U.S. E-Authentication Identity Federation Operational Standards

Business Owner: Federation Management
Creation Date: 12/26/2006
Last Updated: 9/15/2007
Version: EA-PR-0099-1.0.2-F
Audience: Public

GSA

Document History

Status	Release	Date	Comment	Audience
Draft	0.0.1	08/22/06	Document creation.	Limited
Draft	0.1.0	08/24/06	Submitted to PMO for review.	PMO
Draft	0.1.1	08/25/06	Made revisions based on comment from PMO.	Limited
Draft	0.2.0	08/28/06	Submitted to PMO for review.	PMO
Draft	0.2.1	08/30/06	Made revisions based on LWG meeting comments.	Limited
Draft	0.3.0	08/30/06	Submitted to PMO for review.	PMO
Draft	0.3.1	08/31/06	Made revisions based on PMO comments.	Limited
Draft	0.4.0	08/31/06	Submitted to PMO for review.	PMO
Draft	0.4.1	09/11/06	Made revisions based on RP & CSP Member Council meeting.	Limited
Draft	0.4.2	09/21/06	Made revisions based on comments received.	Limited
Draft	0.5.0	09/22/06	Submitted to PMO for review.	PMO
Draft	0.5.1	10/12/06	Made revisions based on comments received.	Limited
Draft	0.5.2	10/16/06	Made revisions based on PMO comments.	Limited
Draft	0.5.3	10/17/06	Made revisions based on comments received.	Limited
Draft	0.6.0	10/19/06	Submitted to PMO.	PMO
Draft	0.6.1	11/20/06	Made revisions based on LWG comments.	Limited
Draft	0.7.0	12/05/06	Submitted to PMO.	PMO
Draft	0.8.0	12/21/06	Includes comments from several agencies	Limited
Draft	0.8.2	12/22/06	Incorporates changes suggested by VA and DoED	Limited
Draft	0.8.3	12/26/06	Incorporated changes from PMO	Limited
Final	1.0.0	12/27/06	Ready for distribution	ESC, Members
Draft	1.0.1	7/9/07	Revisions necessitated by Architecture 2.0	Internal
Draft	1.0.2	9/15/07	Revisions per PMO comment	Internal

Editors

Georgia Marsh	Myisha Frazier-McElveen	Doug Hansen
Dave Silver	Chris Broberg	Steve Lazerowich
Kendra Brown		

Table of Contents

1 INTRODUCTION

1.1 Overview

Public trust in the security of information exchanged with or among Federal agencies over the Internet plays a vital role in the E-Government transformation. The U.S. E-Authentication Identity Federation (Federation) makes that trust possible. As part of the President's Management Agenda, the Federation enables trust and confidence in E-Government transactions through the establishment of an integrated policy and technical infrastructure for electronic authentication. Through the Federation, citizens and businesses will have simpler access to multiple Relying Parties (RPs) through the verification of Credentials and established identities. Furthermore, the Federation is comprised of RPs and Credential Services (CSs).

The E-Authentication concept is best described through the trust relationships among RPs, Credential Service Providers (CSPs), and End-Users. It is the management of trust among these entities (RP, CSPs and End-Users) that is the essence of the Federation.

1.2 Purpose and Scope

This document defines operational standards for Federation Members and E-Authentication Program Management Office (E-Auth PMO). The standards defined herein leverage both federally mandated standards and commercial best practices. In addition, the standards ensure that the best interests of the Federation, specifically the integrity of the operating environment, are maintained. This document is intended to improve the internal management of the Federal Government. It is not intended to confer any benefits or impose any obligations on the public. It does not create any right or benefit, substantive or procedural, enforceable at law against the RP, government agency CSP, the E-Auth PMO, their officers or employees, the Federal Government, or the public. It neither obligates nor requires any agency to obligate any agency appropriations. The sole and exclusive remedy for any failure on the part of a government agency to carry out its responsibilities as a member of the Federation will be the withdrawal of its authority by the E-Auth PMO to participate in the Federation. End-User requirements are to be provided by Federation Members and are not within the scope of this document.

1.3 Document Organization

The document organizes operational standards into specific categories (e.g., Security) and sub-categories (e.g., Security Standards, Logs). Each category lists relevant operational requirements, and indicates which ones must be complied with even after a Federation Member leaves the Federation (annotated as *Survivable Standard*). Where necessary, the document identifies additional standards and references the appropriate document.

2 SECURITY

2.1 Security Standards

The goal of the security standards is to achieve and maintain information availability, integrity, and confidentiality.

The security standards are intended to protect and secure Federation Member information assets and Systems from threats, whether internal or external, deliberate or accidental. These standards also aim to ensure that software, hardware, and procedural vulnerabilities are identified and mitigated before they can be exploited. The security standards are organized by subject and provided below.

2.1.1 Sensitive Information and Electronic Messaging

2.1.1.1* All Sensitive Information must be marked as *Sensitive Information* by the data/information owner, and the receiver must handle it accordingly unless otherwise specified by these Operational Standards.

2.1.1.2* Federation Members, their Contractors, and their Authorized Agents must employ security measures to safeguard Sensitive Information that is being stored, processed, transported, or disposed. These measures must be based on a risk assessment as provided in applicable NIST and OMB requirements, and apply to paper files, tape backups, call logs, mail messages and other media.

(* = Survivable Standard)

2.1.2 System Security

2.1.2.1 The servers utilized by Federation Members will not have the ability to remotely execute arbitrary outside requests, except for remote management performed by authorized individuals over an encrypted, authenticated channel.

2.1.2.2 For Internet exposed Systems providing services to the Federation, the following standards apply:

1. All routers used within Federation Member Systems are to be segmented to isolate Federation Member Network traffic from outside Network traffic; this segmentation should employ a packet filter that has been configured to disallow access to all protocols not approved by the Federation Member.
2. When a protocol (such as HTTP and HTTPS) is required to call into the Federation Member System, the inbound/outbound traffic must be permitted into the Federation Member's firewall.[1]
3. Federation Members must have and employ an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS).
4. Federation Members Systems must use an encryption Secure Socket Layer (SSL) certificate that is signed by a trusted root and is recognized by common web browsers to authenticate to the End-User web browsers. The E-Auth PMO recommends that the certificate be signed by a root level Certification Authority (CA) such as VeriSign, GeoTrust, or Thawte.
5. Assertion-based Federation Members must acquire certificate(s) from the E-Governance Certificate Authority (E-GCA) to secure the communications between Federation Member Systems, as appropriate for the adopted scheme. The certificate request(s) must be created utilizing a National Institute of Standards and Technology (NIST) approved Federal Information Processing Standard (FIPS) 140-2 cryptographic module and must follow the conventions identified in the Certificate Life-Cycle Methodology E-Governance Certificate Authorities document.

2.1.2.3* Federation Member Systems must enable logging and log sufficient information to provide for individual accountability of all access to, or attempts to access, the data stores that contain Sensitive Information.

2.1.2.4 Federation Member Systems storing or processing Sensitive Information must be stripped and configured with only enabled services and must have unnecessary and unused services disabled.

(* = Survivable Standard)

2.1.3 System Administration

2.1.3.1 When outside a firewall and attempting to access a Federation Member System root, strong authentication procedures (e.g., two-factor authentication such as use of Password and hard Token or a passcode and biometric System) are required.

2.1.3.2 Federation Members will ensure System Password strength is commensurate with the System's Assurance Level.

[1] NIST Special Publication 800-41, Guidelines on Firewalls and Firewall Policy

2.1.4 Physical Access Control

2.1.4.1	Federation Members must implement physical Access Controls to secure physical access to the location, computer room(s), computer equipment storing and processing Sensitive Information, including those locations managed by third parties.
2.1.4.2	Sensitive areas, such as data centers, must be physically protected on a continuous basis.
2.1.4.3*	Federation Member Systems storing or processing Sensitive Information must be physically secure and access must be granted to only authorized-personnel.
2.1.4.4	Access to Federation Member Systems by terminated and transferred employees must be revoked or disabled prior to or upon termination or transfer.
2.1.4.5*	All physical access to areas storing or processing Sensitive Information must be logged.
2.1.4.6	Federation Members must mitigate any breaches of its physical Access Controls immediately upon detection.

(* = Survivable Standard)

2.2 Logs

Federation Member Systems and applications are required to produce specific log records in order to maintain an acceptable level of security and consistency across the Federation. The following sub-sections describe Logging requirements.

2.2.1 General

2.2.1.1*	CSPs must keep related logs of transactions for at least five (5) years after the expiration of the Credential or longer in accordance with applicable federal, state, tribal, or local regulatory requirements.
2.2.1.2	RPs and CSPs must periodically analyze transaction logs for potential fraudulent activity.
2.2.1.3*	RPs must keep related logs of transactions for at least five (5) years or longer in accordance with applicable federal, state, tribal, or local regulatory requirements.
2.2.1.4*	Logs required by these standards must be backed up, including the use of an offsite storage location that has appropriate environmental and security controls.
2.2.1.5	Assertion-based Federation Members must have the ability to correlate local Session Identifiers (Sid) with associated authenticated transactions.
2.2.1.6*	RPs must be able to track the activity of End-Users from the receipt of external authentication through the end of the authentication transaction.
2.2.1.7	Federation Members must review their processes and controls to ensure that logs defined by these standards can support availability, legal sufficiency, reliability, and compliance with other laws for their system(s)[2].

[2] Additional information is available at http://www.usdoj.gov/criminal/cybercrime/eprocess.htm . Federation Members should also consider the significance of the "Electronic Records and Signatures in Global and National Commerce Act" (E-SIGN), as well as the affect of implementing OMB guidance.

2.2.1.8 All logs required by these standards must include a date and time stamp for every log entry.

(* = Survivable Standard)

2.2.2 Assertion-based Authentication –SAML Artifact Profile Interface Specification 1.0 and 1.0.1

2.2.2.1 Upon sending a Security Assertion Markup Language (SAML) Artifact, an Assertion-based CS must log the SAML Artifact.

2.2.2.2 Upon receiving a SAML Artifact, an Assertion-based RP must log the SAML Artifact.

2.2.2.3 Upon sending a SAML Assertion, an Assertion-based CS must log the following

- From the assertion:
  - AssertionID
  - IssueInstant
  - End-User Identifier (Uid)
  - Credential Service Identifier (CSid)
  - commonName
  - assuranceLevel
- RP Agency Application Identifier (AAid) being sent

2.2.2.4 Upon receiving a SAML Assertion, an Assertion-based RP must log the following:

- From the assertion:
  - AssertionID
  - IssueInstant
  - Uid
  - CSid
  - commonName
  - assuranceLevel
- RP AAid
- Assurance Level at time assertion is received

2.2.2.5 Upon a failed authentication, an Assertion-based CS must log the following:

- Authentication failure
- Token and Credential used by the End-User to authenticate

2.2.3 Assertion-based Authentication – SAML Artifact Profile Interface Specification 1.1

2.2.3.1 Upon sending a SAML Artifact, an Assertion-based CS must log the SAML Artifact.

2.2.3.2 Upon receiving a SAML Artifact, an Assertion-based RP must log the SAML Artifact.

2.2.3.3 Upon sending a SAML Assertion, an Assertion-based CS must log the following:

- From the assertion:
  - AssertionID
  - IssueInstant
  - Uid
  - CSid
  - commonName
  - assuranceLevel
  - specVer
  - Sid
- RP AAid being sent
- Transaction Identifier (Tid)

2.2.3.4 Upon receiving a SAML Assertion, an Assertion-based RP must log the following:

- From the assertion:
  - AssertionID
  - IssueInstant
  - Uid
  - CSid
  - commonName
  - assuranceLevel
  - specVer
  - Sid
- RP AAid
- Assurance Level at time assertion is received
- TID

2.2.3.5 Upon a failed authentication, an Assertion-based CS must log the following:

- Authentication failure
- Token and Credential used by the End-User to authenticate

2.2.4 Assertion-based Authentication – SAML 2.0 SSO Profile Using HTTP POST Interface Specification

2.2.4.1 Upon sending a SAML Assertion, an Assertion-based CS must log the following:

- From the assertion:
  - ID
  - IssueInstant
  - NameIdentifier
  - NameQualifier
  - Issuer
  - urn:oid:2.5.4.3
  - us:gov:e-authentication:basic:assuranceLevel
  - us:gov:e-authentication:basic:specVer
  - us:gov:e-authentication:basic:Sid

2.2.4.2 Upon receiving a SAML Assertion, an Assertion-based RP must log the following:

- From the assertion:
  - ID
  - IssueInstant
  - NameIdentifier
  - NameQualifier
  - Issuer
  - urn:oid:2.5.4.3
  - us:gov:e-authentication:basic:assuranceLevel
  - us:gov:e-authentication:basic:specVer
  - us:gov:e-authentication:basic:Sid
- Assurance Level at time assertion is received

2.2.4.3 Upon a failed authentication, an Assertion-based CS must log the following:

- Authentication failure
- Token and Credential used by the End-User to authenticate

2.2.4.4 Upon a failed digital signature verification, an Assertion-based CS must log the following:

- Digital signature verification failure
- From the SAML Message:
  - ID
  - IssueInstant
  - Issuer

2.2.4.5 Upon a failed digital signature verification, an Assertion-based RP must log the following:

- Digital signature verification failure
- From the SAML Message:
  - ID
  - IssueInstant
  - Issuer

2.2.5 Certificate-based Authentication

2.2.5.1 When authenticating an End-User, a Certificate-based RP must log the distinguished name of the certificate and whether authentication was successful.

3 SERVICE AGREEMENTS

3.1 Monitoring

To ensure that the System maintains availability, a certain level of monitoring must be performed. The following standards for achieving the level of monitoring necessary to maintain the Federation apply:

3.1.1 The E-Auth PMO will monitor the availability of Federation Member Systems and will contact members if an unscheduled outage or degradation of their service is identified.

3.1.2 CS Federation Members must achieve 99.9% availability of all services during scheduled operating times for systems made part of the Federation.

3.1.3 RP Federation Members must achieve 99% availability of all services during scheduled operating times for systems made part of the Federation.

3.2 Performance Requirements

Availability of the information technology systems of Federation Members is critical and this section provides the following Federation Member performance standards to assure Availability:

3.2.1 The recommended routine maintenance window requiring downtime for Federation servers is from 9 p.m. to 6 a.m. (Eastern Time (ET)) Monday through Friday and anytime on Saturday, Sunday, and Federal Holidays. Any maintenance downtime from 6 a.m. to 9 p.m. (ET) Monday through Friday, excluding Federal Holidays, must be coordinated through the E-Auth PMO.

3.2.2 Federation Members must notify the E-Auth PMO helpdesk (eauth.service.help@gsa.gov) of scheduled and unscheduled maintenance requiring downtime as soon as detected. For scheduled maintenance, where possible at least 30 days notice, but no less than 7 days notice.

3.2.3 The E-Auth PMO must ensure the Federation Portal (Portal) is continuously available 99.9% of the time.

3.2.4 The E-Auth PMO must ensure that E-GCA revocation data is continuously available 99.9% of the time.

3.2.5 The E-Auth PMO must ensure that Federal Public Key Infrastructure (FPKI) certificate revocation lists (CRLs) are continuously available 99.5% of the time, and are refreshed prior to individual expiration.

3.2.6 Federation Members will display a service unavailable web page during planned or unplanned service unavailability when practical.

4 OPERATIONAL AGREEMENTS

4.1 Metadata (Assertion Based only)

Metadata will be shared between Federation Members. The following standards apply:

4.1.1 Assertion-based Federation Members must make all Metadata[3] available to the E-Auth PMO which will share it with Connected Members and, if applicable, configure the Federation Portal accordingly.

4.1.2 Assertion-based Federation Member Systems must be configured with all necessary Metadata.

4.1.3 Assertion-based Federation Members must notify the E-Auth PMO of any planned Metadata changes no less than six (6) weeks in advance of the changes.

4.1.4 Assertion-based Federation Members must acknowledge the receipt of Metadata and respond within three (3) business days.

4.1.5 Assertion-based Federation Members must encode Metadata as required by the adopted scheme.

4.1.6 If required, Assertion-based Federation Members must sign Metadata as directed by the adopted scheme.

4.2 Configuration Management

The following configuration management standards apply:

4.2.1 System Changes

4.2.1.1 The E-Auth PMO must be notified thirty (30) days in advance of any changes that affect other Federation Member Systems.

4.2.2 Change Management

4.2.2.1 Federation Members must comply with the Federation Change Management Process.

4.3 System Configuration

When connecting to Compatible RPs and CSs, Federation Members must abide by the following standards:

4.3.1 SAML connections must be established between assertion-based CSs and new Compatible RPs of the Federation within ninety (90) days of the new Compatible Federation RP going live.

4.3.2 SAML connections must be established between assertion-based RPs and new Compatible CSPs of the Federation within ninety (90) days of the new Compatible Federation CSP going live.

[3] SAML 2.0 metadata elements are defined in the E-Authentication Federation Architecture 2.0 Interface Specifications. Contact the PMO for SAML 1.0 metadata elements.

4.3.3 Within ninety (90) days of the new Certificate-based Compatible Federation CS going live, a Certificate-enabled RP must establish validation capabilities for those PKI certificates issued by the new CSP.

4.4 Optional Attributes (Assertion Based only)

The ASC Technical Suite states attributes of the SAML assertion that are optional. The following standards are not optional:

4.4.1 Before going live, Assertion-based CSPs must notify the E-Auth PMO of which attributes they are willing and able to assert.

4.4.2 The E-Auth PMO will provide Assertion-based RPs with information about what attributes each Assertion-based CSP submits.

4.4.3 Assertion-based CSs are prohibited from sending SAML Assertions that contain attributes that the RP cannot receive.

4.4.4 The E-Auth PMO must maintain records of the capabilities and restrictions related to optional attributes in the Federation.

4.5 Add-on Services

The ASC Technical Suite provides a mechanism for additional services to be added to the trust relationship established between Federation Members[4]. The following standards apply for any of these additional services:

4.5.1 Federation Members must notify the E-Auth PMO of the existence and nature of add-on services.

4.5.2 Add-on services must adhere to the E-Authentication architecture, governance, and standards. They will also adhere to the same laws and policies governing the architecture.

4.6 Time Synchronization

For security and operational purposes, it is important that each Federation System have time synchronization. The following standard applies:

4.6.1 Federation Member Systems must run time synchronization software.

[4] This is accomplished through the use of the session identifier (Sid) field in the assertion.

APPENDIX A: ACRONYMS

Acronym	Definition
AAid	Agency Application Identifier
ASC	Authentication Service Component
CA	Certification Authority
CCB	Change Control Board
CRL	Certificate Revocation List
CS	Credential Service
CSid	Credential Service Identifier
CSP	Credential Service Provider
E-Auth PMO	E-Authentication Program Management Office
E-GCA	E-Governance Certificate Authority
ET	Eastern Time
FIPS	Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
GSA	General Services Administration
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
RP	Relying Party
SAML	Security Assertion Markup Language
Sid	Session Identifier
SSL	Secure Socket Layer
Tid	Transaction Identifier
Uid	End-User Identifier