“It is a very sad thing unquestionably that railways, which mechanically have succeeded beyond anticipation and are quite wonderful for their general utility and convenience, should have failed commercially.”

The Economist, 1857
The Central Pacific and Union Pacific meet at
Promontory Summit, Utah
May 10th, 1869
Agenda

- Web Security Primer
- Security and Interoperability
- SAML Background
- Airline Industry Case Study
- Lessons Learned
- SAML and Identity Management
- Business Drivers
- SAML Readiness
Web Security Primer – User Access

User provides credentials to authenticate and generate session.

Security Domain
• Policy Enforcement Point (PEP)
• Policy Decision Point (PDP)
Many scenarios require users to access resources in multiple, independent security domains. These scenarios drive the need for standards.

B-2-B Scenarios
- Service Levels
- Aggregated Services
SAML Background

- Security Assertion Markup Language (SAML)
  - Defines XML schema for security assertions and protocol.

- SAML Assertions
  - Authentication
  - Authorization
  - Attribute

- SAML and Cross Domain SSO

- Related Web Services Standards
  - Liberty Alliance
  - WS-Security
  - XACML
  - SPML
Airline Industry Case Study

Step 1: User must login at Airline to gain access

Step 2: User must login at Aerospace company to gain access

Multiple Logins are inconvenient for users

User credentials must be maintained in both security domains

Help desk calls to both domains

No single point of user revocation
Step 1. User login at Security Domain 1 to gain access

With SAML, user credentials are only maintained in Security Domain 1

Step 2. After SAML assertion exchange, user seamlessly accesses Security Domain 2 without additional login
Airline Industry Case Study

Security Starts With The Right Foundation
Lessons Learned

- Project Plan Should Include “Out of Band” Considerations:
  - Coordination
    - Intra Company Processes
  - Technical Integration
    - PKI
  - Attention to Detail
    - Shared Support
    - Common Identifiers
  - Ongoing Administration
    - Identity Management
SAML and Cross Domain Identities

- Users in Common Model
- Ongoing Identity Administration
  - User Lifecycle
  - Entitlements
- Delegated Administration
- Workflow
- Self-Service
- Identity Web Services
SAML Business Drivers

- Significant Business Impact
  - Cost Avoidance/Reduction
  - Improved User Experience
  - Embedded Services

- Opportunity for IT/Business Partnership
SAML Readiness Assessment

- Survey Existing B2B Relationships
  - User Experience
  - Administration Structure
    - Help Desk
    - Password Reset
  - Existing Security Model
NetPoint SAML Services

- In Production
- Support for Inbound and Outbound SAML
- Tightly Integrated With COREid
  - Leading solution for delegated admin, self-service, self-registration
  - Identity Web Services (IdentityXML)
- Support for Bookmarked URL’s
- Support for Domain Verification
- Domain Aware Error Messages
Discussion

For More Information:

• Oblix Web Site
  • http://www.oblix.com

• OASIS SAML Information
  • http://www.oasis-open.org/committees/wss/