials that are:** • *resistant to theft, tampering, counterfeiting, and exploitation* • *recoverable from loss, compromise, theft and can be effectively revoked or suspended* • *issued based on sound criteria for verifying individuals and devices* • *capable of being utilized by multiple service providers*	Secure & Resilient Secure & Resilient Secure & Resilient Secure & Resilient	• Common Operating Rules • Certificate Policy • Certification Practice Statement • Accreditation,

Table 1:
NSTIC PRINCIPLES INCORPORATED INTO TRUST FRAMEWORK

CATEGORY	REQUIREMENT	NSTIC PRINCIPLE	IMPACTED FRAMEWORK/ GOVERNANCE DOCUMENTS
			Certification & Audit Process
Solution & System Design	**Implement identity solutions that:**		- Common Operating Rules - Multi-Lateral Trust & Operating Agreement - Certification Practice Statement - Criteria & Methodology for Cross-Certification - Technical Specifications - Accreditation, Certification & Audit Process
	- *apply principles of confidentiality, integrity and availability*	Secure & Resilient	
	- *allow for identity portability*	Interoperability	
	- *apply data usage restrictions selected by user to all parties in the system (if available)*	Privacy-Enhancing	
	- *utilize technologies that exchange data using well-defined and testable interface standards*	Interoperable	
	- enable a variety of transactions (anonymous, pseudonymous, and uniquely identified)	Privacy-Enhancing	
	- are modular, simple to use, intuitive, and require minimal user training	Interoperable, Cost-Effective, Easy to Use	
	- build in security that is transparent to the user	Secure & Resilient	
	- detect compromise and promptly restore, revoke and recover compromised identities	Secure & Resilient	
	Use privacy-enhancing technology and systems that:		
	- *eliminate superfluous "leakage" of information that can be invisibly collected by third parties*	Privacy-Enhancing	
	- *minimize ability to link credential use among multiple service providers*	Privacy-Enhancing	
	- *provide mechanisms to allow individuals to access, correct, and delete personal information*	Privacy-Enhancing	
	- *at individual's request, protect, transfer and securely destroy information when terminating business operations or overall participation*	Privacy-Enhancing	
	- request individuals' credentials only when necessary for transaction and appropriate to risk	Privacy-Enhancing	
	- limit data collection (including individuals')and transmission to minimum necessary for transaction's purpose and legal requirements	Privacy-Enhancing	
	- limit retention of data to time necessary for providing end-user services for which data was collected, except as otherwise required by law	Privacy-Enhancing	
Operations	**Operate federated system that:**		- Common Operating Rules - Multi-Lateral Trust & Operating Agreement - Certification Practice Statement - Criteria & Methodology for Cross-Certification - Technical Specifications - Accreditation, Certification & Audit Process
	- *employs auditable security processes*	Secure & Resilient	
	- accepts external users authenticated by third parties	Interoperable	
	- operates in a manner that allows individuals to easily switch service providers	Interoperable, Resilient, Easy to Use	
	- utilizes open and collaboratively developed security standards for exchange of identity data	Secure & Resilient, Interoperable	
	- maintain availability of identity system and federation by meeting service-level requirements	Cost-Effective, Easy to Use	
	- minimizes data aggregation and linkages across transactions	Privacy Enhancing	
	- maintains forensic capabilities to maximize recovery efforts, enable enhancements to protect against evolving threats, and permit attribution, when appropriate	Secure & Resilient	
	- establishes accuracy standards for data used in identity assurance solutions	Privacy-Enhancing	
	- provides accountability for use of information and mechanisms for compliance, audit, and verification	Privacy-Enhancing	

Table 1:
NSTIC PRINCIPLES INCORPORATED INTO TRUST FRAMEWORK

CATEGORY	REQUIREMENT	NSTIC PRINCIPLE	IMPACTED FRAMEWORK/ GOVERNANCE DOCUMENTS
Business Policies	**Establish business policies and processes that:** • *are common across the federation (e.g., liability, identity proofing, and vetting)*	Interoperable	• Common Operating Rules • Multi-Lateral Trust & Operating Agreement • Certification Practice Statement
	• allow for voluntary participation	Privacy-Enhancing	
	• provide effective redress mechanisms and advocacy for users who believe their data have been misused	Privacy-Enhancing	
	• provide timely and easy-to-understand notice to users on how personal information is collected, used, disseminated, and maintained	Privacy-Enhancing	

Trust Framework Providers and federations typically establish and adhere to requirements that meet the needs of their communities of interest and to comply with applicable laws. As such, these requirements are incorporated into their TFs and governance documents. For example, contractors and organizations that interoperate with the Federal government agencies comply with FICAM requirements; those who interoperate with DoD establish a bilateral trust to comply with the DoD PKI requirements.

The NSTIC PMO has developed a set of requirements derived from the NSTIC principles. The NSTIC strategy's overall goal is to promote the raising of security standards on the day-to-day transactions that occur over the Internet, particularly those conducted by the general public. The average citizen may or may not have secure credentials that have been issued to them through their employment or organizations with which they conduct business; even if they do, these credentials typically cannot be used to conduct personal business transactions. Thus more commonly, the public uses credentials - user names and passwords - established at each online website with which they conduct business. Raising the standards to uphold the NSTIC principles for average citizen transactions over the Internet will require a period of migration because the derived requirements would need to be adopted by various Trust Framework Providers and implemented through the federations' technical solutions and governance documents.

A number of the NSTIC derived requirements have already been adopted by some communities and federations, particularly those that use credentials at the higher levels of assurance (as indicated in Table 1). Nonetheless, there still remains a substantial list of requirements that are not met. The most significant ones relate to privacy because there is a "deployment gap" between public transactions and organizational transactions. When individuals use the secure credentials (for example: smart badges and one time password devices) issued to them by their employers, they use them to conduct business transactions; in this context, their private data isn't collected or transmitted in the course of a transaction performed as an employee as the employer and the application service provider have a contract limiting the amount of information the application service provider can collect, and how it can be used and shared. On the other hand, online commercial and retail entities still tend to employ usernames and passwords for authentication, but also collect and have access to their customers' personal data. The gap between low security retail transactions and high security business transactions is fairly wide.

Communities and federations that are considering adoption of NSTIC derived requirements will weigh several factors. First, they will consider the nature of the requirement. Some requirements are easy to implement, while others are not. Most requirements lead to increased costs (some more costly than others) associated with transaction processing, operations and issuance. In fact, some organizations may determine that the cost of implementing any given requirement may outweigh the related risk. Unless implementing a requirement will significantly improve their business posture, or is required by law or compliance with their community, a federation will carefully consider and weigh the benefits. Certainly if the IDESG decides to issue a trustmark associated with compliance to the NSTIC principles and requirements, organizations and federations would consider the advantages of NSTIC alignment in making their decision.

Over the 8 months, the TSCP and NSTIC Pilot Collaboration groups will be reviewing and working to evaluate and refine the derived requirements and to assess the feasibility of adoption and implementation. This TFDG will be updated in the next version to reflect the progress made.

2.3 Services under the Trust Framework

A federation organization can offer a variety of services. The breadth of services depends on the number and types of credentials that are authenticated within the community and the requirements of the RPs that are part of the trust framework. Generally, a federation organization offers one or more of the following services, which are covered under the trust framework:

- **Basic Interoperability Service** for trusting the use of federated credentials between organizations, businesses, states and international governments.
- **Extending Interoperability Service to include the Federal Government,** which may include cross–certification to the Federal PKI Bridge or a bi-lateral trust with the DoD PKI system.
- **Extending Interoperability Service to other Trust Frameworks,** which may include cross certification to commercial Trust Framework Providers.
- **PKI Certification Authority and Infrastructure Services** for the issuance and authentication of digital certificates at LOA 3-4.
- **Credential and Attribute Exchange Service** for authentication transactions at non-PKI LOA 2-3 to include attributes.
- **Accreditation and Certification,** a service provided to perform and maintain accreditation and certification of the entity to the Trust Framework.

2.4 Federation/Trust Framework Provider Roles & Responsibilities

A federation (or an association that operates a federation) has the following roles and responsibilities:

- Trust Framework Provider
- Federation Operator
- Organizational Governance
- Technical & Operational Governance

Each role and responsibility is described in the sections that follow.

2.4.1 Trust Framework Provider

A Trust Framework Provider (TFP) is an organization or association that establishes the structure and governance for a given TF; it defines how those who wish to operate under the TF will interoperate with one another and the requirements associated with each component of the framework. Thus, the TFP may define the requirements for: the credential types exchanged or validated, the operational infrastructure, credential issuance and management, operating environment, authentication processing, security and communications requirements, and audit requirements. A TFP does not, however, necessarily operate a federation that performs credential exchange and authentication processing.

2.4.2 Federation Operator

A federation operator provides services to facilitate the exchange and authentication of secure credentials for the benefit of its members or participants. For the purposes of this document, the federation bridge/hub service consists of:

- **PKI Bridge Service.** Bridge service that operates among the TF members and is cross-certified to Federal Bridge and maintains a bi-lateral trust to DoD's PKI system – LOA 3-4 (PKI). Enables members to interoperate with each other and with the Federal government.

- **Credential Exchange Service.** Credential exchange service for member, government and commercial credentials at lower levels of assurance (LOA1-3, non-PKI).

2.4.2.1 Interoperability & Infrastructure Requirements

Operational federations offer a technical solution to allow users, organizations and systems to trust in entities that have been certified by the federation operator (as a TFP). Entities certified against the federation's Common Operating Rules may include, IdPs, RPs, APs and Attribute Exchanges. The TFP must allow public verification of whether or not an entity has been certified, the policies against which it has been certified, as well as whether it remains in good standing with the TFP.

An example of an established technical mechanism for conveying trust exists in the PKI community, where approved PKI providers are cross-certified by PKI bridge servers, allowing for transitive trust across Certificate Authorities. By revocation of cross-certificates and the subsequent publication of the revocation by the bridge via a certificate revocation list, only members and individuals who meet TF requirements continue to be trusted.

For non-Certificate Authority trust, there are a variety of technical methods for establishing trust. Examples of methods for a TFP to convey trust status of an entity include:

- Posting of entity status via digitally signed list on the TFP website;

- Issuance of assertion signing certificates: The TFP can issue specialized PKI certificates used by IdPs that convey the certifications the IdP has obtained;

- Publication of metadata: Metadata can be used to express trust and assurance-related information. The TFP vouches for the integrity of the metadata it makes available to the public. Federation participants trust the TFP to vet the metadata content; and,

- Issuance of verifiable trust marks.

2.4.2.2 Interoperability with the Federal Government

Several TFPs enable interoperability with the Federal government. Interoperability with the Federal government involves one or more of the following:

- **Alignment to FICAM Roadmap.** A federation can align its policies and architecture the Federal government's FICAM Roadmap. The *FICAM Roadmap and Implementation Guidance*[1] establishes a common architecture and implementation guidance for Federal agencies that incorporates strong security practices and a consistent approach to deploying and managing identity assurance, credentialing and access control services and thereby establishing a foundation for interoperability. *PIV Interoperability for Non-Federal Issuers*[2] further provides a set of minimum requirements for non-federally issued identity cards that can be trusted by the Federal government.

- **Cross-Certification to the Federal PKI Bridge.** A federation can issue PIV-I credentials and cross-certify to the Federal Bridge for highly secure transactions (LOA4). The Federal Public Key Infrastructure (FPKI) enables the government to issue and manage digital certificates for its users and business partners for strong authentication and the protection of data. The Federal Bridge Certificate Authority interoperates with and creates trust paths between many other PKIs (DoD, states, universities, countries) to enable the users to conduct secure transactions between and across these communities. For Federal government users, the common identity credential is the Personal Identity Verification (PIV) credential, which contains the user's digital certificates. PIV cards can only be issued to U.S. Federal government users. Other government and nongovernment organizations and commercial entities who wish to interoperate with the U.S. Federal government using the PKI may issue PIV-Interoperable credentials, which meet the PIV technical specifications for interoperability with PIV infrastructure elements and are issued in a manner that can be trusted by the U.S. Federal government. The Federal Bridge Authority cross-certifies with the full spectrum of entities to facilitate trust.

- **FICAM Trust Framework Provider (TFP) Application Process.** A federation can become an approved TFP under FICAM for credentials at one or more LOAs thereby enabling its members to interoperate amongst themselves and with the U.S. Federal government at various credential

[11] *Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance*, Version 2.0, Federal Chief Information Officers Council, December 2, 2011.

[2] *PIV Interoperability for Non-Federal Issuers,* Federal Chief Information Officers Council, May 2009.

levels. The application and approval process requires an applicant to demonstrate organizational maturity and a mapping of its security and privacy guidelines to U.S. Federal government requirements.

- **Bi-Lateral Trust to the DoD PKI System.** The DoD has a one-way trust relationship with the Federal Bridge, allowing others to trust its certificates but not trusting certificates issued by others without additional testing and agreements. A federation can establish a bi-lateral trust to the DoD PKI system, which allows members to interoperate with DoD programs, as permitted. Note that under the Federal Bridge CP, RPs are never required to trust any other entity even though the CP sets requirements for the cross-certified members that facilitate trust.

2.4.3 Organizational Governance

A federation may organize itself as an informal or legal partnership, alliance or association depending on its mission. Thus, an organization's mission may solely be to operate a federation or may have a broader mission that includes the operation of a federation. In either case, its governance structure and documents lay out:

- How the organization and federation and its members will operate;
- How decisions will be made;
- Who in the organization will perform what duties/responsibilities; and
- How the members will be bound to the federation and its rules.

The sections that follow will describe key governance bodies and membership and participation requirements and processes.

2.4.3.1 Governance Bodies

There is no one way in which a federation must be organized; however, typically there is an executive body, a management body and various committees and subcommittees, and even working groups. Examples of key governance bodies include:

Executive/Governance Board. The Federation's Executive or Governance Board is responsible for establishing and ensuring adherence to its broad policies and goals. It approves or recommends actions or proposals brought by the members and is accountable to the members for the organization's performance, including the operation of the federation, and determines the broad requirements for membership in the organization. As such, it has the authority to adopt, amend or repeal Bylaws. It also is responsible for ensuring the availability of adequate financial resources and approves the annual budget.

Policy Management Authority (PMA). The PMA is a governance body composed of Federation members, which establishes and approves policies and standards related to its Certificate Authority and the PKI systems and manages the environment in which members can trust each other's PKI credentials. The PMA determines that the appropriate levels of assurance are satisfied by the policies supported in the PKI domain and that the PKI domain fulfills its responsibilities under these policies. The PMA also enforces digital certificate standards for trusted identity authentication across and between members/participants.

Non-PKI Policy Management Authority/Committee. Historically, this governance body manages the policies and decisions related to the federation's non-PKI system. As organizations and federations start to migrate towards the common usage of non-PKI credentials, there must be a management body that manages policies and makes decisions around this component of the framework. This body will determine the roles and responsibilities of the participants and types of transactions the association will support and that sufficient trust is embodied in the Common Operating Rules and required associated agreements.

As a federation migrates towards increased usage of non-PKI credentials, an option for streamlining the governance structure may be to maintain a single PMA that governs both PKI and non-PKI, which might be designed to include two separate subcommittees, one dedicated to the management of PKI and one dedicated to the management of non-PKI.

2.4.3.2 Member Approval Process

For an organization whose sole purpose is to operate a federation, there may not be a membership approval process separate from the federation agreement. A federation that operates within a membership organization, however, typically requires that a potential member undergo a membership approval process. Specifically, the candidate completes an application that binds the member to the organization's bylaws and governance structure and the payment of dues. The candidate chooses the category of membership and the specific requirements associated with the category of membership.

For an association whose mission extends beyond participation in a federation, approved members opt whether or not to participate in the bridge/credential hub exchange services.

2.4.3.3 Participation & Federation Agreements

Members who chose to participate in the association's federation services sign and execute a multi-lateral federation services agreement which lays out the requirements of the various parties, i.e., the federation operator, IdPs, CSPs, APs and RPs. This agreement establishes the roles and responsibilities of the member within the role they apply for, e.g., requirements for integration, credentials and attributes, authentication processing, and access control. Although certainly separate agreements can be established for each category of participant, a multi-lateral agreement streamlines the process and enables each participant to easily see how the other participants are required to perform within the federation. As part of the agreement, all relevant governance documents are incorporated by reference; these documents further define how members must perform in accordance with their trust framework roles. (See section 2.7.)

Note that for federations who associate for the sole purpose of participating in a federated system, a set of operating guidelines (in addition to a participation or operating agreement) might be sufficient.

2.4.3.4 Accreditation, Certification & Audit Process

A federation can develop its own TF or chose to adopt the TF of an established organization. In the event a federation chooses to adopt an existing TF, it will be required to comply with the accreditation, certification and audit processes established by the TF organization. Accreditation, Certification & Audit Services enable federation members to validate that their governance and system/infrastructure components adhere to federation requirements either through self-assertion or a formal third-party audit process.

The Federation accreditation, certification and audit processes associated with the TF laid out in this document will be completed and available in TFDG v.3.

TSCP has an existing audit process associated with its governance around PKI; however, it must be expanded to include the other credential and transaction types. Recently, TSCP developed the audit requirements for compliance with the FICAM TFPAP process.

In addition, TSCP is working with the NSTIC PMO and GSA to determine how the NSTIC privacy and security requirements will be codified into requirements. As a starting point, the FIPPS and FISMA privacy requirements were mapped against the FICAM TFPAP. The results of that mapping formed the basis for recommendations for changes to the FBCA CP and supporting documents.

The completed Federation Accreditation, Certification & Audit Process will enable members to certify to and achieve accreditation by the federation and undergo periodic audits. The process will include PKI, non-PKI (attribute exchange) and NSTIC privacy/security requirements.

2.4.4 Technical & Operational Governance

A federation's operations are based on interoperability through a set of policies, standards, and technical requirements that are embodied in the operational governance documents. The primary technical and operational governance documents are the: Certificate Policy, Certification Practice Statement and Common Operating Rules (see Section 2.7). In addition, a federation operator issues technical specifications related to its specific applications as part of its services to its members.

2.4.4.1 Interoperability & Interfaces

A federation operator supports technologies that enable credential, identity, and attribute re-use. Technologies selected should be open standards supported by multiple vendor COTS offerings. It should actively follow relevant technology trends and standards, and incorporate new technology trends into its trust framework policies and specifications. A federation operator also monitors relevant government laws, policies, and guidance for new requirements that may impact its operations and members.

2.4.4.2 Issuance of Specifications

The Federation may issue specifications that address specific use cases related to its community/communities of interest. These specifications should constrain or extend existing standards to enable interoperability between entities; they define standards to be followed and specifications for interfaces and formats for credentials and interoperable authentication transactions as expressed in the Common Operating Rules. The Federation should publish such specification for use by its members and may make specifications publicly available. An example of such a specification may be an attribute profile for authorization policies unique to a particular industry. Such a specification may outline technical formatting details under existing standards as well as usage and policy controls.

2.5 Member/Participant Roles & Responsibilities

The sections that follow describe the roles and responsibilities of the IdPs, CSPs, APs, Attribute Exchange Service Providers and RPs. There three main governance documents that include requirements and responsibilities for all participants are:

Multi-Lateral Agreement. For all parties, this agreement establishes the relationships of the parties as well as requirements and responsibilities for personnel, configuration, technical operations, access policy management, audit requirements, privacy and security requirements, risk and liability limits and arbitration. (See Section 2.7.2.1 for additional details.) Multi-lateral Agreements invoke the requirements of the relevant Common Operating Rules and CP, as applicable.

Common Operating Rules. All parties must comply with the Federation's Common Operating Rules. They include requirements for general administration, facility management and operational controls, procedure and personnel controls, audit logging procedures, compromise and disaster recovery, termination, records, transfer and archival controls, privacy controls and reporting requirements. Requirements and responsibilities specific to participant roles are described in the sections below.

Certificate Policy. For participants that use the PKI system for authentication, the Federation's Certificate Policy lays out requirements for the Federation Operator and Credential Service Providers. (See Section 2.7.2.2 for additional details.)

For a cross-walk between TF elements and governance documents, see Table 2.

2.5.1 Identity Service Providers & Credential Service Providers

Within a federated network, the IdP is responsible for creating, maintaining, and managing identity information for its users and authenticating the identity during a credential authentication transaction. For very strong credentials, they are responsible for the vetting of credential holders. The Common Operating Rules specify requirements for authentication process controls and assertion controls.

A CSP is responsible for issuing digital identities to users and performing identity-proofing and vetting that may be required to ensure a valid binding of the credential to the user. The Common Operating Rules and CP specify requirements for credential and certificate issuance (PKI and non-PKI), registration and issuance controls, credential management and requirements controls and reporting.

Note that the IdP and CSP may or may not be part of the same organizations, however the functions are distinct. The IdP is responsible for ensuring that the CSP meets all of the requirements required for conducting transactions in the federation.

See section 2.8.1.2 for further discussion related to IdPs/CSPs and federation.

2.5.2 Attribute Providers

An Attribute Provider (AP) is an entity that is responsible for storing authoritative data related to its users and providing access or validation of the attributes during an authentication transaction. It is responsible for all the processes associated with establishing and maintaining a subject's identity and authorization attributes and providing assertions of the attributes to RPs within the federated network.

For example, in some federated systems, an IdP is asked to provide information beyond the credential in the form of identity attributes. These attributes might include a unique identifier or other information such as organizational affiliation, status, email address, etc. Identity attribute values are based on information maintained in the identity management system of an IdP or in a database of a dedicated AP. The IdP or AP sets policies about which attributes and values are sent to which Service Providers. The Common Operating Rules specify requirements for authentication process controls and assertion controls.

2.5.3 Attribute Exchange Service Providers

An Attribute Exchange Network is an online gateway for Relying Parties to access user-asserted, permissioned, and verified online identity and authorization attributes from third-party Attribute Providers or Identity Providers. Relying Parties are able to verify additional user identity and authorization attribute claims such as name, street address, phone number, age, organization affiliation to satisfy varying security requirements and reduce risk.

2.5.4 Relying Parties

The Relying Party (RP) is an individual, government, company or other organization, and sometimes a device, that through an application or website uses an IdP and/or AP to authenticate a user who wants to log into its site; it accepts an assertion as a method authentication of a user. The RP is responsible for deciding what sort of identity credential, attribute or combination of credential and attributes is adequate for the RP to grant access to the application or website. The RP is responsible for deciding whether or how to check the validity of the asserted identity and attributes. Once an RP decides to accept the asserted identity and attributes, it is the RP's responsibility to keep an adequate record of any transaction to support its business or personal needs.

The COR specifies requirements for administration, system and operations and processing for the RP. Administration requirements include Relying Party federation services identification, credential reliance and level of assurance. The system and operations requirements include session lifecycle requirements, claim and token profiles, facility, management and operation controls, technical security controls, integration to federation operator and conformance to federation operator design/technical specifications. The processing section includes requirements for identity validation processing and authentication processing.

See section 2.8.2 for further discussion related to RPs and federation.

2.6 Business & Legal Governance Structure

Because of HSPD-12, the development of secure credentials and the exchange of those credentials originated in the government sector. And policies, particularly around strong credentials even on the commercial side, historically have aligned with these government standards. In the same way that the card networks incorporate the requirements of the Electronic Funds Transfer Act (EFTA) and related laws and regulations into their governance frameworks, the identity federations have incorporated the body of government policies related to identity credentials and access management largely because until now these corporate and commercial credentials have largely been used in government programs.

In order to extend the usage of secure credentials (that have already been issued through employment or contract) into the commercial and retail sectors, there are important factors that shape the governance around federation: the policy and legal framework, the liability structure, and the business structure.

2.6.1 Policy and Legal Framework

At the foundation of most TFs lies a set of policies and even laws that define the goals and constraints under which the federation will operate. They are constructed in a way that will enable the federation to uphold the trust and security standards of the community and to interoperate within its community of interest, and in many cases, with relevant government entities and even other communities of interest. For example, numerous government policies (e.g., HSPD-12 and Federal Bridge Certificate Policy) are incorporated into the FICAM framework. Federations that interoperate with the U.S. Federal government by adhering to or aligning with the framework comply with those policies.

In addition to common standards for protecting identity and access control, a community of interest may have specific laws, regulations, and policies for protecting its data, e.g., electronic medical records, high-value financial transactions, transcripts, etc. In order to incorporate the relevant policies, laws and standards into the framework, requirements are derived from the policies and laws and are translated into the governance documents, and where possible, into the architecture and infrastructure of the federated system itself.

Development of TF legal and policy requirements needs to remain flexible to permit a true federation-of-federations. As new business sectors are added to the framework, additional laws, regulations, and policies may be applicable requiring changes in technical implementations and in liability and other legal terms. Establishing a TF requires careful consideration of the laws, regulations and policy that apply and drafting of clear policy that sets the parameters of personal use of credentials.

For the successful extension of business-issued credentials into the commercial/retail space, two additional issues need to be addressed – permissible use and privacy.

2.6.1.1 Permissible Use Policies

Identity credentials that are issued by a federation's members (governments, companies, or organizations) to their employees to support their business transactions may be subject to use restrictions. Employees normally sign subscriber agreements that may impose restrictions on their use of the identity credentials for certain types of transactions, including personal transactions. In the absence of any restrictions in subscriber agreements, restrictions may be imposed by policy.

Employer-imposed use restrictions may prohibit all personal use of the identity credentials, some personal uses of the credentials, or may restrict use on a completely unrelated basis. For example, an employer may allow employees to use identity credentials to take advantage of discounts provided based on affiliation or for company-provided health benefit plans, but not allow use of those credentials to do personal banking transactions. Or the use restriction may relate solely to proper use of the credential in a transaction, such as restrictions that prohibit use of credentials for illegal transactions. In cases where employers do not impose any restrictions on employee use of identity credentials, the credentials can be used freely to engage in personal transactions.

2.6.1.2 Privacy Policies

A significant issue in the consumer environment, particularly when extending the usage of business credentials into the consumer space, is privacy. Another issue is related to differences in privacy laws and expectations for use of business identity credentials for personal transactions. Privacy is a key consideration under the NSTIC principles.

While a federation's or member company's policies and governing documents may be adequate to address authentication and privacy needs in an employee-employer environment, they may not necessarily be well-suited to address additional user privacy concerns when credentials are used for personal transactions. In the traditional employer-employee environment, there are a myriad of reasons and legitimate needs to collect, use, and maintain Personally Identifiable Information. There are also important business reasons to track employee emails and Internet transactions.

The tension between privacy expectations and employer requirements, legal and policy-based, may cause employers to think twice before allowing the use of credentials for personal transactions and employees to think twice before using employer issued credentials in a personal transaction. There are ways to mitigate risks. For example, in order to encourage use of PKI certificates in personal transactions, additional privacy policy is needed in a federation's CP and its cross-certified CPs. Additional privacy policy may also need to be implemented in Certificate Practice Statements. See Appendix I for a White Paper on Privacy.

2.6.2 Liability Structure

A federation's liability framework normally revolves around its member organizations and liabilities imposed by external policies such as PIV-I liability policies and the requirements of the Federal Bridge. Overall, the perspective is that the proofing, vetting, and credential issuance and checking behind PIV and CAC credentials are much more secure than user pins and passwords – which are still largely in use for most applications. Thus, in B2B transactions, the expectation is that RPs should be willing to accept them without imposing unbounded liability on the IdPs. In fact, the liability model for reliance on PKI certificates is well-understood in the industry and has been in CPs since their inception. A similar model can be expanded for other credential and attribute providers at other levels of assurance. In fact, such a model is proposed in the Multilateral Agreement in Appendix B.

Within a federation, when using a PIV-I or similar company credentials for conducting business, liabilities are assigned and allocated in the event a member fails to operate in compliance with the federation's CP, COR and agreements and damages result. Allocation can be adjusted depending on the type of transaction, the business model used, and nature of the relying party.

However, when an individual uses a credential for personal business, the B2B model does not necessarily work. If an employer issues a credential to an employee who decides to use that credential to do his or her personal banking, the employer has not necessarily contemplated the use of the credential for this personal purpose. Unless the employer agrees to the transaction with the RP and receives some fee or pay for providing the service, the employer is not likely to be willing to accept liability for reliance on the credential.

In this regard, an analogy can be drawn between PIV and CAC credentials, and drivers' licenses as identity verification documents for personal transactions. States have never asserted that drivers' licenses could be used for verification of identity in personal transactions, but over time, these licenses have become the identity standard for a myriad of transactions, including opening a bank account, proving identity in real estate transactions, applying for loans, and more. While there is an analogy, it may not be wise to carry it too far. Historically, the reliance on drivers' licenses occurred without any backend checking of the license, although technology is changing that paradigm. Identity credentials are designed to require verification prior to reliance. The identity space begs for a complete liability model for both government-issued credentials and company-issued credentials that addresses both B2B use and personal use of credentials.

A key part of the TSCP-NSTIC is working to extend the use of LOA-4 credentials into commercial/retail applications and enabling the use of LOA 2 -4 credentials. As part of the pilot work, the TSCP-NSTIC team is working with the members and pilot participants to develop a liability allocation model for adding Financial Institutions to the PIV-I framework, liability allocation for attribute exchange, and liability for using business credentials for personal use. This liability allocation will be incorporated in the TSCP CP, COR, reference Bilateral and Multi-lateral Online Federated Identity Framework Agreements, and the membership agreements as required.

2.6.3 Business Structure

For federations that exist today, which are largely closed/intra-federations, members often act in the roles of both IdPs and RPs. In the role of IdPs/CSPs, they typically cover their own credential issuance and management costs. When acting as RPs, they cover their enablement costs. The federation operator, through membership dues and fees, assumes the costs of operating the bridge/hub service. The extension of the usage of business credentials into commercial/retail applications requires the dissociation of the IdP and credential issuance from RP applications and authentication in that they will be unrelated. Once this intermediary model is established (that dissociates credential issuance from authentication), IdPs and RPs will need to justify the costs of credential exchange by way of a business case. In addition, extending the usage of secure credentials into the commercial/retail sector further dissociates the IdP's business case from the RP's business case. The costs will have to justify the value.

The business model adopted by a federation must reflect value allocation across the community. The business model should be flexible and recognize that decisions about fees, cost allocation and liability, will need to be made based on the facts surrounding the implementation. For example, RPs can claim a benefit or value if they can accept secure credentials in lieu of issuing and managing lower levels of credentials to access their own applications. IdPs/CSPs, on the other hand, may expect to be compensated for the use of their strong credentials in retail applications, particularly if they are expected to accept liability. And bridge services and/or credential exchanges would also expect to be compensated for providing the infrastructure and services that enable the interoperability between the IdPs and RPs.[3]

While the bank card model provides the best available analogy, it falls short on two points when comparing it to identity/credential federation:

- **Financial vs. Identity Transaction.** In a bank card transaction, it is relatively easy to extract pennies from an essentially financial transaction to cover processing and business costs. For a fee associated with an identity authentication transaction, on the other hand, the collection and payment would have to be a separate process.
- **Liability Allocation.** In the bank card transaction process, the consumer rarely directly pays for a bad or fraudulent transaction. Except for interest fees, normally it is the acquirer (RP) who assumes the liability of a bad transaction. It remains to be seen whether a similar liability allocation would work in the identity space.

There could be at least four types of identity/credential issuance uses in the federated environment. The business case for each type should be evaluated along.

- **Business Credentials for Business Use.** Secure credentials issued to employees for official business (e.g., PIV/PIV-I for official business).
- **Business Credentials for Related Applications.** Use of employee credentials for employee related applications (e.g., employee ID/credential to access company 401K or health insurance account).
- **Business Credentials for Personal Use.** Use of employee credentials for commercial/personal use (e.g., company IDs and attributes that employees can use for personal business).
- **Commercial Credentials.** Secure credentials issued through a commercial service (e.g., Verizon credentials).

See section 3 for further discussion on business issues related to federation.

2.7 Key Trust Framework Documents

A federation's TF is memorialized in its trust framework documents; these can be categorized into organizational governance and operational trust documents, which are described in the sections that follow.

2.7.1 Organizational Governance Trust Framework Documents

The organizational governance trust framework documents consist of its bylaws and membership agreement. Although these documents don't directly impact the operations of the federation, they do so indirectly by establishing the overall goals and activities of the organization and the scope of membership.

[3] Note that the federal government cannot accept liability except as provided in the Federal Tort Claims Act and other laws specifically granting authority to accept liability.

2.7.1.1 Bylaws

An organization's bylaws describe the roles and responsibilities of the organization and its members for the governance of the federation. It is the document that establishes membership and participation requirements, how the governance body will be selected and structured, and how decisions will be made for the organization.

Through the bylaws, members bind themselves to the decisions made by the representatives who have been elected to make these decisions. They establish working groups to study issues, vote on fees and dues, select technologies to be used, and decide which applications and solutions will be developed by the federation/organization.

2.7.1.2 Membership Agreement

Each member signs a membership agreement that describes a member's rights and responsibilities and the terms related to confidentiality, termination, warranties and dispute resolution. The agreement also commits the member to paying dues and fees (when applicable) and to comply with the organization's bylaws.

Appendix A provides a reference Membership Agreement.

2.7.2 Operational Trust Framework Documents

The operational trust framework documents for the exchange of PKI credentials consist of the multi-lateral trust and operating agreement, Certificate Policy (CP), Certification Practice Statement (CPS), Criteria & Methodology for Cross-Certification, and any service agreements associated with the operation of the federations. These are described in the sections that follow.

2.7.2.1 Multi-Lateral Trust & Operating Agreement

In a federation, there are multiple parties that agree to interoperate in order to validate, authenticate and accept identities or credentials for the purpose of access to applications and websites. Absent a multi-lateral agreement, each federation participant would be required to execute a bilateral agreement with each participant with whom it wished to conduct business. A multi-lateral agreement is prepared by the federation operator; each IdP/CSP, AP and RP signs and executes this agreement. The multi-lateral agreement includes the requirements, right and responsibilities of each of the participants. Thus, each participant agrees to fulfill its responsibilities while acknowledging the rights and responsibilities of the other participants.

Appendix B provides a reference Multi-Lateral Trust & Operating Agreement.

2.7.2.2 Certificate Policy (CP)

A federation's Certificate Policy (CP) is the set of rules that defines the applicability and use of its PKI certificates within the community, its program applications and common security requirements. It defines the standards, policies, and procedures for processing certificates across the community. The CP is maintained by the federation's Policy Management Authority.

Appendix C provides a reference CP.

Because TSCP's CP aligns to the FBCA CP, in order for TSCP to incorporate the NSTIC guiding principles around privacy and security into its CP and related processes and procedures, additional requirements have been proposed for the FBCA CP. Additionally, as part of the work associated with the Financial Institution pilot, the TSCP-NSTIC Team is determining the additional privacy and security requirements that are necessary for financial-related transactions in the retail sector using PIV/PIV-I/CAC credentials, which will be incorporated into the TSCP CP and other reference documents including the reference CPS.

The resulting TSCP CP will be the model for the issuance and use of strong LOA 4 credentials for commercial/retail applications. The reference CPS is a basis for implementing the CP requirements to establish trusted identity credentials.

2.7.2.3 Certification Practice Statement (CPS)

A federation that operates a PKI Bridge has a Certificate Authority that issues a Certification Practice Statement (CPS), which describes the federation's practice for issuing and managing public key certificates, i.e., issuance, publication, archiving, revocation and renewal practices, in order to maintain the required level of PKI security. By detailing the practices, a CPS assists interested parties in judging the relative reliability of a given certificate authority. A CPS is an expansion of the CP in that it is a detailed technical and procedural document that takes into account the operation of the supporting infrastructure. It describes how the CP is interpreted in the context of the system architecture and operating procedures of its members. A CPS also documents the means by which participants interact with the CA; a CPS is a CA-specific document, whereas a CP may be common across many CAs in the same PKI.

Also, a federation may cross-certify to another federation in order for its members to be able to interoperate with another community. An example is a federation operator that is cross-certified to the Federal Bridge or the DoD PKI system. In either case, the federation's CP would need to maintain compliance to the CPs of the FBCA and/or the DoD PKI system.

Because an organization's CPS describes how it will meet requirements, it is considered confidential. Appendix D provides a template for the development of a CPS.

2.7.2.4 Criteria & Methodology for Cross-Certification

Federations that wish to interoperate with other federations for the exchange of PKI credentials must go through a cross certification process. The process and steps are defined in a Criteria and Methodology document. The document identifies the criteria for eligibility for cross-certification and defines the methodology for implementing and maintaining cross-certification with the federation organization.

Appendix G provides a reference for the development of the Criteria & Methodology.

2.7.2.5 Service Agreement(s)

Service agreements are used to bind third-party providers to the trust framework of the federation.

Table 1:
TRUST FRAMEWORK ELEMENTS & DOCUMENTS

TRUST FRAMEWORK ELEMENTS	ByLaws	Operating Rules	Multi-Lateral Agreement	Membership Agreement	Service Agreement	Certificate Policy	Certification Practice Statement	Criteria & Methods	Technical Specifications	Accreditation, Certification & Audit
ORGANIZATIONAL GOVERNANCE										
Member Requirements/Approval	✓			✓						
Federation Participation Approval			✓							
Governance of the Federation	✓	✓		✓						
Accreditation & Certification Requirements						✓	✓			✓
Cross-Certification to other Bridges								✓		
OPERATIONAL GOVERNANCE										
Scope of Services										
Participating Credential Types										
Federation Operator Responsibilities		✓	✓			✓	✓	✓	✓	
Identity/Credential Provider Responsibilities		✓	✓			✓	✓		✓	
Attribute Provider Responsibilities		✓	✓						✓	
Relying Party Responsibilities		✓	✓							
Attribute Exchange Responsibilities					✓					
Authentication Processing		✓				✓			✓	
Security Requirement/Procedures		✓	✓			✓	✓	✓	✓	
System Performance Metrics		✓								
Member Notification Requirements		✓								
Interoperability/ Infrastructure Responsibilities		✓					✓		✓	
Technical Support		✓							✓	
LEGAL GOVERNANCE STRUCTURE										
Federal Policies										
Permissible Use Policy										
BUSINESS/LIABILITY STRUCTURE										
Identity/Credential Provider Liability										
Relying Party Liability										
Federation Operator Liability										
User Liability										
Fees/Costs			✓	✓						

2.7.2.6 Common Operating Rules

A Federation's Common Operating Rules (COR) define the roles, requirements and responsibilities for participants in an operational federation (including the federation operator). They include the responsibilities of all parties for credential issuance and authentication transactions within the community of interest as well as operational requirements such as identity vetting and proofing, enrollment, issuance, termination, and security controls for each operational process. They also establish mandatory operational policy for Credential Providers and IdPs that, when implemented, enables Relying Parties to have increased confidence in the identity of the user.

The COR provides one document in which participants, prospective participants and other federations can easily ascertain the governance and TF for a federation and how the federation operates and interoperates.

The participation agreement includes a provision that requires the participant to agree to be bound to the existing and future versions of the Operating Rules, thus, while participants will generally have a right to comment or vote in the Operating Rules change process, once a change is approved participants are not required to sign new agreements with each amendment to the Operating Rules.

2.7.2.7 Technical Specifications

A federation operator may define, test, and publish vendor-agnostic specifications for identity and security functions related to the mission of the organization. These specifications enable the members to implement solutions for the operational functions required by the federation, for example, specifications for document sharing and automated data exchange.

Because technical specifications are specific to an organization or federation, there are no related reference documents included in the Appendix.

2.7.2.8 Accreditation, Certification & Audit Process

The initial accreditation process consists of a checklist for certification, accreditation, and audit to FICAM requirements. For federations that choose to cross-certify to the Federal Bridge, for example, a C&A and audit process must be developed to audit against FICAM PKI.

The Federation Accreditation, Certification & Audit Process will be completed for TFDG V.3.

As part of the TFPAP process, TSCP will develop audit requirements for compliance with the FICAM TFPAP. In addition, TSCP will work with the NSTIC PMO and GSA to determine how the NSTIC privacy and security requirements will be codified into requirements. As a starting point, the FIPPS and FISMA privacy requirements were mapped against the FICAM TFPAP. The results of the mapping will form the basis for recommendations for changes to the FBCA CP and supporting documents.

The completed Federation Accreditation, Certification & Audit Process will include PKI, non-PKI (attribute exchange) and NSTIC privacy/security requirements.

3 Business & Legal Issues

The sections that follow present business and legal issues that will need to be resolved in order for a functional and robust Identity Ecosystem to operate using secure credentials for a wide array of commercial Internet transaction types. During the course of the NSTIC pilots, TSCP will work with other pilot participants to discuss and evaluate models acceptable to the commercial sector for incorporation into the TFDG.

3.1.1 Business Value & Liability Flows

A key objective of the NSTIC pilot(s) is to test the use of secure credentials that have been issued to users from business or commercial service providers for commercial and retail transactions. From a technical perspective, these transaction models are relatively easy to implement through a federated model. The issues that need to be resolved are those business issues associated with cost and liability allocation, as well as the imposition of fees. This section will propose the considerations that will be addressed in the pilot(s) in order to obtain resolution on value, risk, and liabilities acceptable for the participants for the purpose of establishing a business model.

3.1.1.1 Business Member IdPs/CSPs

An IdP and/or CSP can issue four categories of credentials, which are described below.

Business Credentials for Business Use. Members of a federation issue credentials to their employees for internal business uses and external business uses related to official business. In their roles as the Identity/Credential Providers, members typically cover the costs associated with identity/credential issuance and management, application enablement and interoperability for federation.

Liability allocation is normally based on risk at each step of the authentication process, which in turn is defined by the business model. The liability allocation model is established in the multi-lateral agreement with the federation operator. The Identity Provider accepts some liability for direct damages related to credential usage provided the Relying Party uses the credential in accordance with the process laid out in the agreement.[4]

Business Credentials for Related Applications. Members of a federation may allow their employees to use company-issued credentials for use with company related transactions, e.g., to access the user's company 401K plan. Often, a link is provided directly from the company's network. The employer/IdP covers the direct costs associated with identity/credential issuance and management and interoperability to covered applications; the cost of enablement on the RP side would be assumed by the RP. In this case, as the Relying Party is receiving the benefit of a more secure credential without paying a fee, the liability notionally rests with RP. Liability would be the subject of an agreement between the employer/IdP and the RP.

[4] Note that per the Federal Tort Claims Act, the U.S. Government never accepts liability except as otherwise provided in statute.

Liability is tied to risk and agreement at each step of the authentication process and would be established in the multi-lateral agreement with the federation operator.

Business Credentials for Personal Use. In this case, the federation member would issue employee identity credentials and allow them to be used for personal transactions, i.e., to access non-company financial or retail applications. The employer/IdP would cover the cost of application enablement and its connection to the federated operator to facilitate B2B transactions. In order to take advantage of the secure employer issued credentials, the RP would cover the costs of application enablement. The secure credential represents a convenience, potential risk mitigator and cost saver for the RP and the RP would be expected to accept liability. In this scenario it is likely that the RP accepts liability for use of credentials unless the RP pays a fee of some sort to obtain validation of the credential. Liability would be established in a multi-lateral agreement with the federation operator.

For business-issued credentials, the questions that need to be answered through the pilots are:

- Would the IdP/CSP agree to cover the costs for validating the credential or would they expect the RP to pay a fee? Is there an additional cost?
- If the IdP/CSP validates credential and accepts risk, what would they expect to be paid?
- Would the RP be willing to pay for this service? Would the RP perceive that the risk of accepting trusted external credentials is worth the savings associated with divesting itself of the cost of issuing and managing less secure credentials?
- What would the federation operator expect to be paid for routing and processing the transaction and accepting the related risk?

3.1.1.2 Commercial IdPs/CSPs

In this case, the federation would allow the use of commercially issued credentials to its members' users to conduct secure commercial/retail transactions over the Internet. The commercial IdP would charge users (or user organizations) for the issuance, management and validation of credentials as well as for connection to the federated operator.

As the commercial IdP earns fees for the issuance and management of the credentials, it would be expected to assume some of the risk and liability for negligent issuance and use of credentials that results in losses associated with transactions based on those credentials. The RP would cover the cost of application enablement and connection to the federated operator and would accept the risk of loss for misuse on the application side, i.e., using credentials without authenticating them or using an inappropriate credential (e.g., a credential not strong enough for the contemplated transaction).

For commercially-issued credentials, the questions that need to be answered through the pilots are:

- What liability, if any, would an IdP be willing to assume?
- How much would the IdP charge the user for the credential?

- Would a user be willing to pay for such a credential? How widely would the credentials be accepted?

- Would the IdP expect the federation operator/RP to pay a validation/processing fee?

3.1.2 Relying Parties

Over the last decade, millions of secure credentials have been issued by business/company and government entities for use in business applications. Many of these companies and government agencies are members of one or more federations to facilitate and extend the usage of their secure credentials in related RP applications. To further extend the usage of these secure credentials into commercial/retail applications (an NSTIC objective) will require significant engagement and participation by a broad range and number of RPs.

In an environment where multiple types and levels of secure credentials will be exchanged and the goal is to catalyze their use across many industries and users, the participation of RPs who are dissociated from IdPs and CSPs through federation must be encouraged and promoted.

For RPs, the questions that need to be answered through the pilots are:

- Would RPs be willing to pay to obtain the benefit of secure credentials?

- Would the RP perceive that the risk of accepting an externally issued credential outweigh the benefit of divesting itself of the cost of issuing and managing less secure (or equally secure) credentials?

3.1.2.1 Need for Definition & Governance

In today's federation market, requirements and specifications and even governance have largely focused on the IdPs and CSPs. As we move into a federated environment that encompasses RPs, APs and Attribute Hubs, their roles, responsibilities, and liabilities within the federation need to be defined. In particular, if there is to be broad adoption, the governance surrounding RP participation needs to be established and accepted by all parties.

3.1.2.2 Extent of Incorporation into the Federation

For RPs, the questions that need to be answered through the pilots are:

- Do RPs need to be "official" participants of the federation by signing and executing member agreements or RP agreements?

- Must RPs be full members of the federation or should there be a "quasi" membership option for RPs?

- To what degree can RPs be assigned responsibilities?

- Should RPs be audited? If so, what should the audit format be (self-audit vs. third-party)?

- What is the right balance between imposing burdens on RPs and encouraging their participation?

3.1.2.3 Motivators & Inhibitors

In order to establish a business model that would stimulate the participation of RPs, the motivators and inhibitors for federation need to be evaluated and incorporated into an effective business model, for example:

- **Applications Requiring Confidentiality.** Would RPs be motivated to accept secure credentials for applications that require confidentiality (e.g., financial, business and health care)?

- **Acceptance/Payment Motivators.** What would motivate RPs to accept, and potentially pay to accept, secure credentials that they don't issue themselves?

  - Enhanced security
  - Decreased risk
  - Customer demand/goodwill
  - Compliance/regulation
  - Desire to divest of the identity/credential management function
  - Cost Savings

- **Federation Inhibitors.** What would inhibit RPs from moving to a federated model? Is there a benefit in maintaining the IdP function themselves (customer relationship, marketing, etc.)?

- **Federation Benefits.** Would RPs be motivated to federate because of the ability to accept multiple secure credentials through a single connection to the federation operator?

3.1.3 Federation Operators

For federation operators, the questions that need to be answered during the pilots are:

- What is the potential risk to the federation operator – what piece of the risk does it assume?

- For what components of the infrastructure is the federation operator responsible?

- What liability is allocated to the federation operator?

- How does the federation operator cover the liability?

- What would the federation operator expect to be paid for routing and processing the transaction and accepting the related risk?

4 Appendices: Trust Framework Documents

4.1 Appendix A: Federation Organization Membership Agreement

4.2 Appendix B: Multi-Lateral Trust & Operating Agreement

4.3 Appendix C: Certificate Policy

4.4 Appendix D: Certification Practice Statement

4.5 Appendix E: Federation Accreditation, Certification & Audit Process

To come in TFDG V.3.

4.6 Appendix F: Service Agreement(s)

TBD

4.7 Appendix G: Reference Criteria & Methodology for Cross-Certification

4.8 Appendix H: Common Operating Rules

4.9 Appendix I: Privacy White Paper