First Line of Defense against Hackers: Secure, Trusted Identity Credentials under a Federation Trust Framework

In the wake of seemingly daily news articles about the theft of personal identity, financial, and proprietary information, many businesses, including those in the financial sector are considering how to approach the problem of securing information in the cyber world. Solving the problem will take a multi-pronged approach, but managing who can gain access to information and having a way to quickly cut off the flow of information when circumstances change is a key element in the solution. Federated trust frameworks have been used successfully to increase security by managing identity vetting and access through a common technical baseline and a set of policy and governance rules.

The Transglobal Secure Collaboration Program (TSCP) is a non-profit 501(C)(6) technical trade association that provides a governance trust framework and identity federation services, which started with the Aerospace and Defense (A&D) community, but now also to other members who seek to issue or accept secure credentials for their applications. TSCP represents hundreds of thousands of end users who conduct business transactions with their employee credentials. TSCP is currently conducting a pilot to test extending the use these secure credentials into the commercial marketplace.

The TSCP Trust Framework has been used successfully to secure and manage access to information. The infrastructure that has resulted from the major A&D community investment can be leveraged to secure and manage information across multiple market sectors. By engaging other service providers with a wide-range of technology solutions, TSCP is expanding its Trust Framework to provide flexibility to its members to effectively manage risk and cost. TSCP maintains trust anchors to, and interoperates with, the Federal government (civilian) and the Department of Defense (DoD) as vital business partners. As a federation whose members value secure access, TSCP is in the process of establishing a trust anchor for the financial services industry to establish standards for security, interoperability and privacy.

This paper describes TSCP’s governance trust framework, its identity federation operations, and the community in which it operates. It also describes the challenges that are addressed for financial institutions by operating under a trust framework and federation and the specific benefits associated with participation.

Background

Over the last 12-18 months, the financial services community has been considering the future of usernames and passwords for access into its commercial and consumer accounts. While most acknowledge that this model will probably never be completely eliminated, the prospect of leveraging third-party credentials, social media credentials and even credentials issued by financial services’ corporate customers is being explored.

Over the last decade, government and various companies have implemented identity and access management (IAM) 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 their communities of interest. More recently, they are starting to set up identity federations in order to facilitate the exchange of credentials across sector communities.

Financial institutions have invested in extensive infrastructures to enable their commercial and consumer customers to access services and applications online. Often, this has been accomplished in a “stovepipe” manner, business line by business line. Financial institutions are looking for ways to leverage their identity-related infrastructures and maintain mandatory identity policies, but also add an innovative layer that modernizes and streamlines the identity management and authentication function. In addition, with the rise of
and publicity associated with cyber incidents, they want to be able to provide secure authentication methods for their customers, but ones that offer choice and are not unduly onerous.

A solution that has gained attention and consideration by financial institutions is identity federation. Identity federation is a method of decentralization that decouples identity and credentials from relying party applications, which can be implemented across unrelated domains, and eliminates the need for passwords (unlike SSO). It enables the use of identity attributes from one (or a few) systems to authenticate into applications through alignment to commonly accepted standards, identities, credentials and interfaces for interoperability.

In communities such as financial institutions that must be able to trust the identities – not only to validate users’ identities, but also their suitability and authorizations for access to applications – they need to operate in a trustworthy environment. In the TSCP identity federation, for example, for high assurance credentials, there are established processes for vetting and proofing users; the successful completion of these processes is “bound” to the identity. While each member company may utilize slightly different methods internally, for the purposes of federating across the community, they have harmonized these processes around a minimum core of standards.

The term “identity federation” can refer both to a solution and an organization. A simple identity federation solution is a matter of mechanics and technology. In this case, a number of entities who need to interoperate can agree to implement an identity federation solution that facilitates technical interoperability among them. An identity federation organization, on the other hand, brings communities together to establish and agree to a trust framework with the development of common standards, processes and governance – governance includes a business model and a structure for sharing and allocating liabilities.

Financial institutions benefit in joining an identity federation such as TSCP by participating in, on the one hand, a community in which members can work out and agree to standards and processes, and on the other hand, a governance structure that ensures that all members comply with the rules and share liability. For example, for highly secure credentials, the A&D community follows vetting and proofing methods established by the Federal government/DoD because they perform transactions for related contracts and programs across the major integrators, the DoD/Federal government and thousands of supply chain companies. Similarly, TSCP financial institutions members could establish and agree on a facsimile process, for example, vetting and proofing for customers using the existing “Know thy Customer” procedures already followed by financial institutions. The purpose and advantage of joining an identity federation is that the federation’s trust framework can be expanded to encompass additional sets of standards to address the requirements of broad communities.

TSCP has invested years and substantial member funds in the development of its trust framework and federation operation and related infrastructure. For companies like financial institutions, it enables them to compete on services, not on credentials; it allows banks to focus on their mission and business. Because of the decoupling and tighter role distinction between the participant groups (identity and credential providers, attribute providers and relying parties), individual participants are able to assume the role or roles that serve its business and offload other functions to other members. For example, financial institutions can participate as relying parties and provide services to their customers and leave the identity management and interoperability of the system to the other TSCP members. The operating rules of the identity federation lay out the roles and responsibilities of the participating groups and identifies the different types of credentials available within the federation; each member can decide what role or roles they wish to play and what credentials and transaction types they are going to use and they only needs comply with the requirements and rules related to them. The graphic below illustrates how financial institutions could leverage TSCP’s trust framework and infrastructure in the exchange of secure credentials.
Today, the majority of trust frameworks 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 credentials. In a move to increase their functionality and offer value and savings to other communities, trust framework providers 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 in order to minimize the number and types of credentials a user will have to procure and maintain. In addition, in an effort 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 of trust (and resulting liability) for federated credentials.

**Analogy to the EFT Trust Framework**

The secure IAM credential market today can be compared to the bank card industry some 45 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 and a common accepted trust framework consisting of terms and conditions, operating rules, and a liability and business model has been accepted by all parties involved in the transaction. The user experience is optimized with one bank card that works pervasively across the various POS retail and financial networks (federated use). Business has a clearly defined financial business model with identifiable risk, all based on the collection of all parties agreeing to the trust framework.

**Governance Trust Frameworks & Identity Federation**

The section that follows will define a governance trust framework; explain the distinction between a trust framework and identity federation; and describe TSCP’s trust framework and identity federation.

**What is a Governance Trust Framework?**

Governance starts with the any law and regulation and adds a set of common policies that establish the requirements for vetting and establishing identities, issuing credentials and making access decisions. Identity federation governance leads to the expectation that interoperating system participants will follow the same processes and procedures when validating identities for enabling access. To enable them to be operationalized, standards, specifications and rules are derived from these policies. Each network or system establishes a trust framework that incorporates these standards and defines the rights, responsibilities and requirements for participants to operate within that system. Individual trust frameworks may have been created for specific purposes – TSCP, for example, was originally established to support the A&D industry.

In order for credentials to be trusted and access enabled between and across various systems, the individual trust frameworks must adopt the processes and procedures of a common trust framework. Finally, checks and balances need to be established in the form of accreditation authorities to validate that participants are abiding by the rules.

As illustrated in this graphic, in the broadest sense, a trust framework is composed of the participants, their interactions, their shared infrastructures and governance structure that binds the federation together to ensure it interoperates according to its mission or purpose through a common set of requirements.

First, the participants are bound to their roles and the components of the trust framework by a governance body, participation agreements and governance documents.

Second, they are bound by the operational components of the trust framework — the federation operator and participants’ infrastructure that connect and authenticate through the implementation of the technical documents and specifications. (For more detail, see below, *TSCP: Trust Framework for Identity Federation.*)
Trust Framework vs Identity Federation

There are several organizations that have established and operate trust frameworks, i.e., trust framework providers (TFPs), for example the Kantara Initiative and the Open Identity Exchange (OIX). As another example, FICAM is the trust framework for the Federal government. 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. Members who want to implement credential exchange establish bilateral agreements using the trust framework as a basis and how they technically interoperate must be worked out between them.

An operational federation such as TSCP goes a step further. It has a trust framework, but also interoperability technical specifications that harmonize Standard Operating Procedures (SOPs) from all its members with an infrastructure that enables the actual exchange of credentials and secure authentication; there is a bridge and/or exchange hub that sits between issuers and relying parties who each integrate using a single interface to the bridge and a single multi-lateral agreement that flows down to all participants.

TSCP: Trust Framework for Identity Federation

A trust framework is composed of several elements that, when all bound together, establish the governance around an identity federation. The principal components of the TSCP trust framework are illustrated in the graphic below.

Each element of the TSCP trust framework is described in the table below.

<table>
<thead>
<tr>
<th>TSCP TRUST FRAMEWORK ELEMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TF Element</strong></td>
</tr>
<tr>
<td>Governance Body</td>
</tr>
<tr>
<td>TF Element</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Members/Participants</td>
</tr>
</tbody>
</table>
| Trust Framework Provider & Federation Operator | As a trust framework provider, TSCP has established the structure and governance for its trust framework; it defines how those who wish to operate under the trust framework will interoperate with one another and the requirements associated with each component of the framework. Thus, TSCP defines 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.  

As a federation operator, TSCP also provides services to facilitate the exchange and authentication of secure credentials for the benefit of its members. Toward that end, TSCP operates a PKI Bridge, Certificate Authority and credential exchange service. It provides an interface to its services system and establishes technical specifications for interoperability. |
| Participation/Membership & Federation Agreements | Members who chose to participate in TSCP’s federation services sign and execute a multi-lateral federation services agreement that lays out the requirements of the various parties, i.e., the federation operator, identity and credential providers, attribute providers and relying parties. 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. 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. |
| Common Operating Rules                        | All parties must comply with the TSCP’s Common Operating Rules and related Standard Operating Procedures. They include the responsibilities specific to TSCP and participant roles, 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. |
| PKI Policies & Methods (PKI Only)             | For participants that use the PKI system for authentication, TSCP’s Certificate Policy lays out requirements for TSCP as the federation operator and its members who are PKI credential service providers. TSCP’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 TSCP’s Policy Management Authority. TSCP also publishes its 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.  

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 TSCP’s Criteria and Methodology document, which identifies the criteria for eligibility for cross-certification and defines the methodology for implementing and maintaining cross-certification with TSCP. |
| Infrastructure & Technical Specifications     | Operational federations such as TSCP offer a technical solution to allow users, organizations and systems to trust in entities that have been certified by the federation operator; participants certified against the TSCP’s Common Operating Rules. TSCP also issues technical specifications that enable its members to interface to the federation services and to address specific use cases related to its community/communities of interest. A federation may also establish an Approved Products List, which identified technology solutions that easily integrate to the |
TSCP TRUST FRAMEWORK ELEMENTS

<table>
<thead>
<tr>
<th>TF Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Trust Anchors: Business &amp; Legal Framework</td>
<td>At the foundation of trust frameworks such as TSCP’s 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, partners and 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 such as TSCP interoperate with the U.S. Federal government by adhering to or aligning with the framework comply with those policies. Thus, TSCP has established “trust anchors” to the Federal government (civilian) and DoD. TSCP is also in the process of establishing a trust anchor to the financial services community. These “trust anchors” are important for improving interoperability and providing legal grounding for liability risk.</td>
</tr>
<tr>
<td>Accreditation, Certification &amp; Audit Process</td>
<td>TSCP’s members must periodically demonstrate that they comply with the governance and technical requirements established by TSCP. TSCP’s Accreditation, Certification &amp; Audit process enables TSCP’s 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.</td>
</tr>
<tr>
<td>Approved Product List (Future)</td>
<td>TSCP is developing an Approved Product List (APL), which will be a register of technology products and services that have been tested for efficient integration into the TSCP infrastructure.</td>
</tr>
</tbody>
</table>

Challenges Addressed by Federation

In an IAM environment where organizations and companies more and more need to facilitate secure access across domains, they are looking to identity federation to address the challenges related to security and interoperability. Although the last two sections of this paper will describe specific business benefits related to identity federation, this section lays out the major structural challenges that are addressed through identity federation under a trust framework.

Efficient Interoperability

Identity federation offers the most efficient configuration for interoperability. This is best illustrated by describing the difference between the non-federation model and the federation model.

**Non-Federation.** In a non-federation model, each entity has to establish agreements and interfaces with each entity with which it does business. Entities often act as both credential issuers and relying parties and typically issue and manage credentials for access to their applications. They also have to manage each new external secure credential they are planning to accept. Users are typically issued credentials for each entity where they do business and often these credentials are not secure.

**Federation.** In a federated model, each entity signs one agreement and establishes a single interface to a federation operator. Entities can act as identity providers only or relying parties only with ability to accept
strong credentials. Relying parties only need manage authentication and access to their applications. Through federation, relying parties are able to accept one (or more) strong credentials and lower level credentials for applications not requiring highly secure authentication. Also, users can have one or few secure credentials, and therefore, they may reduce the number of credentials needed for online transactions.

Facilitated Interoperability with Other Communities/Industries

In the future, the expectation is that these community federations will want to authenticate between and across communities - inter-federation – in order to minimize the number and types of credentials a user will have to have.

An inter-federation trust framework would be composed of various trust frameworks that agree to align through multi-lateral agreements, in essence, a federation of federations.

Again, an analogy can be made to bank card services. So for example, while Visa, MasterCard and Amex all have their own policies and standards, they are able to interoperate across the same infrastructure because they share common policies and standards as well as that infrastructure. Ultimately, this sort of framework of frameworks will have to exist for identity if users/citizens are to be able to transparently use their credentials at any internet access point.

Role Efficiency & Contraction

Financial institutions don’t compete on the credential or how it is authenticated, but rather on the services and applications they offer their customers. In a non-federated environment, entities are often required to perform multiple roles in order to conduct business. This may include issuing and managing credential and enabling partners to access their networks. In a federated environment, entities are able to select the role that best meets their business needs and leave the other functions to other members of the federation.

Standardization & Consistency

Participating in identity federation with a trust framework provides the standardization and consistency to facilitate the efficient exchange of credentials. Participants align to common credential issuance and authentication standards and processes that enable all members within and even across communities to securely access accounts and data (as authorized by the participants).

In addition, options are available within the framework. For example, the TSCP uses several credential types for varying levels of assurance depending on the sensitivity of the transaction. A member can choose to use whatever number of credential types that suits its purpose. Also, because of the credential options offered by the federation operator, a participant can opt to participate as a relying party only and leverage the credentials issued by other members.

Another area of consistency lies in the governance of the federation. Instead of having to establish bi-lateral agreements and technical specifications with each entity with which a member does business, the member executes one multi-lateral agreement and implements one set of technical interoperability specifications with the federation operator.
Benefits of Identity Federation under a Trust Framework

For entities that require secure collaboration or seek to have a diverse set of users access data they want to protect, identity federation represents several benefits, which include:

- **Reduced Risk.** As a result of roles distinction, the Identity Provider is responsible only for the user’s identity data and to validate for authentication; Relying Parties no longer need to establish and manage identities and be at risk for handling a user’s privacy data. The risk is clearly defined and limited to the roles associated with each party.

- **Increased Speed to Market.** When operating through an intermediary model, each party needs only to integrate to the federation operator as opposed to each party in the association. This enables all parties to more quickly bring services and applications to market and enables users to access a broader set of services and applications.

- **Assured Identities for Relying Parties.** Relying Parties are able to rely on the validity of the credentials they accept, that they are current, and that they are associated with identities that have had some degree of vetting and proofing.

- **Preemptive Security Solution.** Because of the ability to validate identities and credentials, a federation model represents a preemptive solution to secure access (letting legitimate people in) as opposed to a reactive one (keeping the wrong people out).

- **Privacy Protection.** Only identity data required for authentication is passed to the Relying Party. Users no longer need to divulge extraneous data at multiple Relying Party sites, which preserves the integrity and confidentiality of the user’s personal information.

- **Enhanced User Experience.** The user needs to maintain fewer accounts and passwords while being allowed to access multiple resources and have their personal data protected.

- **Reduced Operational Costs.** Although the migration to federation involves up-front costs, in the longer term, it provides reduced account overhead through simplified password management, better provisioning and de-provisioning and less integration work associated with each Relying Party application and multiple Identity Providers as a result of standard interfaces.

- **Efficiency in Governance.** Federation participants are able to execute a single multi-lateral agreement with the federation operator as opposed to bi-lateral agreements with multiple Identity Providers or Relying Parties.

- **Single Point of Integration & Policy Enforcement.** In a federation model, all participants integrate to the federation operator using common standards, which also provides a single point for governance and policy enforcement.
Specific Benefits of TSCP to Financial Institutions

TSCP is in the process of developing a trust anchor to the financial services community and is looking for a few major financial institutions to assist in establishing IAM federation standards. The benefits of participation are:

- **Participation in Broad Industry Movement.** As a key player in the financial services industry – an industry with a keen and current interest in secure identity credential and access management for its commercial and retail customers – Financial Institutions can join other stakeholders that have successfully addressed this market for years, namely, the Aerospace & Defense (A&D) industry.

- **Leadership Role in Identity Protection.** Financial Institutions has the opportunity to establish a leadership role in an industry effort to establish financial institution requirements for incorporation into the TSCP Federation Trust Framework. Under the TSCP Federation, Financial Institutions could collaborate with another major financial institution to establish the de facto standard requirements for the financial services industry.

- **Leveraging Standardized Approach.** To service and attract customers, financial institutions look to securing and simplifying access to their commercial and retail applications; the issuance and management of credentials, however, represents a cost with no significant benefits. The TSCP community has been considering how to leverage the progress in IAM standardized models in order to offload duplicative functions and streamline operations. Financial Institutions can leverage a strong model derived from DoD and the A&D community through the TSCP Trust Framework and Federation.

- **Leveraging Work of TSCP Members.** TSCP works with various industry stakeholders to ensure that important requirements are incorporated into its framework, e.g., privacy requirements for consumer transactions, development of credential levels (low, medium, high) to accommodate various transaction types, etc. Financial Institutions can leverage years of work towards standardized credentials and interoperable access management already performed by TSCP members.

- **Power of One Voice.** TSCP is comprised of many major stakeholders as well as thousands of supply chain companies representing hundreds of thousands of end users. This considerable base of stakeholders commands strong influence in the marketplace both in terms of establishing de facto standards and influencing technology product roadmaps.

---

**BENEFITS OF IDENTITY FEDERATION TO FINANCIAL INSTITUTIONS**

- More and more entities are moving to having third parties issue and manage credentials for access to their applications.

- Affiliating with a federation operator and its trust framework would provide financial institutions with standardized credentials and authentication processes.

- Identity issuers can offer financial institutions standardized credentials at varying strength levels (e.g., high, medium, low); thus, financial institutions can opt not to issue credentials and act only as a relying party.

- Financial institutions can “offload” their credential issuance and management to a third-party service provider for access into its customer applications.

- As relying parties, financial institutions can interoperate with any credential issuer and relying party in the system, in particular, financial institutions’ commercial and retail customers.

- If financial institutions see a value and business case to issue (and sell) strong credentials, they could do so and sell them beyond its existing customer base.