One Identity Trust Framework for all Business and Personal Transactions

Establishing a Key Cornerstone for Cyber Security to Achieve Trust
In the wake of seemingly daily news articles about the theft of personal identity, financial, and proprietary information, many businesses today are searching for an affordable solution to the problem of securing information in the cyber world. Solving the problem takes a multi-pronged approach.

TSCP’s Federated Trust Framework has been used successfully to increase security by managing identity vetting and access through a common technical baseline, a set of policy and governance rules, and one agreement flexible enough to address any need.

TSCP is the Transglobal Secure Collaboration Program established in 2002, TSCP is a non-profit 501(c)(6) technical association, which relies on Government-Industry Partnership to accomplish:

- Managed Trust through a Federated Trust Framework with all the agreed governance documents e.g. business, technical, legal, privacy.
- Scalable Trust to the Supply Chain.
- Pooling resources to accomplish specification development, validation in a production and operational environments.
- Sharing lessons learned.
- Leveraging of International Standards adding the framework to meet operational needs.
- Providing the Cornerstone for Cyber Defense.

What is the Problem?

Organizations must be able to trust identities – not only to validate users’ identities, but also their suitability and authorization for access to applications and data – in order to operate in a trustworthy environment.

Today each organization has its own security policies governing data access. While all of these security policies are valid, in the current environment, interoperability is hampered by various security practices invoking different Levels of Assurance and standards. This lack of a common standard and a single agreement is precluding businesses from making good trust decisions. Hence, there is no accepted common trustworthy environment for business commerce.

What is the TSCP Solution?

TSCP’s operational federation goes a step further than other trust frameworks or credential services. The TSCP Bridge and Exchange Network was designed to harmonize and map member identity and access management solutions to a set of common operating rules. These rules provided for a flexible, scalable trust for any type of business transaction. With a common set of governance documents and one agreement, you choose the right identity credential and attributes for each type of transaction across your enterprise. Please visit www.tscp.org for additional information.

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).
The TSCP Trust Framework has been used successfully to secure and manage access to information. The infrastructure that has resulted from the major TSCP member community investment can be leveraged to secure and manage information of multiple stakeholders across the community.

By engaging service providers with a wide-range of technology solutions, TSCP is expanding its Trust Framework to provide flexibility to its members to manage risk and cost. Please visit www.tscp.org for additional information on our Operational Trust Framework.

Who is participating and why you should participate in the Trust Framework?

For TSCP members — IT System Integrators, Aerospace and Defense, Critical Infrastructure, Financial and Retail — this framework enables secure access to other members’ sensitive data by creating a collaborative environment based on scalable and efficient trust mechanisms. TSCP’s chain of trust includes collaboration with U.S. government entities and their prime contractors, their allies and coalition partners.

The chain of trust extends to the defense supply chain. At any given time within the defense global supply-chain, there are hundreds of thousands of supplier companies working on government contracts, representing roughly 3 to 4 million individuals. The defense supply chain can leverage TSCP specifications, capabilities and business processes as they develop their access management solutions. As concerns of cyber threats, data leakage, intellectual property protection and export control compliance began to rise, TSCP established an industry approach to protect sensitive information, an approach based on interoperable trust mechanisms.

Participation in the TSCP Trust Framework provides:

- Opportunity to be part of an industry-wide movement to achieve broad adoption of common policies related information sharing.
- Opportunity to lead, versus follow, the effort to establish identity protection requirements for incorporation into the TSCP Federation Trust Framework.
- Opportunity to leverage standardized approach to secure and simplify access to commercial applications.
- Opportunity to leverage existing operational common operating rules, requirements and policies of TSCP members.
- Opportunity to use the power of One Voice to command strong influence in the marketplace both in terms of establishing de facto standards and influencing technology product roadmaps.
TSCP supports an Attribute Exchange Network (AXN) as an Internet-scale cloud-based managed service and marketplace for federating online credential authentication and attribute exchange services in federation with ISPs, telecommunications service providers, credit bureaus and Relying Party (RP) customers. The AXN allows Identity Providers (IdPs), Attribute Providers (APs), RPs, and users to exchange and reuse credentials and attributes across multiple sites in a policy-driven, low-risk manner, and at an affordable cost. The AXN is built on open industry standards as a neutral, extensible transaction and claims management hub that can enforce privacy and security precepts driven by industry.

- Users preregister through the Trust Framework to the Exchange to establish obtain identity credentials and establish a path to attributes to replace user name and password for each online service (steps 1, 2).
- For online transactions, a user logs into Applications through the Trust Framework Exchange with their devices, trusted credentials, and established attributes (steps 1, 2, 3).
- In each case, users assert their identity credential and/or attributes, consent for credentials to be authenticated and attributes to be verified, and opt-in to share the Online businesses and retailers can verify user membership or affiliation to provide benefits or discounts and enable payment transactions with assurance attributes and verification claims with an online service.

### What are the next steps?

**Step 1 - TSCP Trust Framework Certification Application.** This step allows an Applicant to express intent to certify at one or more assurance levels and describe the nature of their certifying entity.

**Step 2 - Initial Mapping Review.** This step allows TSCP to map the Applicant core operating and security procedures to the TSCP Common Operating Rules. This is an iterative and interactive process.

**Step 3 - TSCP Member Review and Approval.** After receiving a mapping, recommendation TSCP Policy Management Authority makes a decision on the application and agreements are executed.

**Maintenance Phase.** It includes the annual review process and other maintenance tasks that sustain the Trust Framework relationship over time.
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.

- **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.

- **Attribute Exchange Network (AXN).** Standard transaction processes enable the following benefits: 1) Transaction Proxy/Privacy; 2) User Consent/Privacy/User Experience; 3) Spoofing Attacks: Denial of Service Attacks; 4) Man-in-the-Middle (MITM) Attacks; 5) Lower UI and API Maintenance Costs; 6) Simplified User Account Creation and Credential Federation (Web SSO); 7) Lower Account Management Costs: Lower Attribute Verification and AP Contract Management Costs and 8) Leverage the latest developments in identity.

- **Approved Credential Product List.** TSCP’s Cross Credential Cyber Working Group (C3WG) maintains a list of approved Identity and Credential providers that have successfully mapped to the TSCP Trust Framework and mapping of combinations of credentials and attributes to standard levels of authentication that are recognized throughout TSCP’s Trust Framework.

- **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.

- **Single Flexible Agreement and Harmonized SOPs.** TSCP’s Federated Trust Framework has been used successfully to increase security by managing identity vetting and access through a common technical baseline, a set of policy and governance rules, and one agreement flexible enough to address any need.

- **Securing the Supply Chain.** Standards are established for third-party/contract-based identities whose providers participate in the multi-lateral agreement with the federation operator rather than executing multiple bi-lateral agreements with each participant.

- **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.

- **Assured Identities for Business and Consumer Applications.** 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 been vetted.

- **Ability to Meet Government Acquisition Requirements.** TSCP standards and processes align with the Federal government identity and access control, cyber security and export control requirements, which facilitates participants’ ability to meet government acquisition requirements.

- **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.

- **National Strategy for Trusted Identities in Cyberspace (NSTIC) Guiding Principles.** TSCP’s Federation Trust Framework has incorporated the NSTIC guiding principles privacy enhancing and voluntary, secure and resilient, interoperable and cost effective and easy to use for enterprise organizations and end users.
CONTACT INFORMATION

Keith Ward
President & CEO
Phone: 703.760.7897
Email: keith.ward@tscp.org