



Secure Access through Federation

Iana Bohmer
Director, Identity Management
Northrop Grumman

May 15, 2008

Topics

- TSCP Membership
- TSCP Origin
- TSCP Mission & Vision
- Common Framework for Secure & Federated Collaboration
- Challenge of Domain Awareness
- Certipath - Trust Hub for Federation
- Business Challenges that TSCP Aims to Solve
- TSCP Specification: Secure E-Mail
- Upcoming Specifications
- Summary: Membership Benefits

TSCP Membership



Government-industry partnership focused on facilitating solutions to the most critical issues in Aerospace and Defense (A&D) today.

TSCP Origin

Created in **2002** by U.K. MoD, U.S. DoD and global A&D companies, the original goal was to define secure data sharing and collaboration for the **entire supply chain**, even when it begins with a government customer. The collaboration environment was characterized by:

- Large defense contracts involving **thousands of companies**
- Information sharing **across company and country boundaries**
- **Different policies/laws** in each company and country
- Increasing risks of **data breaches** or violating import/export regulations
- Unproven and inconsistent **identity vetting and management**
- Non-existent **information and personal profiling**

TSCP Vision & Mission

Vision: International government-A&D industry partnership that seeks:

- **Risk Mitigation.** Mitigation of inherent IT risks in large multi-national collaborative programs:
 - Complexity
 - Cost
 - Compliance
- **Frameworks.** Establish frameworks for secure collaboration and information-sharing while protecting IP.
- **Interoperability.** Cooperative effort to establish interoperability specifications:
 - Determine **impediments** to sensitive data sharing
 - Define **requirements** for solution
 - Implement prototype to test the **specification**
 - Encourage vendors to create **compliant solutions**

Mission: TSCP's mission is to establish an environment in which employees, contractors and suppliers can securely access data required to execute on contracts and programs.

Common Framework for Secure & Federated Collaboration



- **Meet government agencies' emerging requirements for identity assurance across domains**
- **Demonstrate compliance with export control regulations**
- **Protect corporate IP in collaborative and other information sharing programs**
- **Protect personal privacy data of employees**
- **Have collaborative toolsets that will interoperate with customers and suppliers**
- **Re-use collaborative capabilities among multiple programs**
- **Provide assurance that collaborative partners can be trusted**

Challenge of Domain Awareness

- **Large, Complex Space.** Difficult to monitor a large global space.
- **No Central Authority.** No single or centralized authority.
- **Pervasive Threat.** Small cells create pervasive threats to large nation states



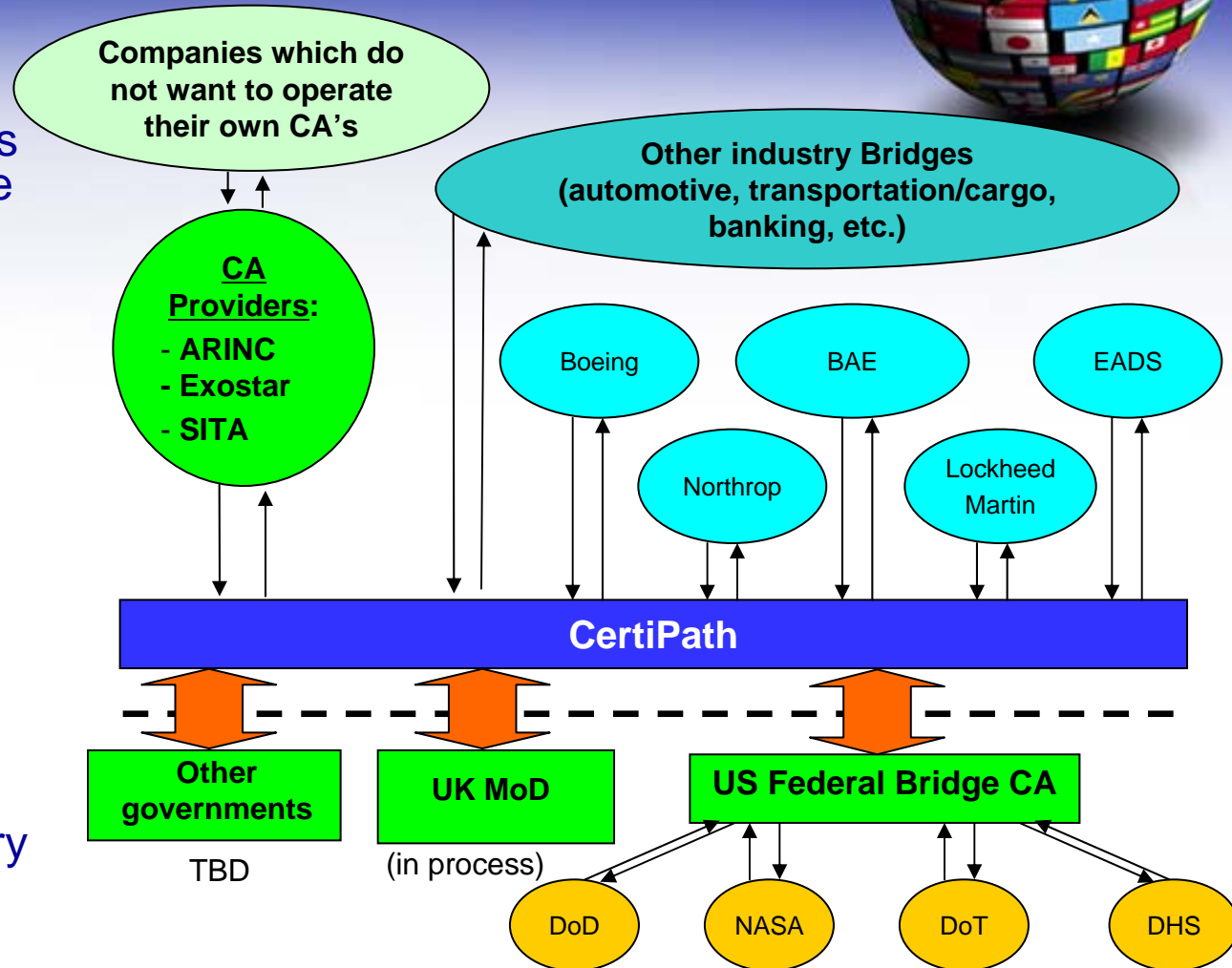
CertiPath – Trust Hub for Federation



Trust. Mechanism by which member companies and governments can use trusted digital IDs.

Identity Assurance. Central, trusted authority that issues CertiPath-enabled digital identities, which assures that identities are verified and validated.

Interoperability. System that providing interoperability of participants' credentials across industry & government.



Business Challenges that TSCP Aims to Solve

Mutual Confidence (Trust)

Mitigating risk and ensuring quality between parties in the circle of trust can be performed through:

- Definition of business standards
- Definition of minimum requirements
- Enforcement through certification and audits

Liability

Allocation of liability in the event of failure of a critical transaction due to malfunction of a shared authentication component:

- Extent of liability
- Definition of dispute resolution process

Risk

- Pooled Knowledge: sharing of customer information (e.g. # of customers, customer names, etc...) between enterprises
- Revocation Procedures: increased reliance on third parties for authentication
- Fraud Protection: broadened potential for fraud if an identity is ever compromised
- Security Incident Procedures: coordinated effort for analysis and correlation of audit logs among parties involved

Compliance

- Privacy Legislation: ensure privacy terms are not violated when federating an identity between enterprises

TSCP Specification: Secure E-mail

TSCP has established specification for secure collaborative e-mail:

- Organizations can **trust and identify** e-mail senders and recipients
- Eliminates inherent identity and data transmission security flaws
 - E-mail can only be shared by **trusted, vetted parties**
 - Based on users and desktops
- Available to all A&D industry - and beyond
 - **Free step-by-step guide** on TSCP.org
 - Developed with COTS products and open-source software
 - Leverages **CertiPath** trust federation
- **Controlled Unclassified Information** and sensitive program data can be shared among thousands of partners
- For Microsoft Outlook and Lotus Notes

Upcoming Specifications

TSCP is working on specifications that will be available in the near future:

- **PKI Authentication:** IP protection and export control inside of a (PLM) environment
 - In production in 2008
- **Information Asset Protection:** IP protection and export controls in real-time collaboration, such as online white boarding.
 - Proof of concept in 2008
- **Document Sharing with Identity Federation (DSIF):** Sharing of documents across member domains using federation for authentication of identities.
 - Pilot in 2008
- Same process as with Secure E-mail
 - **Free step-by-step guide** on TSCP.org
 - Developed with COTS products and open-source software
 - Leverages **CertiPath** trust federation

Summary: Membership Benefits



TSCP Microsoft meeting Feb 2007.

*On any given day, over 100 engineers
are working on TSCP projects*

To Governments & Prime Contractors/OEMs

- Influence to drive a common approach and specifications
- Efficiency of working together on common problems
- Mitigation of risk exposure in reference to the insecurity of data sharing
- Reusable specifications that reduce integration complexity, coordination time and collaboration costs

To Solution Providers/Vendors

- Exposure to motivated customer base and goodwill
- Defined roadmap and business case
- Working prototypes that ease development costs
- Reusable specifications



QUESTIONS and DISCUSSION



Contact Information:

www.tscp.org