Federal Identity, Credential, and Access Management Trust Framework Solutions

Identity Scheme and Protocol Profile Adoption Process

Version 2.0.0
DRAFT: 11/11/13

Questions?
Contact the FICAM TFS Program Manager at TFS.EAO@gsa.gov

Table of Contents

1. PURPOSE

This document is the *Identity Scheme and Protocol Profile Adoption Process* and defines the process whereby the government can assess the efficacy of specific subsets of identity management standards (i.e., schemes and profiles) for federal purposes so that an Agency online application or service and Identity Provider application or service can implement the schemes confident that secure, reliable and privacy respecting technical interoperability will be achieved at a known level of assurance comparable to one of the four Office of Management and Budget (OMB) Levels of Assurance.

1.1 Audience

This guideline is intended for:

- **Token Managers, Identity Managers and Credential Service Providers**, who are seeking to offer their services for use by the U.S. federal government.
- **Trust Framework Providers**, who are seeking to map their security and privacy guidelines to U.S. federal government security and privacy requirements
- **Security and Privacy Practitioners**, who recommend, design, build or provide solutions that meet U.S. federal government requirements

1.2 Usage

1. Read the *Trust Framework Solutions Overview* to understand the background, authorities and components of the FICAM TFS Program
2. Read the *Identity Scheme and Protocol Profile Adoption Process* to understand how protocol profiles are created, adopted and used by the government to ensure that the RP application and the CSP communicate in a confident, secure, interoperable and reliable manner.
3. Read the *Trust Framework Provider Adoption Process (TFPAP) for All Levels of Assurance* to understand the role of the Trust Framework Provider
4. Read the *Authority To Offer Services (ATOS) for FICAM TFS Approved Identity Services* to understand the requirements for offering services to the U.S. Federal Government

2. BACKGROUND

The FICAM Trust Framework Solutions (TFS) is the federated identity framework for the U.S. federal government. It includes guidance, processes and supporting infrastructure to enable secure and streamlined citizen and business facing online service delivery.

The *Trust Framework Solutions Overview* document provides a holistic overview of the components of the TFS which consists of:

- *Trust Framework Provider Adoption Process (TFPAP) for All Levels of Assurance*
- *Authority To Offer Services (ATOS) for FICAM TFS Approved Identity Services*
- *Identity Scheme and Protocol Profile Adoption Process*
- *Relying Party Guidance for Accepting Externally Issued Credentials*
- E-Government Trust Services Certificate Authority (EGTS CA)
- E-Government Trust Services Metadata Services (EGTS Metadata Services)

The protocol profiles as developed via this process describe the technical standardized and interoperable interface agreements that will be used to exchange identity information between disparate government systems that cross organizational and policy boundaries.

3. IMPLEMENTATION

Standards development is a long, painful process and often results in a compromise everyone involved can live with. In particular there is a great tension around the need to provide flexibility and extensibility, security and privacy, and interoperability in the standards development process. The result often ends up being a standards document that provides multiple ways of accomplishing the same thing, all of which are "compliant" to the standard but often may not be interoperable.

For the federal government to utilize industry standards, they need to be widely deployed by multiple vendors, interoperable, and meet the security and privacy policy requirements articulated by authoritative federal government bodies. The adoption process defined herein, based on guidance from the OMB, NIST, and review from private sector partners, provides a consistent, standard, structured means of identifying, vetting, and approving identity schemes and protocol profiles (i.e., an identity scheme or protocol profile meets all applicable ICAM requirements, as well as other Federal statutes, regulations, and policies).

In addition, the structured process provides assurance to all ICAM participants that underlying identity assurance technologies are appropriate, robust, reliable, secure and privacy respecting. This confidence is essential to government-wide acceptance and use of ICAM.

3.1 Standardized Assurance Level URIs

The TFPAP, in recognizing Component Identity Services, utilizes the following terminology for token and identity assurance levels, while continuing to utilize the existing LOA terminology for credential assurance:

- **Token Assurance Level (TAL)**: The degree of confidence that that an individual, organization or device has maintained control over what has been entrusted to him or her (e.g., key, token, document, identifier) and that the token has not been compromised (e.g., tampered with, corrupted, modified)
- **Identity Assurance Level (IAL)**: The degree of confidence that an individual, organization or device is who or what it claims to be.
- **Level of Assurance (LOA)**: In the context of OMB M-04-04, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued

The following standardized assurance level URIs, which are conformant to the FICAM XML Namespace Requirements, are provided for use by all FICAM Identity Schemes and Protocol Profiles:

Token Assurance Level 1-4:

- http://idmanagement.gov/ns/assurance/tal/1
- http://idmanagement.gov/ns/assurance/tal/2
- http://idmanagement.gov/ns/assurance/tal/3
- http://idmanagement.gov/ns/assurance/tal/4

Identity Assurance Level 1-4:

- http://idmanagement.gov/ns/assurance/ial/1
- http://idmanagement.gov/ns/assurance/ial/2
- http://idmanagement.gov/ns/assurance/ial/3
- http://idmanagement.gov/ns/assurance/ial/4

Credential Level of Assurance 1-4:

- http://idmanagement.gov/ns/assurance/loa/1
- http://idmanagement.gov/ns/assurance/loa/2
- http://idmanagement.gov/ns/assurance/loa/3
- http://idmanagement.gov/ns/assurance/loa/4

NOTE: ICAM LOA URLs, as described in the FICAM SAML 2.0 Web Browser SSO Profile v1.0.2 and earlier, and the Authentication Policy URL as described in the FICAM OpenID 2.0 Profile v1.0.1 and earlier, are depreciated and will not be supported in future versions of those profiles.

4. SCHEME AND PROFILE ADOPTION PROCESS

Identity scheme adoption is driven by industry standards, and Federal government policies and Profiles. OMB and the National Institute of Standards and Technology (NIST), who are the primary authoritative bodies driving the applicable Federal government policies, standards, and policies.

4.1 Value Determination

The FICAM TFS Program Manager, after consultation with relevant government agencies and organizations, determines whether adoption of a published identity scheme would be valuable to Federal Agencies. In doing so, the FICAM TFS Program considers whether the identity scheme has (or is gaining) industry traction, uses proven technology, has (or is gaining) penetration in particular communities, and has direct applicability to Federal activities.

4.2 Standardization Review

The FICAM TFS Program Manager establishes a Profile Assessment Team to review the identity scheme to determine whether it is standards-based, a basic requirement. Proprietary schemes are discouraged, though if a compelling case can be made for adopting one, the government will consider it. The review determines, among other things, whether the identity standard is fully documented, well maintained, available in commercial-off-the-shelf (COTS) products, interoperable across COTS products, and open (i.e., non-proprietary).

If the assessment indicates the scheme is viable, the FICAM TFS Program Manager makes a determination to:

1. Adopt an existing industry Scheme Profile as a baseline provided it meets the Federal government's security, privacy and interoperability criteria; or
2. Create a new Scheme Profile

The Scheme Profile does not alter the standard, but rather specifies which areas of the standard will be used for technical interoperability of government applications, and how they will be used. Specifically, the Scheme Profile specifies the subset of requirements and functionality within the scheme that is

acceptable for government use at various Levels of Assurance based upon compliance with NIST SP 800-63 and other privacy and security requirements.

The Profile Assessment Team works closely with the FICAM TFS Program Testing Facilities during profiling to assess viability of the Profile with COTS products to ensure the Profile is practical and interoperable. The Scheme Profile is subsequently used to ensure implementations of the identity scheme:

1. Meet Federal standards, regulations, and laws; and
2. Minimize risk to the Federal government and maximize interoperability.

Upon conclusion of this step, the Profile Assessment Team delivers a Report to the FICAM TFS Program Manager.

4.3 Scheme and Profile Adoption Decision

The FICAM TFS Program reviews the Profile Assessment Team Report on standardization of the identity scheme, and after consultation with relevant government agencies and organizations, decides on whether to adopt the identity scheme. Upon adoption, the scheme is added to the Approved Identity Scheme List, Relying Parties and Credential Service Providers may be notified of the adoption as necessary, and the Scheme Profile can be used by the Federal government.

4.4 Ongoing Activities

Once adopted, a scheme is subject to review in the event of the following:

- Activities related to newer versions of a scheme (e.g. SAML 1 to SAML 2), which could result in revision or decommission of the adopted scheme or adoption of a new scheme;
- Determination as to whether the scheme should be discontinued (i.e., no longer acceptable to the Federal government). Discontinuance may be for reasons including, but not limited to, no longer applicable to the Federal government, no longer compliant with the applicable Profile, no longer supported by COTS products;
- Compliance assessment against applicable Profile to the degree specified in NIST SP 800-63; and
- Other justifiable reasons as defined by the FICAM TFS Program.

4.5 Scheme and Profile Adoption Process Maintenance

The ICAM Program will evolve over time. As the needs of the Program change or become clearer, it is likely that the identity scheme adoption process will evolve. The FICAM TFS Program has responsibility for identity scheme adoption process maintenance. Draft revisions of this document will be made available to applicable Federal government agencies and organizations, as well as COTS vendors, for comment.

APPENDIX A – REFERENCE DOCUMENTATION

[1] HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors
http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

[2] OMB M-04-04: E-Authentication Guidance for Federal Agencies
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[3] OMB M-06-22: Cost Savings Achieved Through E-Government and Line of Business Initiatives
http://www.whitehouse.gov/omb/memoranda/fy2006/m06-22.pdf

217 # APPENDIX B - DEFINITIONS

Term	Definition
Identity Management Standard	Identity standards, such as SAML and Liberty Alliance, specify protocols and standards for federated identity mechanisms for different entities to share identities without requiring the end user to manage multiple accounts.
Scheme	Precisely scoped subset of an identity management standard.
Scheme Adoption	Acceptance of precisely scoped subset of an identity management standard by the Federal government after rigorous review and determination of usefulness with respect to ICAM objectives.

218

219 # APPENDIX C - ACRONYMS

Acronym	Definition
CIO	Chief Information Officers
COTS	Commercial off the Shelf
FCIOC	Federal Chief Information Officers Council
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive
ICAM	Identity, Credential, and Access Management
NIST	National Institute of Standards and Technology
OGP	Office of Governmentwide Policy
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language
SP	Special Publication

220