



Smart Card Alliance International Strong Authentication Use Cases



What is TSCP?

- TSCP is the **Transglobal Secure Collaboration Program** established in 2002. TSCP is a non-profit 501(C)(6) technical association.
- **Government-Industry Partnership** is focused on mitigating the risks, complexity, cost of IT inherent in large-scale, collaborative programs that span national jurisdictions. TSCP provides:
 - Influence to drive a common approach and specifications
 - Efficiency of working together on a common problem
 - Lower costs of development and implementation – leverage common solutions
 - Requirements, architecture, prototypes, deployed capabilities.
- TSCP Defense IT companies have invested over \$400M into internal federated systems using TSCP's common operating rules and specifications.



Common Framework for Federated Collaboration

Key focus is on providing the mechanism and governance for:

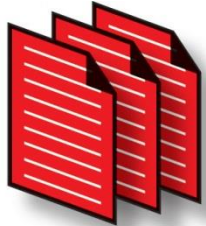
- **Trust.** Member companies' and governments' users digital identities can be trusted by others.
- **Identity Assurance.** Trusted authority assures that its users with cross-certified-enabled digital identities are who they say they are.
- **Interoperability through Federation.** Member companies and credentials are interoperable across the industry and government.



What Has TSCP Accomplished?



SPECIFICATIONS DEVELOPMENT. Develops common specifications for secure collaboration solutions across the TSCP membership that align to government requirements. The specifications fall into these categories:



- Secure information exchange
- Identity credentials/digital identities and attributes
- Federated identity
- Information assurance
- Data labeling and protection and ITAR/Export



VALIDATION THROUGH REFERENCE LAB. Before TSCP publishes its specifications, the capability is in production with two or more members.



GOVERNANCE. Establishes policy and governance for TSCP Solutions.



- Interoperable Identity Federation Trust Framework
- Common Operating Rules
- Legal Framework & Allocation of Liabilities
- Accreditation & Trustmark



FEDERATED HUB. Hosts a Federated Hub for TSCP Membership that enables secure collaboration between TSCP membership and government customers.

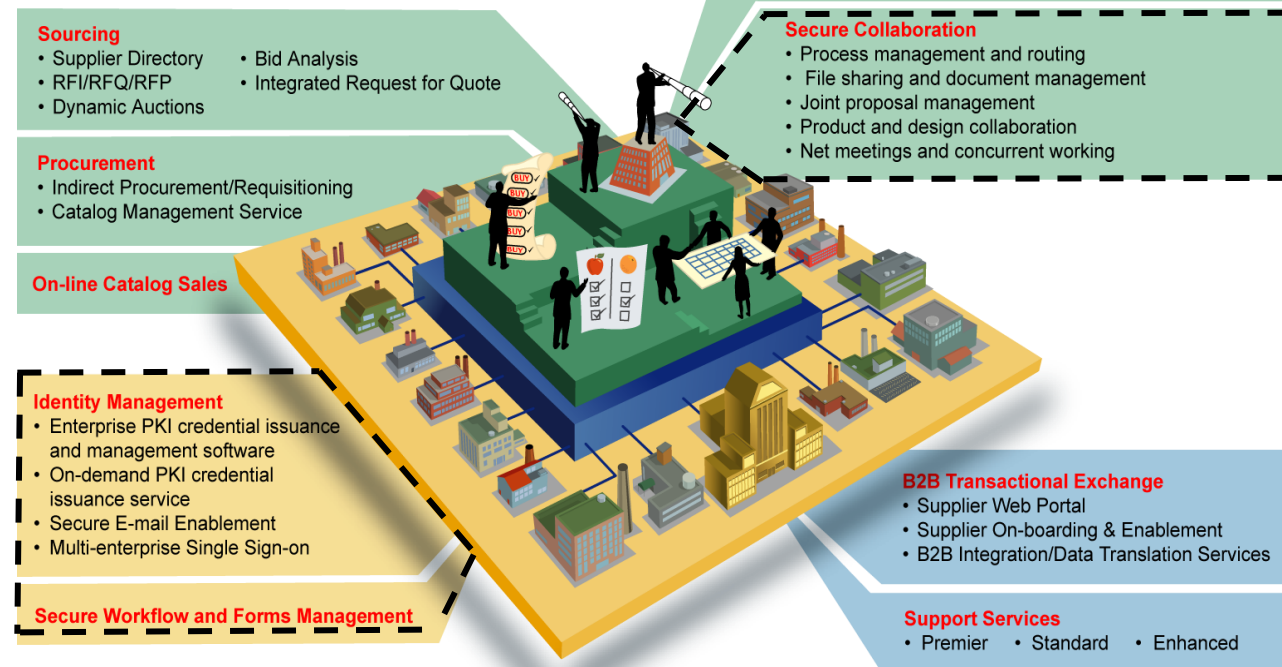


Benefits for the Supply Chain

- Information Security
- Regulatory Compliance
- Compliance with International Collaborative Agreements
- One-Time Spend on Identity & Authentication for Third Parties
- Reduced Acquisition Costs
- Strengthened Trading Partner Relationships
- Secure Information Sharing

TSCP extends chain of trust to the supply chain.

A&D companies are responsible for vetting their supply chain. At any given time within the A&D global supply chain, there are approximately **300,000 supplier companies** working on government contracts, representing roughly **3 to 4 million individuals**.

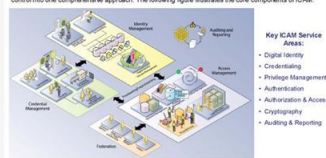


Alignment to Strategic Government Roadmaps

Federal CIO Council - TSCP Industry Standards Body



What is Identity, Credential, and Access Management (ICAM)?
ICAM represents the intersection of digital identities (and associated attributes), credentials, and access controls into one comprehensive approach. The following figure illustrates the core components of ICAM.



The Roadmap

The Federal ICAM Roadmap addresses unified federal identity, credential, and access management programs and how the Executive Branch of the Federal Government will interact with external organizations and individuals. It provides a new government-wide segment architecture for ICAM.



For more information, visit www.idmanagement.gov

PAGE 6 | CONFIDENTIAL | TSCP

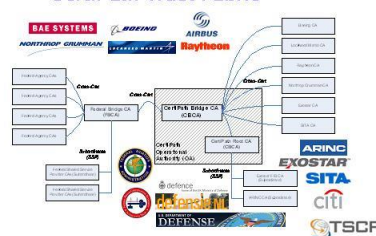


Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance - Cites

External industry guidance and standards bodies to include Transglobal Secure Collaboration Program (TSCP).

Government-industry partnership specifically focused on facilitating solutions for Aerospace and Defense (A&D) issues. Currently working on identity federation issues in international defense and aerospace programs.

CertiPath Trust Fabric



Mapping US DoD Goals to TSCP Strategic Goals

TSCP Strategic Goal 1:
Enable secure information sharing within and between industry and governments.

TSCP Strategic Goal 2:
Enable collaboration compliant with export control and relevant policies and company Intellectual Property protection policies.

DOD Business Process Modeling Common Vocabulary

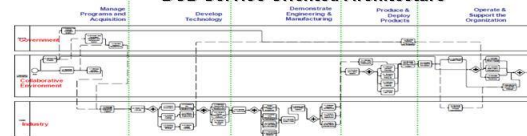


DOD Business Rules Technical Infrastructure Standards Information Assurance Standards

TSCP Strategic Goal 3:
Define a set of interoperable specifications and solutions that enables re-use in a cost effective manner across multiple programs.

TSCP Strategic Goal 4:
Make TSCP specifications and solutions a standard in the A&D community.

DOD Service Oriented Architecture



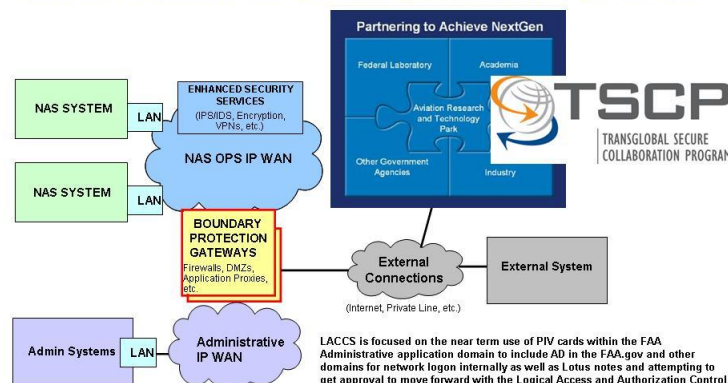
Dennis Wiznosky US DoD DCMO BMA CTO & Chief Architect

PAGE 8 | CONFIDENTIAL | TSCP

8

TSCP Partnering with FAA & Aviation Tech Park

Network Isolation and Boundary Protection & Enclaves



LACCS is focused on the near term use of PIV cards within the FAA Administrative application domain to include AD in the FAA.gov and other domains for network logon internally as well as Lotus notes and attempting to get approval to move forward with the Logical Access and Authorization Control Service program. The program office has not been getting the cooperation necessary from the LOBs that own/control the IT infrastructure. LOBs address sing both Admin and the NAS suggesting we can leverage investment to satisfy both. Additionally each major LOB has its own roadmap. And have been trying to align them around a set of Enterprise security services.

PAGE 10 | CONFIDENTIAL | TSCP

17

Mapping TSCP Strategic Goals to MODIS Four Effects

TSCP

MODIS

Goal 1: Enable secure information sharing within and between industry and governments

Accessibility & Trust – Simplify and standardise to ensure information accessibility and integration

Goal 2: Enable collaboration compliant with export control and relevant policies and company IP protection policies

Information Exploitation – Enable maximum utility of information in compliance with policy and standards

Goal 3: Define interoperable specifications and solutions that enable re-use in a cost-effective manner across multiple programs

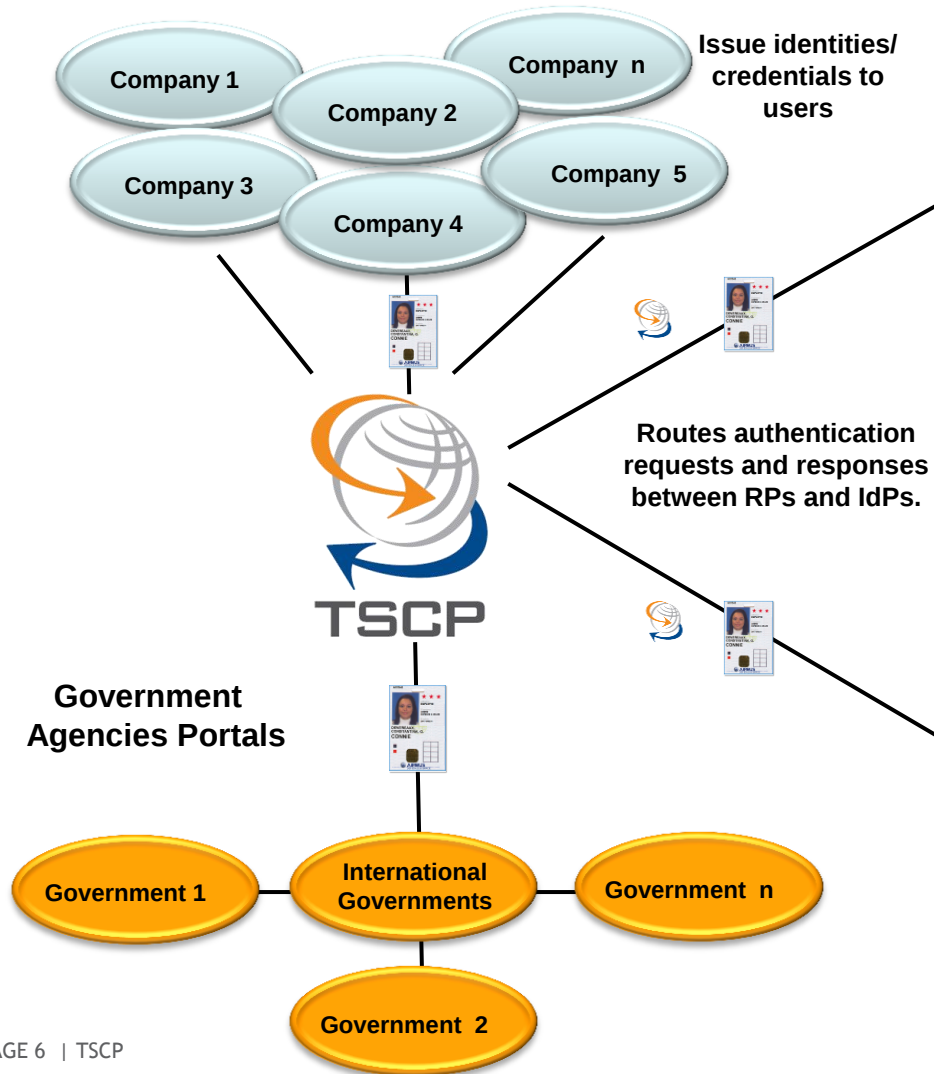
Value for Money – Exploit technology and “sweat our assets” to provide optimum return on investment

Goal 4: Make TSCP specifications and solutions a standard in the A&D community

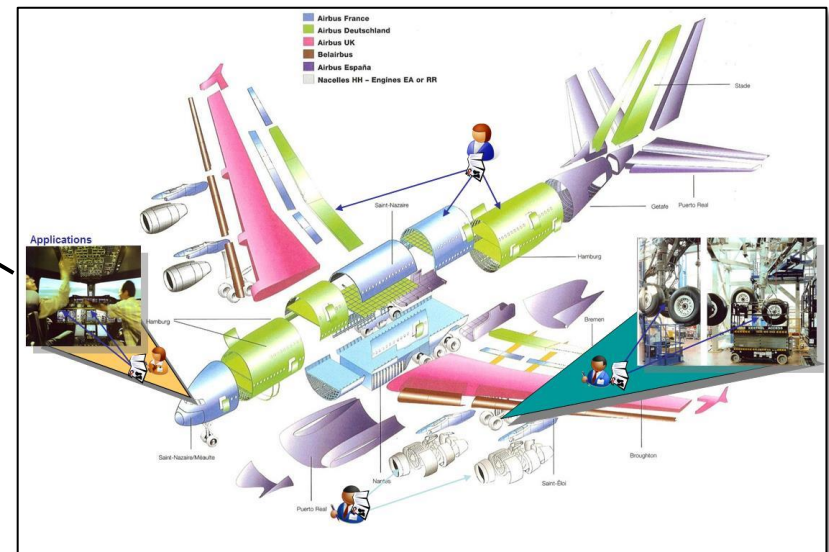
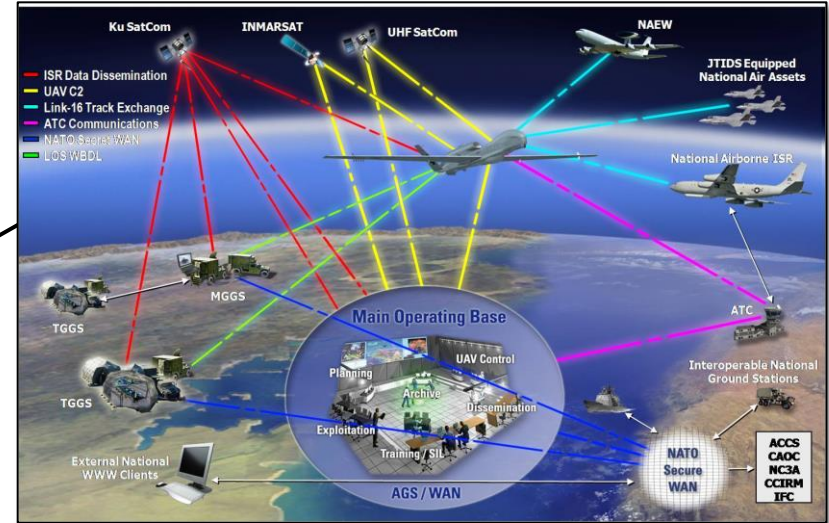
Strategic Alignment – Overcome challenges to interoperability through international alignment

Federation and Mission Support

TSCP Member IdP(s)



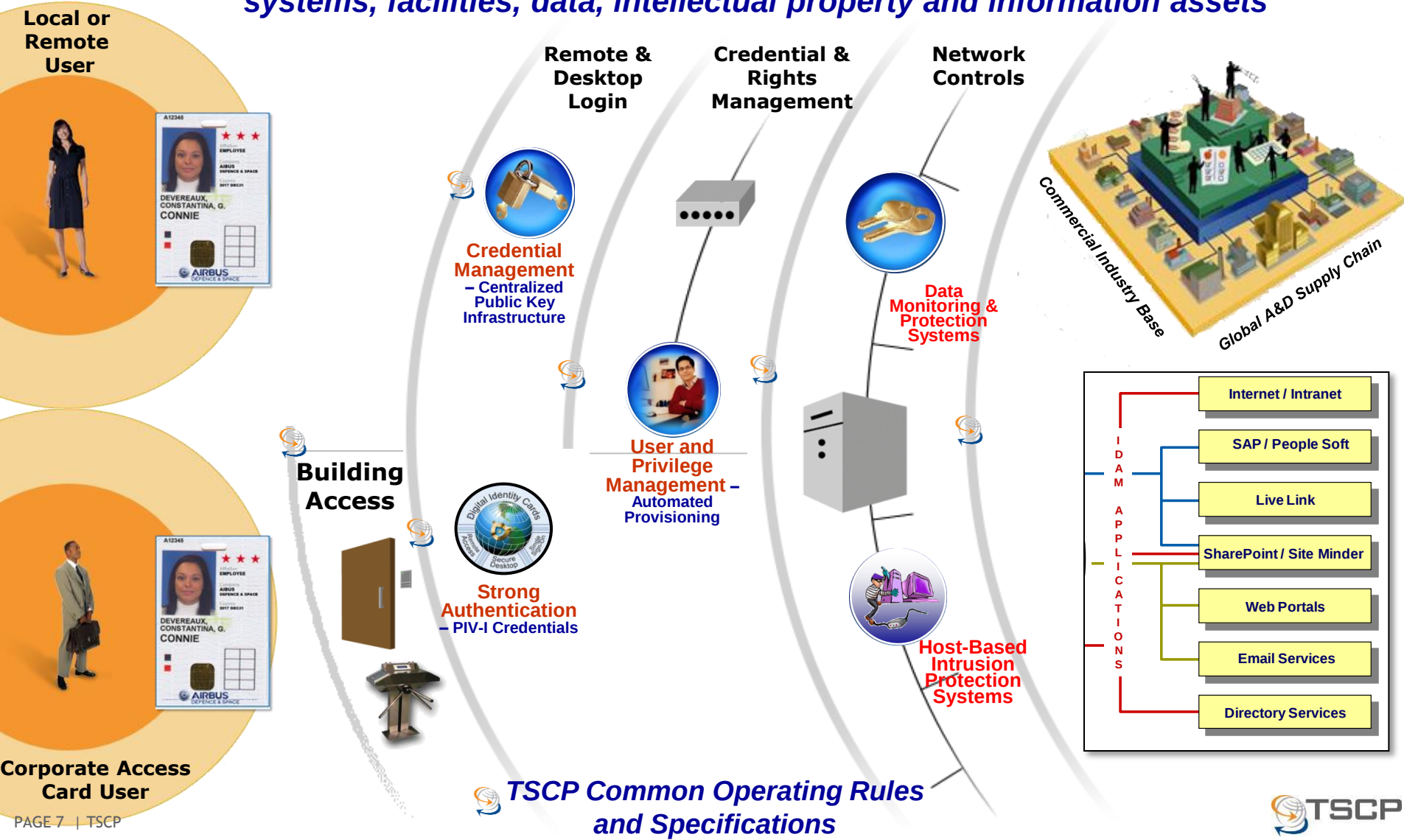
Programs / Operations



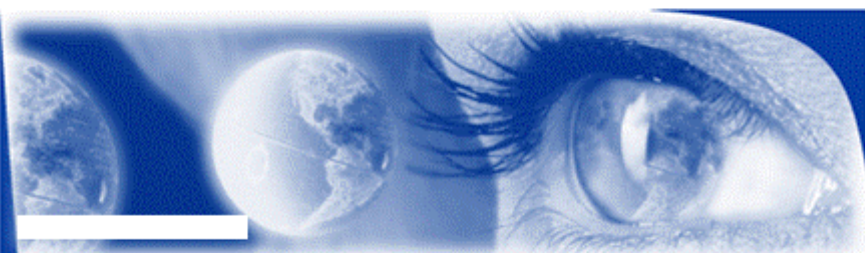
Supply Chain

Use Case 1: Multi-Layer Security across the enterprise

Multi-Layered approach to provide additional security layers across our networks, systems, facilities, data, intellectual property and information assets



Use Case 2: Secure Collaboration - ILH/ITAR



Scenario: Netherlands Ministry of Defence (NL MoD), a Boeing customer of the fictional X-Heli helicopter, is proceeding to acquire more helicopters. Several organizations (Boeing, NL MoD, NLR — National Aerospace Laboratory) must collaborate on the design, requirements, test, and certification.

IDENTITY FEDERATION

Boeing, NL MoD, and NLR use Identity Federation technology to login to the NL MoD X-Heli document share site by asserting identity attributes and/or claims in line with TSCP specification DSIF v1.2. The NL MoD X-Heli document share consumes these claims and dynamically provides attribute based access control (ABAC).

Business Protection: Attributes provide a way to allow more granular access control, scalability, and better identity assurance.

CLASSIFICATION OF DOCUMENTS*

To ensure appropriate protection, it is necessary to classify data/documents. This can be achieved by adding visual markings and meta-data labels to a document. The three parties use the TSCP Information Labeling & Handling (ILH) Protection Profile. The document itself gets populated with labels utilizing software that meet TSCP ILH specifications.

Business Protection: Protection Profiles defined and agreed between collaborating organizations provide the foundation for controlling access.

ENFORCEMENT OF UPLOADED DOCUMENTS*

Documents uploaded to the NL MoD X-Heli document share automatically get prepopulated with its meta-data. Deny rules matching specific meta-data can prevent documents from being uploaded.

Business Protection: Ensures documents consistently maintain their classification and protection across systems.

TRIMMING OF DOCUMENT SHARE LIBRARIES*

The NL MoD X-Heli document share enforces the access controls defined in the protection profile. A user can only see a trimmed list of documents they are authorized to see. Search results provide the same behavior.

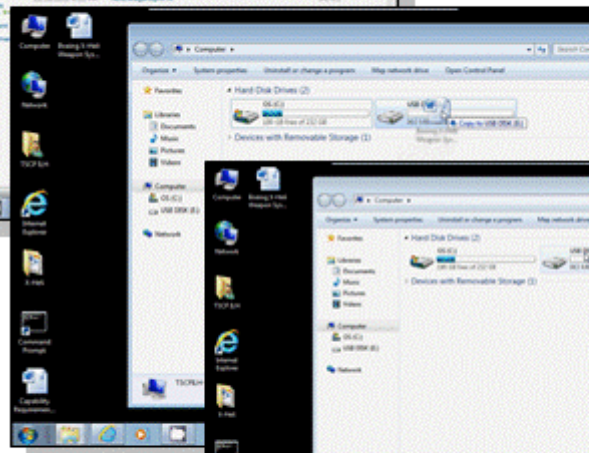
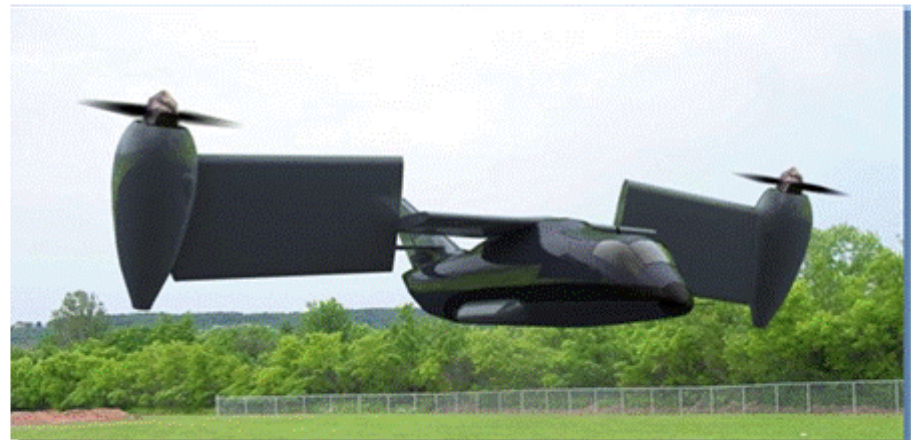
Business Protection: Prevents unauthorized access by relying on attribute based access controls.

DATA LOSS PREVENTION OF DOWNLOADED FILES*

By using Data Loss Prevention (DLP) technology, downloaded files with sensitive information can be prevented from being opened and accessed by unauthorized users.

Business Protection: Provides fine-grained access control on the document itself.

Secure Collaboration Proof of Concept Demo



*Powered by
NEXTLABS



Ministerie van Defensie



Use Case 3: PIV-I into Adjacent Markets: Financial & Retail Sectors

Physical World

John



Devices



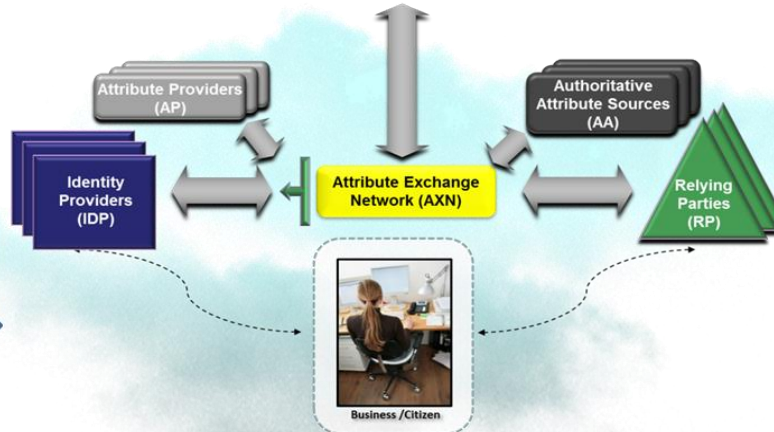
Credentials



Online Access



Trust Framework



Applications (examples)

Retail



Online Trading



Supplier Portals



TSCP Pilots

- **USERS HAVE ONE or FEW SECURE CREDENTIALS.** Users may reduce the number of credentials needed for online transactions. With federation, they can select one secure credential for access to all of their retail applications.
- **FINANCIAL INSTITUTIONS ARE RELYING PARTIES ONLY WITH ABILITY TO ACCEPT STRONG CREDENTIALS.** Financial institutions only manage authentication and access to their applications. Through federation, they are able to accept one (or more) strong credential and lower level credentials for applications not requiring secure authentication.
- **FINANCIAL INSTITUTIONS DON'T ISSUE OR MANAGE CREDENTIALS AND MAINTAIN ONLY A SINGLE EXTERNAL CONNECTION.** Financial institutions no longer need to issue credentials. They don't manage external credentials nor multiple connections. They maintain a single connection to a federated service for acceptance of credentials.

Use Case 4: TSCP Trust Framework Information Sharing Exchange

TSCP Trust Framework

Data Providers

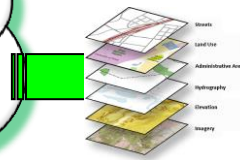


Data Access Controls



Information Sharing Exchange Cloud Environment

GIS Layer Access



Data Consumers Federal



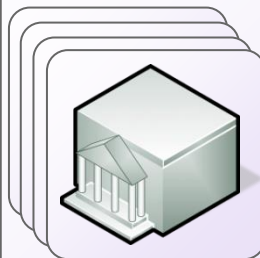
SLTT



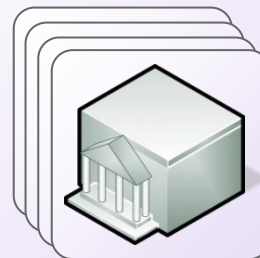
EOC



Identity Claims Providers

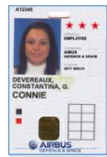


Commercial
Identity Providers



State Government
Identity Providers

Higher Level Credential



Higher Level Credential



Questions?

TSCP Inc.

Keith Ward | President and CEO

8000 Towers Crescent Drive, Suite 1350, Vienna, VA 22182

(M): (703) 945-9875 | (F): (703) 760-7899 |

Email: keith.ward@tscp.org | www.tscp.org

