E-Authentication Federation Operational Standards

Version 1.0.0
12/26/06

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

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-Gov transformation. The General Services Administration's (GSA's) E-Authentication Federation makes that trust possible. As part of the President's Management Agenda, the E-Authentication 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

This document defines operational standards for Federation Members. The standards defined herein leverage both Federally-mandated standards and commercial best practices and 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 E-Authentication Federation will be the withdrawal of its authority by [insert entity or method] 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

This document provides specific areas that a Federation Member must implement. The document is organized in to specific standards and for each subject. Where necessary, additional standards are identified by reference and the appropriate document is listed.

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.

2.1.1.3* 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 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 provide a Federation Member's Network traffic in isolation from outside Network traffic; this segmentation should employ a packet filter which 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. Assertion-based Federation Members must use an encryption Secure Socket Layer (SSL) certificate, that is signed by a trusted root and is recognized by common web browsers, to secure the communications between Federation Member Systems. The E-Auth PMO recommends that the certificate be signed by a root level Certification Authority (CA) such as VeriSign, GeoTrust, or Thawte.
5. As necessary Federation Members must acquire a server certificate from the E-Governance Certificate Authority (E-GCA). The server certificate request 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 & hard Token or a passcode & biometric System) are required.

[1] NIST SP 800-41 – Guidelines on Firewalls and Firewall Policy

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

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 continuously.

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 will need to produce particular log records. To maintain a level of security and consistency across the Federation, the following standards apply:

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 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 after 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].

2.2.1.8 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 – Architecture 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] 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) (Pub.L. 106-229, June 30, 2000, 114 Stat. 464, codified at 15 U.S.C. §§ 7001 -- 7006), and implementing OMB guidance.

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 – Architecture 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 Certificate-based Authentication

2.2.4.1 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 Credential Service Federation Members must achieve 99.9% availability of all services during scheduled operating times for systems made part of the Federation. Relying Party 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.

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 configure the Portal accordingly.

4.1.2 Assertion-based Federation Member Systems must be configured with both E-Authentication and scheme specific 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.

4.2 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 Federation Change Management Policy.

4.3 System Configuration

When connecting to Compatible RPs and CS, 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 completing the Federation Boarding Process.

[3] Metadata elements are defined in the E-Authentication Interface Specification.

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 completing the Federation Boarding Process.

4.3.3 Within ninety (90) days of the new PKI-based Compatible Federation CSP completing the Federation Boarding Process, a PKI-enabled RP must establish validation capabilities for those PKI certificates issued by the new CSP

4.4 Optional Attributes (Assertion Based only)

The 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 in regard to 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 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: Glossary

Some terms used in these Operational Standards have commonly accepted definitions, and therefore are not defined in the Glossary.

Term	Definition
Access Control	Mechanisms, methods and policies that restrict access to information systems and/or facilities.
Agency Application Identifier (AAid)	Mechanism used to identify a RP System within the Architecture Service Component (ASC).
Approved	Acceptance by the E-Auth PMO to participate in the E-Authentication Federation, or other inclusion or use in the E-Authentication Federation.
Assertion-based (Assertion-based Authentication)	PIN or Password based authentication, where End-Users authenticate to a selected CS, which in turn asserts the End-User identity to the appropriate RP.
Assurance Level	Level of trust, as defined by Office of Management and Budget (OMB) Guidance for E-Authentication (M-04-04). This guidance describes four identity authentication Assurance Levels for E-Government transactions. Each Assurance Level describes the agency's degree of certainty that the user has presented an identifier (a Credential in this context) that refers to his or her identity. In this context, assurance is defined as 1) the degree of confidence in the *vetting process* used to establish the identity of the 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 four levels of assurance are: Level 1: Little or no confidence in the asserted identity's validity. Level 2: Some confidence in the asserted identity's validity. Level 3: High confidence in the asserted identity's validity. Level 4: Very high confidence in the asserted identity's validity.
Authentication	The process of establishing confidence in user identities.
Authentication Service Component (ASC)	A common infrastructure for electronically authenticating the identity of End-Users of E-Government services. The ASC accomplishes this by leveraging Credentials from multiple CSPs through certifications, guidelines, standards adoption and policies – which is the basis of trust for Federation Credentials.
Authorized Agent	Persons selected by a RP or CSP to provide services in regard to the E-Authentication Federation.

Term	Definition
Availability	The security goal that generates the requirement for protection against— • Intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data • Unauthorized use of system resources.
Boarding Process	Includes all the activities involved in converting a Federation Member candidate into an official Federation Member. It includes verification that all applicable agreements and standards have been satisfied or waived, acceptance testing to ensure interface specification compliance, change control board (CCB) approval of member system integration, and CCB recommendation of the member candidate's request for a production E-GCA certificate.
Certificate-based (Certificate-based Authentication)	X.509v3 digital certificate based authentication in a public key infrastructure (PKI). CAs issue certificates to End-Users, and End-Users present their certificates to applicable RPs for authentication.
Certification Authority (CA)	Issues PKI certificates to End-Users for the purposes of authenticating to RPs.
Compatible	Two Federation Members are considered Compatible if: 1. the CS has an equal or higher identity Assurance Level, as defined by OMB M-04-04, “E-Authentication Guidance for Federal Agencies,” than the RP; 2. the CS provides all attributes required by the RP in accordance with the requirements of the Technical Suite, which is cited in the E-Authentication Federation Governance document; and 3. the CS and RP can communicate directly, or indirectly through an E-Auth PMO-provided service, in accordance with the requirements of the Technical Suite, which is cited in the E-Authentication Federation Governance document.
Confidentiality	The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and in transit.
Connected Members	Federation Members that have directly connected one or more of their Systems to allow SAML exchanges. Every Member of the Federation is not connected to every other Federation Member, for example CSs are not connected to other CSs, higher Risk RPs are not connected to lower assurance CSs, etc.

Term	Definition
Contractor	Person that is under contract to provide a Federation Member with services, supplies, or other needs.
Credential	Digital documents used in authentication that bind an identity or an attribute to a subscriber's Token. This document uses "Credential" broadly, referring to both electronic Credentials and Tokens.
Credential Service (CS)	Creates, maintains, and manages identity information for End-Users, and may provide End-User authentication to RPs. A CS is also considered a CA when it issues PKI certificates for use by the Federation.
Credential Service Identifier (CSid)	Mechanism used to identify a CSP System (i.e., CS) within the ASC.
Credential Service Provider (CSP)	Organizations (commercial or government) that provide the Federation with identity management services.
E-Authentication Federation (Federation)	A public-private partnership that enables citizens, businesses and government employees to access online government services using credentials issued by trusted third-parties, both within and outside the government.
E-Authentication Program Management Office (PMO)	Established by GSA to manage the Federation on an ongoing, day-to-day basis.
E-Governance Certificate Authority (E-GCA)	Established by the government to issue certificates that allow RPs to retrieve SAML Assertions from CSs over a client and server authenticated SSL channel, effectively controlling which entities can participate.
End-User	Any individual or person (including, but not limited to states, tribes, local governments, business, or non-profit organizations) that authenticates to a RP using a Credential issued by a CS.
Federation Change Management	Policies and processes agreed to by Federation Members to review, approve, and roll out architecture changes to production.
Federation Member	Federation Members are business entities or government organizations (RPs and CSPs), that sign an agreement with the E-Auth PMO to participate in the Federation.
Federation Portal (Portal)	A website that helps End-Users locate the CSs and RPs they need to complete their transactions.

Term	Definition
Integrity	The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).
Metadata	Information necessary for Federation Member Systems to technically interoperate. It may encompass: • E-Authentication specific information– scheme-independent information pertaining to E-Authentication Federation Members (e.g., CSid) and E-Authentication policies (e.g., Assurance Levels, issuers, client/server certificates) • Scheme specific information – information that directly supports technical interoperability for a scheme. Some or all of the information for a scheme may be used for a different scheme.
Network	An open communications medium, typically the Internet, that is used to transport messages between parties. Unless otherwise stated, Networks are assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking…) and passive (e.g., eavesdropping) attacks at any point between the parties.
Operational Standards	Day-to-day technical practices and policies Federation Members and the E-Auth PMO agree upon in order to ensure Federation security, consistency, and service standards.
Password	A secret that is used to authenticate an End-User. Passwords are typically character strings that may consist of letters, numbers, and/or symbols.
Relying Party (RP)	A department, agency, government sponsored corporation, or other organization, or any state, tribal or local government that provides online services requiring End-User authentication. A RP is also referred to as a Federation Member System (Internet based) that takes action based on identity information from a trusted Federation Member System (i.e., CS).
Risk	Risk is a function of the likelihood that a given threat-source will exploit a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

Term	Definition
Scheme Translator	Supports interoperability among different authentication schemes by translating between CSs and AAs using different schemes. A scheme translator may be called a Step Down Translator when used to translate from certificate schemes to assertion schemes.
Security Assertion Markup Language (SAML)	XML-based framework for ensuring that transmitted communications are secure. SAML defines mechanisms to exchange authentication, authorization and nonrepudiation, allowing single sign-on capabilities for Web services.
Security Assertion Markup Language (SAML) Artifact	A SAML Artifact is carried as part of a URL query string such that, when the artifact is conveyed to the source site, the artifact unambiguously references an assertion. The artifact is conveyed via redirection to the destination site, which then acquires the referenced assertion by some further steps. Typically, this involves the use of a registered SAML protocol binding. This technique is used in the browser/artifact profile of SAML.
Security Assertion Markup Language (SAML) Assertion	A statement from a verifier to a relying party that contains identity information about a subscriber. SAML Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol.
Sensitive Information	Information that requires protection from unauthorized access, modification, disclosure or destruction.
Session Identifier (Sid)	Mechanism for indicating to the RP that there is data available for transfer.
Survivable Standard	A standard that a Federation Member must abide by after leaving the Federation.
System	A Federation Member's web-based application that has been Approved by the E-Auth PMO to participate in the Federation.
Token	An item that the End-User possesses and controls (typically a key or Password) used to authenticate the claimant's identity.
Transaction Identifier (Tid)	Mechanism for tracking transactions across various components in the architecture. TIDs will be generated by the Portal, and will be passed with the End-User, via query string, as they are redirected from (1) the Portal to CSs, (2) from CSs to RPs, and, (3) once generated by the Portal, to the Portal by RPs or CSs.

APPENDIX B: 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 PMO
E-GCA	E-Governance Certificate Authority
ET	Eastern Time
FIPS	Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
GSA	General Services Administration
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