

Interagency Advisory Board

Meeting Agenda, July 28, 2010

1. **Opening Remarks**
2. **Research Collaboration in the Cloud: How NCI and Research Partners Are Improving Business Processes using Digital Identities** (*Sherry Ansher, NIH/NCI and Cindy Cullen CTO Safe Bio-Pharma*)
3. **Minimum Standards for Proof and Verification of Personal Identity** (*Graham Whitehead, NAPSO*)
4. **Planned Changes to the Federal PKI** (*Judy Spencer, FICAM Co-Chair*)
5. **The Status and Future Plans for the GSA Shared Service** (*Steve Duncan, MSO Director*)
6. **The ICAM Return on Investment (ROI) WG** (*Tim Gaines, ICAM Chair*)
7. **Proposed Federal Profile for SAML 2.0 for LOA 1 through 4** (*Tim Baldrige, FICAM AWG*)
8. **TSCP Implementation Pilots to demonstrate NTSIC Goals & Objectives** (*Keith Ward*)
9. **Closing Remarks**



Federal CIO Council
Information Security and Identity Management Committee

Identity, Credential, and Access Management

ICAM SAML 2.0 Profile Change Highlights

Tim Baldridge
AWG Co-Chair
NASA

Chris Loudon
AWG Co-Chair
Protiviti Government Services



Status for Federal SAML 2.0 Web SSO Profile

- Multiple review cycles in Federal ICAMSC AWG
 - Distribute Draft
 - Solicit Revisions and Comments
 - Review and disposition comments
- Currently under Review by Federal ICAMSC
 - Sent to ICAM-SC Distribution list
 - Comments or Intent to Comment due by August 13, 2010



New Approach

➤ **Alignment with other Profiles**

- Aligns to a great degree with
 - Egov 1.5
 - InCommon SAML 2 Profile
 - Legacy E-Auth SAML 2.0 Profile
- Fosters interoperability among these communities
- ICAM SAML 2.0 Profile is most the interoperable profile ever
- COTS support

➤ **Deployment Profile rather than Product Profile**

- Guidance to agencies on how to implement/configure in their infrastructures, rather than defining what the products do



Additions to the Profile

- **New way to convey Level of Assurance (LOA)**
 - In old way, LOA was conveyed in a SAML Attribute,
 - Did not guarantee automatic COTS product behavior to LOA
 - Now expressed in SAML AuthNContext
 - Allows automatic COTS product behavior
 - RP can request a particular LOA for the current authentication
- **Support Trust Framework Providers (TFPs)**
 - PKI is the trust anchor for Federation metadata
 - Metadata establishes trust and configuration requirements among Federation members
 - Distinction made between Federal and non-Federal ICAM member metadata



Additions to the Profile (Continued)

- LOA 4 requires Holder of Key (HoK)
 - SAML Assertions good only to LOA 3
 - HoK Required by NIST SP 800-63 draft 1
 - RP and IdP must perform HoK at LOA 4
 - HoK requires proof of key possession and PKI path validation:
 - End user authenticates to IdP
 - IdP redirects end user to RP with SAML Assertion
 - RP validates SAML Assertion
 - RP then verifies end user possesses HoK certificate
 - RP validates HoK certificate
 - HoK certificate must be cross-certified with the FBCA
 - LOA 4 HoK is the “PIV-SAML” connection



Removed from the SAML Profile

- **Single Logout (SLO)**
 - Removed as a requirement because:
 - COTS product support is lacking
 - Practical limitations to implementation
 - e.g., numerous redirects, limited error handling, usability
 - SLO Guidance provided
- **Common Domain Cookie (CDC)**
 - Removed as a requirement because:
 - Counter to OMB requirement for transient cookies
 - Requires significant infrastructure
 - Does not scale with multiple Federations (inter-Federation)



Changes to SAML Profile

- Approach to Name Identifiers
 - Scoped pseudonym requirement to c-g only
 - Silent on other relationships (e.g., b-g, g-g)
- Encryption/Signature Requirements
 - At LOA 1, TLS encryption is sufficient for Assertions
 - Authentication Requests no longer need to be signed at any LOA
- Approach to Attributes
 - Profile scoped to authentication events
 - Does not require attributes in Assertion
 - Refers attribute exchange to BAE Specification
- Privacy
 - Explicitly defers to TFPAP privacy requirements



Holder of Key Revisited

- Considerations:
 - Oasis HoK specification is not finished
 - HoK COTS support is nearly non-existent
 - COTS crypto modules need to be reworked to support HoK