Federal Identity, Credentialing, and Access Management

Identity Scheme Adoption Process

Version 1.0.0
Release Candidate

July 8, 2009

Document History

Status	Release	Date	Comment	Audience
Draft	0.0.1	4/14/09	Initial Draft	Client
Draft	0.0.2	4/20/09	Revisions per client	Internal
Draft	0.0.3	4/27/09	Revisions per internal review	Internal
Draft	0.0.4	4/30/09	Revisions per internal review	Client
Draft	0.0.5	5/3/09	Revisions per client inputs	Client
Draft	0.1.0	5/26/09	Revised per client inputs	Limited Distribution
Release Candidate	1.0.0	7/8/09	Final release preparation	General Distribution

Editors

Dr. Peter Alterman	Judith Spencer	Chris Louden
Terry McBride	Dave Silver	Terry McBride
Steve Lazerowich		

Executive Summary

It is in the government's best interest to leverage open identity management standards whenever possible. In order to ensure these standards are viable, robust, reliable, sustainable (e.g., available in commercial products), and interoperable as documented, Federal Identity, Credential, and Access Management (ICAM) requires a mechanism to assess the identity management schemes against applicable federal requirements, policies, and laws.

This document defines a process whereby the government can assess the efficacy of specific subsets of identity management standards (i.e., schemes) 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 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. The adoption process is as follows:

1. **Scheme value determination** – management determination whether a scheme is worth investigating in detail;
2. **Standardization review** – architecture working group and lab assessment of the scheme; and
3. **Adoption decision** – Identity, Credential, and Access Management Sub Committee (ICAMSC) vote on whether to adopt the scheme as scoped by the architecture working group.

Subsequent to adoption, a scheme is subject to periodic review and amendment, and possibly discontinuance, as necessary.

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. Draft revisions of this document will be made available to applicable Federal government agencies and organizations, including commercial-off – the-shelf (COTS) vendors, for comment. Those comments will be provided to the ICAMSC before any final revision is approved.

Table of Contents

Figures

1. BACKGROUND

The General Services Administration (GSA) Office of Governmentwide Policy (OGP) is responsible for government-wide coordination and oversight of Federal Identity, Credential, and Access Management (ICAM), comprised of Federal PKI, Federal Identity Credentialing (HSPD-12) [1] and E-Authentication activities. These activities are aimed at improving Electronic government services internally, with other government partners, with business partners, and with the American public.

On October 1, 2008, the GSA began to transition from the E-Authentication Program Management Office hosted by the Federal Acquisition Service to an interagency governance model managed by the OGP. In so doing, E-Authentication became an integral part of the ICAM Program. One outcome of this move has been a transition away from a Federation model to an open model that promotes multiple agency solutions to comply with Office of Management and Budget (OMB) M-04-04 [2] and that encourages agency innovation. GSA's long-range vision for Identity management in government is a broad spectrum of solutions embracing open private sector solutions and high assurance, cybersecurity initiatives such as HSPD-12.

The Information Security and Identity Management Committee (ISIMC) is the Federal CIO Council's (FCIOC) locus of responsibility for cybersecurity and identity management. Comprised of senior agency officials, this committee has been assigned executive decision making authority and oversight for the ICAM roadmap and architecture development.

The high-level strategic goals and objectives for ICAM include:

1. Government-wide implementation of OMB M-04-04;
2. Physical Access Control;
3. Logical Access Control;
4. Consolidation of credentialing and authentication capabilities to comply with OMB M-06-22 [3]; and
5. Developing clearly defined processes and capabilities for enabling trust across the Federal government and between the Federal government and its external constituencies.

The goals of ICAM include:

1. Realizing cost-savings by eliminating agency legacy credential systems through use of standards-based authentication utilities;
2. Exploiting economies of scale by leveraging Federal buying power for both credentialing and credential validation functions;
3. Providing the capability to re-use credentials across applications, eliminating the need to create and maintain a credential system for each application; and
4. Improving the security and privacy posture of the Federal government.

It is in the government's best interest to leverage open identity management standards whenever possible. In order to ensure these standards are viable, robust, reliable, sustainable (e.g., available in commercial products), and interoperable as documented, the government requires processes to assess identity management standards and technology implementations against applicable federal requirements, policies, and statutes.

This document defines a process whereby the government can assess the efficacy of specific subsets of identity management standards (i.e., schemes) 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 technical interoperability will be achieved at a known level of assurance comparable to one of the four OMB Levels of Assurance.

2. INTRODUCTION

Critical to the success of the ICAM Program is the assessment and adoption of identity schemes that best serve the interests of the Federal government. 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 (i.e., an identity scheme 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, and secure. This confidence is essential to government-wide acceptance and use of ICAM.

3. ONGOING ACTIVITIES

This section specifies the process for adopting an identity scheme. Figure 3-1 depicts the general concept of identity scheme adoption, which is driven by industry standards, and Federal government policies and Profiles. OMB and the National Institute of Standards and Technology (NIST) are the primary authoritative bodies driving the applicable Federal government policies, standards, and policies. Figure 3-2 illustrates the high-level process flow to adopt a proposed identity scheme.

Figure 3-1 Identity Scheme Adoption Process

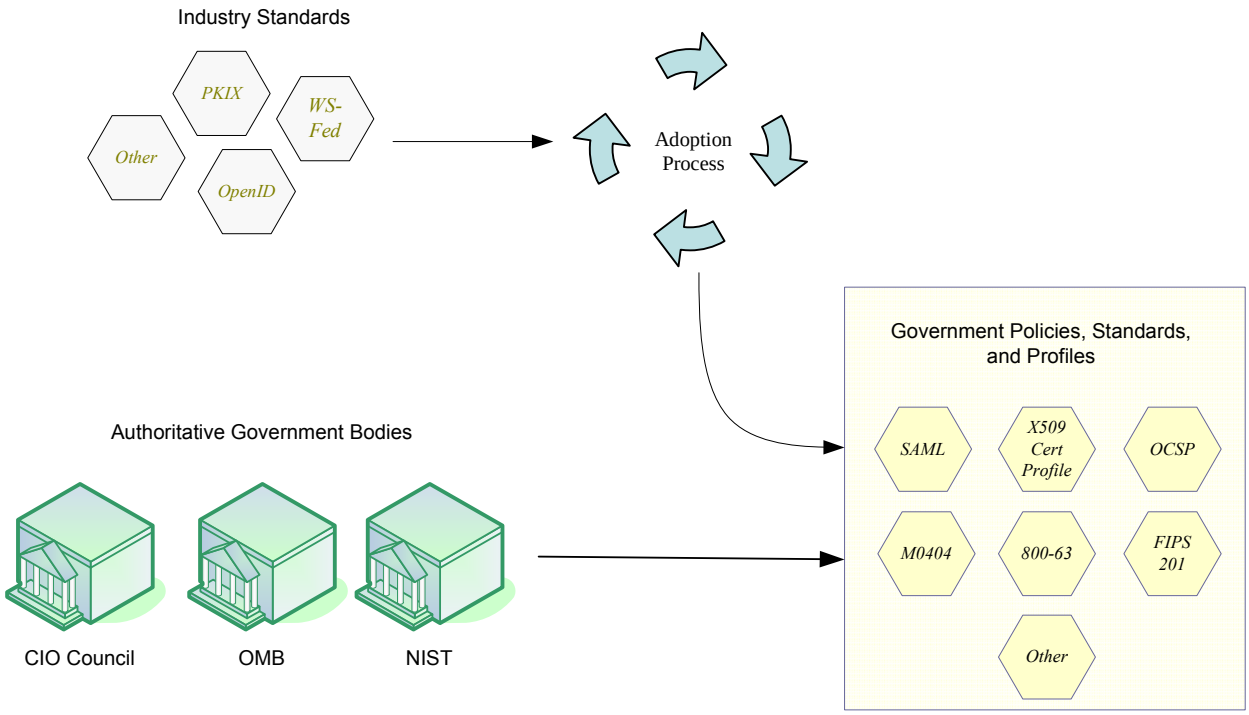
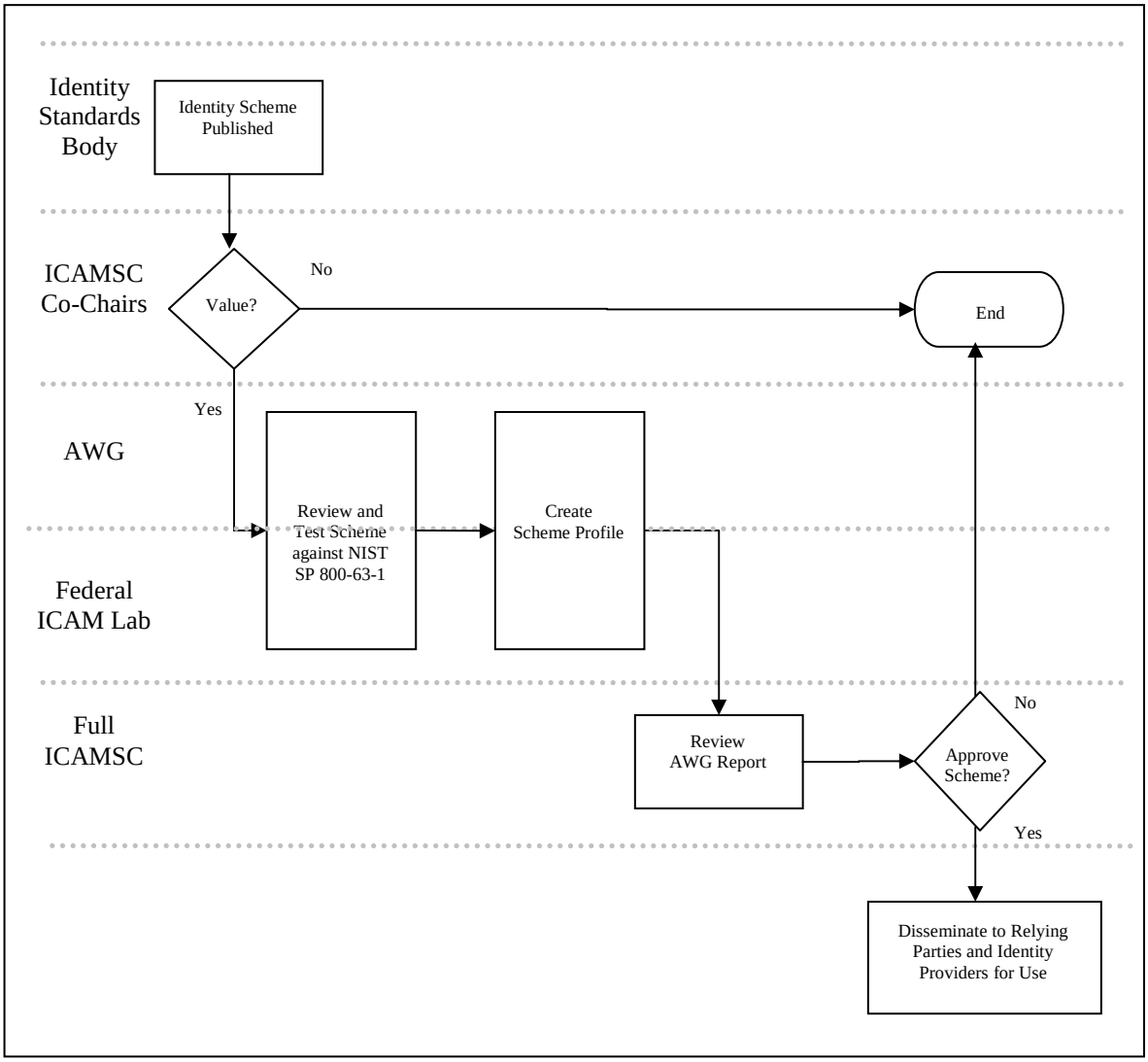


Figure 3-2High-Level Identity Scheme Adoption Process Flow



3.1 Value Determination

The ICAMSC Co-Chairs determine whether adoption of a published identity scheme would be valuable to Federal Agencies. In doing so, the Co-Chairs consider 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.

3.2 Standardization Review

Upon formal approval from the ICAMSC Co-Chairs, the Architecture Working Group Core Team (AWG) reviews 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). The AWG may request testing by the Federal ICAM Lab to determine the actual maturity of the identity scheme's interoperability.

If the assessment indicates the scheme is viable, the AWG creates a Scheme Profile, which defines how the Federal government will use the scheme. 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 AWG works closely with the Federal ICAM Lab 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 AWG delivers a Report to the Full ICAMSC.

3.3 ICAMSC Adoption Decision

The Full ICAMSC reviews the AWG Report on standardization of the identity scheme, and votes on whether to adopt the identity scheme. Upon adoption, the scheme is added to the Approved Identity Scheme List, Relying Parties and Identity Providers may be notified of the adoption as necessary, and the Scheme Profile can be used by the Federal government.

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), as requested by any ICAMSC member. 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, as requested by any ICAMSC member; and
- Other justifiable reasons as defined by the ICAMSC Co-Chairs.

5. 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 ICAMSC has responsibility for identity scheme adoption process maintenance. Draft revisions of this document will be made available to applicable Federal government agencies and organizations, including COTS vendors, for comment. Those comments will be provided to the ICAMSC before any final revision is approved. Any ICAMSC member can request revision to this document, as circumstances warrant.

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

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.

APPENDIX C - ACRONYMS

Acronym	Definition
AWG	Architecture Working Group
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
ICAMSC	Identity, Credential, and Access Management Sub Committee
ISIMC	Information Security and Identity Management Committee
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