E-Authentication Federation Architecture 2.0
Interface Specifications

Version 1.0.0
Final
May 4, 2007

Document History

Status	Release	Date	Comment	Audience
Template	0.0.0	1/18/06	Outline	PMO
Draft	0.0.1	1/19/07	Initial draft	Internal
Draft	0.0.2	2/14/07	Updates per internal review	Internal
Draft	0.0.3	2/19/07	Updates per internal review	Internal
Draft	0.0.4	2/21/07	Updates per internal review	Red Team
Draft	1.0.0 RC1	3/2/07	Updates per Red Team	PMO
Draft	1.0.0 RC2	3/30/07	Updates per public comment	PMO
Draft	1.0.0 RC3	4/20/07	Updates per public comment	Internal
Final	1.0.0	5/4/07	Updates per PMO and Enspier comments	Public

Editors

Terry McBride	Matt Tebo	Dave Silver
Treb Farrales	Steve Lazerowich	Chris Louden

GSA

Document Introduction

As part of the President's Management Agenda, the U.S. E-Authentication Identity Federation (Federation) enables trust and confidence in E-Government transactions via integration of policy and technical infrastructure for electronic authentication. The result is the Authentication Service Component (ASC). The ASC is a federated architecture strategically designed to support different identity assurance schemes simultaneously. Some schemes support assertion-based authentication (i.e., authentication of PIN and Password credentials), while other schemes support certificate-based authentication directly to the relying party (RP) (i.e., authentication of Public Key Infrastructure (PKI) digital certificates).

Adopted schemes are different from one another. Accordingly, each adopted scheme has its own specification for ASC use. At a minimum, the specifications address (a) high-level ASC transaction flows, and (b) governance. One should not assume that topics discussed for one adopted scheme (e.g., features, use cases, transaction protocols, governance) apply to other adopted schemes.

By integrating with the ASC using an interface specification defined herein, Federation members use a standard approach for authentication, rather than building or maintaining an authentication structure of their own.

This document is part of the ASC technical suite, which also includes the Technical Approach for the Authentication Service Component and E-Authentication Interface Specifications (including one for SAML 2.0 SSO Using HTTP POST as an adopted scheme). For complete comprehension, please read this document after the Technical Approach and prior to applicable Interface Specifications.

Figure 1-1 shows the documentation relationships for E-Authentication. The current version of each E-Authentication document is available on the Federation website at http://www.cio.gov/eauthentication.

Figure 1-1 E-Authentication Document Hierarchy

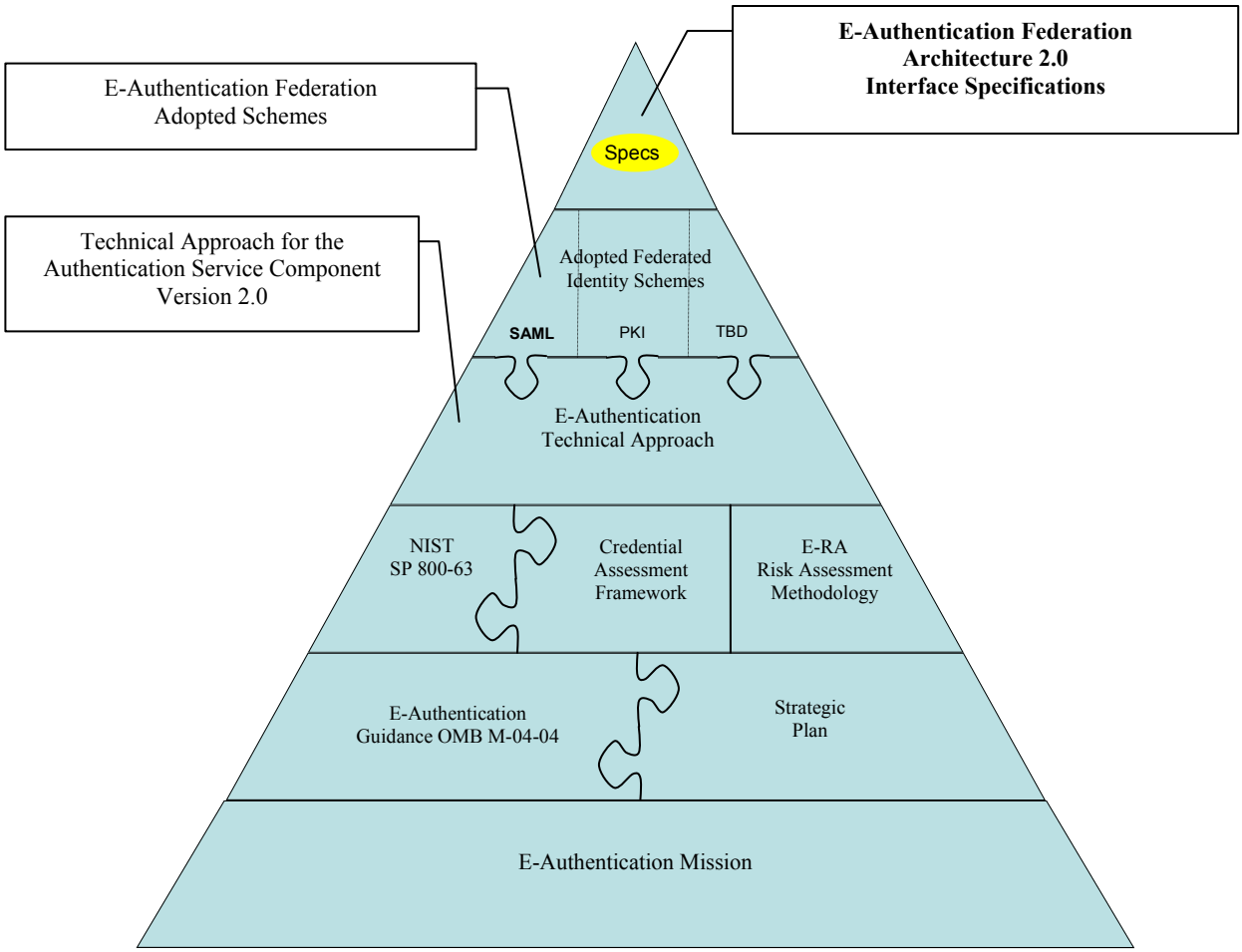

Table of Contents

Figures

Tables

1 INTERFACE SPEC: SAML 2.0 SSO PROFILE USING HTTP POST

1.1 Introduction

Security Assertion Markup Language (SAML) 2.0 Single Sign-on (SSO) Profile Using Hypertext Transfer Protocol (HTTP) POST is one of the schemes adopted by the E-Authentication Program Management Office (PMO) and supported by the ASC. The SAML protocol facilitates exchange of SAML messages (requests and/or responses) between endpoints resulting in delivery of an identity assertion regarding an act of authentication and attribute information about the authenticated end user. In E-Authentication, the endpoints are the RP and the credential service (CS). The CS sends the assertion. The RP receives the assertion.

1.2 Purpose

This interface specification provides guidance on how to use SAML 2.0 SSO Profile using HTTP POST specifically for Federation purposes. This interface specification does not revise or extend the Organization for the Advancement of Structured Information Standards (OASIS) SAML 2.0 specification. Rather, it simply details how the Federation must use SAML 2.0 for Federation purposes. Where this specification does not explicitly provide SAML guidance, one must implement in accordance with SAML 2.0 requirements as documented by the OASIS standards body.

1.3 Document References

[SAML2 Core] "Assertions and Protocol for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005.
Document Identifier: saml-core-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SAML2 Bindings] "Bindings for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005. Document Identifier: saml-bindings-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

[SAML2 Profiles] "Profiles for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005. Document Identifier: saml-profiles-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[SAML2 Metadata] "Metadata for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005.
Document Identifier: saml-metadata-2.0-os http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[SAML2 Context] "Authentication Context for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005.
Document Identifier: saml-authn-context-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

[SAML2 Conform] "Conformance Requirements for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005.
Document Identifier: saml-conformance-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf

[SAML2 Security] "Security and Privacy Considerations for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005. Document Identifier: saml-sec-consider-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf

[SAML2 Glossary] "Glossary for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005. Document Identifier: saml-glossary-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf

[Adopted Scheme] E-Authentication Federation Adopted Schemes, Version 1.0.0
http://www.cio.gov/eauthentication/TechSuite.htm

[CAF] Credential Assessment Framework
http://www.cio.gov/eauthentication/CredSuite.htm

[E-GCA CP] "X.509 Certificate Policy for the E-Authentication Certification Authorities", Version 1.0, September 29, 2004
http://www.cio.gov/fpkipa/documents/EGovCA-CP.pdf

[FISMA] Federal Information Security Management Act
http://csrc.nist.gov/sec-cert/

[FMD] Federation Membership Documents
http://www.cio.gov/eauthentication

[NIST SP 800-52] Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; National Institute of Science and Technology (NIST Special Publication 800-52
http://csrc.nist.gov/publications/nistpubs/

[NIST SP 800-63] Electronic Authentication Guideline; National Institute of Science and Technology (NIST Special Publication 800-63
http://csrc.nist.gov/publications/nistpubs/

[OMB M-04-04] E-Authentication Guidance for Federal Agencies, Office of Management and Budget (OMB) Memorandum M-04-04
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[OMB M-03-22] OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Office of Management and Budget (OMB) Memorandum M-03-22
http://www.whitehouse.gov/omb/memoranda/m03-22.html

[RFC 2459] "RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile", Internet RFC/STD/FYI/BCP Archives).
http://www.ietf.org/rfc/rfc2459.txt

[Tech Approach] Technical Approach for the Authentication Service Component, Version 2.0.0
http://www.cio.gov/eauthentication/TechSuite.htm

[XML Datatypes] XML Schema Part 2: Datatypes Second Edition, W3C
http://www.w3.org/TR/xmlschema-2

[XML Enc] XML – Encryption Syntax and Processing, W3C Recommendation 10 Dec 2002
http://www.w3.org/TR/xmlenc-core/

[XML Sig] XML – Signature Syntax and Processing, W3C Recommendation 12 Feb, 2002
http://www.w3.org/TR/xmldsig-core/

1.4 Reference Links

Topic	Link
SAML	http://www.oasis-open.org/home/index.php http://www.oasis-open.org/specs/index.php#samlv2.0 http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security http://www.oasis-open.org/committees/security/docs
XML	http://www.w3.org http://www.w3.org/XML/ http://www.w3.org/1999/XMLSchema-instance http://www.w3.org/1999/XMLSchema

1.5 Notation

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in IETF RFC 2119 [RFC 2119].

1.6 General Approach

This specification builds upon the SAML 2.0 suite of specifications. It further specifies usage of particular features, elements, attributes, URIs, or other values that are required within the Federation.

For purposes of this document, Transport Layer Security (TLS) includes Secure Sockets Layer V3.0[1].

This document specifies all Federation required and Federation optional attribute data types in accordance with [XML Datatypes].

Where this specification does not explicitly provide SAML guidance, one must implement in accordance with applicable OASIS SAML 2.0 requirements (see Section 1.3).

[1] Use of SSLv3.0/TLS must be compliant with Federal guidelines (e.g., FIPS 140-2, FIPS 180-2, NIST SP 800-52) and agency policies.

1.7 Authentication

1.7.1 Displaying Partners

- Every RP and CS MUST provide a link the end user can select to initiate Federation processing.
- When an end user arrives at an RP without an `<Assertion>` and a common domain cookie (see Section 1.8) is present but does not contain the ID of a compatible CS, the RP MUST display a list of compatible CSs from which the end user can select.
- Upon end user selection of a CS, the RP MUST initiate an `<AuthnRequest>` to the selected CS (see Section 1.7.2).
- When an end user arrives at a CS without an `<AuthnRequest>`, the CS MUST display a list of compatible RPs from which the end user can select.
- Upon end user selection of an RP, the CS MUST send an unsolicited `<Response>` that includes an `<Assertion>` to the selected RP (see Section 1.7.3).
- The CS MAY list specific RP resources (e.g., RP applications) for which it knows the URL.

1.7.2 Authentication Request

- The RP MUST form an `<AuthnRequest>` in accordance with SAML 2.0 Web Browser SSO Profile[2].
- `<AuthnRequest>` MUST be communicated using the HTTP Redirect Binding[3].
- `<AuthnRequest>` MUST be signed by the RP to ensure message integrity and to authenticate the RP to the CS.
- `<AuthnRequest>` MUST be communicated to the end user browser over Transport Layer Security (TLS) and delivered to the SSO Service of the CS using TLS port 443.
- Certificates used to protect the TLS channel MUST be trusted by default in commonly used browsers.

`<Issuer>`

- `<Issuer>` MUST be present and its value MUST be the identifier of the RP.
- `<Issuer>` MUST be agreed upon between the RP and the Federation.
- `<Issuer>` MUST be a URL reference within the RP domain.

`ProtocolBinding`

- If present, `ProtocolBinding` attribute MUST be urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST.

`<RequestedAuthnContext>`

- The authentication request MAY include `<RequestedAuthnContext>`.
- If `<RequestedAuthnContext>` present, `Comparison` attribute MUST be set to minimum.

[2] [SAML2 Profiles], Section 4.1
[3] [SAML2 Bindings], Section 3

IsPassive

- IsPassive MAY be used if the RP does not wish for the CS to take direct control of the end user's browser (i.e., show the end user a page).
- If IsPassive is true, the end user MUST be able to authenticate in some passive manner, otherwise the resulting response MUST NOT contain an <Assertion>.

This feature allows the RP to determine whether it should alert the end user that he or she is about to interact with the CS. Examples of passive situations include:

- The end user having an active session at the CS.
- The end user presenting an X.509v3 certificate over mutually authenticated TLS.

<NameIDPolicy>

- <NameIDPolicy> MAY contain AllowCreate attribute.
- In general, AllowCreate will be set to true so that if the end user has never used the selected CS to access the RP, an end user identifier common to the CS/RP pair can be created, and SAML messages can be exchanged between the parties.
- However, AllowCreate may be useful if the RP wishes to determine in advance whether the end user has federated their identity between the CS and RP.
- If Format present it MUST be urn:oasis:names:tc:SAML:2.0:nameid-format:persistent or urn:oasis:names:tc:SAML:2.0:nameid-format:transient.

1.7.2.1 Session Reset

When an end user has an extended session with or has been inactive at the RP for some time, the RP may wish to refresh the authentication of the end user. In that case:

- The RP MAY issue an <AuthnRequest> with ForceAuthn set to true.
  - If IsPassive present, it MUST be set to false.

ForceAuthn

- ForceAuthn MAY be used to require the CS to force the end user to authenticate to the CS regardless of the end user's authentication session status at the CS.

1.7.3 Authentication <Response>

Whether responding to an <AuthnRequest> from the RP, or sending an unsolicited response:

- The CS MUST create a <Response> in accordance with the SAML 2.0 Web Browser SSO Profile[4].
- <Response> MUST be communicated using the HTTP POST Binding[5].
- <Response> MUST be communicated to the browser over TLS and delivered to the RP's <Assertion> Consumer Service over TLS.
- Certificates used to protect the TLS channel MUST be trusted by default in commonly used browsers.

[4] [SAML2 Profiles], Section 4.1
[5] [SAML2 Bindings], Section 3.5

RelayState

- If an unsolicited assertion, the CS MAY include the URL of an RP resource (i.e., RP application) selected by the end user in the `RelayState` form field parameter.

Version

- `Version` attribute MUST be set to "2.0".

Consent

- If present, value of `Consent` MUST be one of the following:
  - urn:oasis:names:tc:SAML:2.0:consent:obtained
  - urn:oasis:names:tc:SAML:2.0:consent:prior
  - urn:oasis:names:tc:SAML:2.0:consent:current-implicit
  - urn:oasis:names:tc:SAML:2.0:consent:current-explicit
  - urn:oasis:names:tc:SAML:2.0:consent:unspecified

<EncryptedAssertion>

- Each <Response> MUST contain no more than one <EncryptedAssertion>.

1.7.3.1 <Assertion>

After all processing rules have been completed in accordance with the SAML 2.0 specifications, and the CS is satisfied that an <Assertion> can be made about the end user:

- The CS MUST create <Assertion>.
- <Assertion> MUST be signed, encrypted, and included in the <Response> within <EncryptedAssertion>

Version

- `Version` attribute MUST be set to "2.0".

<Issuer>

- <Issuer> MUST be present and its value MUST be the identifier of the CS.
- The identifier MUST be agreed upon between the CS and the Federation.
- <Issuer> MUST be a URL reference within the domain of the CS.

<Subject>

- There MUST be exactly one <Subject> per <Assertion>.

1.7.3.2 <Subject>

- Each <Assertion> MUST contain exactly one <Subject> indicating the end user to which <Assertion> pertains.

<NameID>

- <NameID> within <Subject> MUST contain a `Format` attribute set to urn:oasis:names:tc:SAML:2.0:nameid-format:persistent or urn:oasis:names:tc:SAML:2.0:nameid-format:transient unless the PMO approves otherwise.

1.7.3.3 <AuthnStatement> Element

SessionIndex

- <AuthnStatement> MUST include the SessionIndex of the end user so that the CS can perform single logout (SLO) for that session.
- SessionIndex SHOULD NOT be used to track an end user from RP to RP.
  - Federation members SHOULD use the measures suggested in [SAML2 Core].

SessionNotOnOrAfter

- <AuthnStatement> MAY contain SessionNotOnOrAfter.
- If present, RP is NOT REQUIRED to honor SessionNotOnOrAfter.

1.7.3.4 <AttributeStatement> Element

- The CS MUST send exactly one <AttributeStatement> to an RP during the first transmission of an <Assertion> for a particular <Subject>.
- Each subsequent <Assertion> MUST contain no more than one <AttributeStatement>.
- Each <Attribute> MUST NOT be encrypted.

<Attribute>

- If present, NameFormat of <Attribute> MUST be one of the following:
  - urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified
  - urn:oasis:names:tc:SAML:2.0:attrname-format:uri
  - urn:oasis:names:tc:SAML:2.0:attrname-format:basic
- The actual Name MUST be a URI.
- The optional attribute FriendlyName MAY be used to provide a human readable label for the attribute.
- Where the definition of an attribute includes one or more descriptors for the attribute, FriendlyName, if present, MUST be one of the defined descriptors.

1.7.3.4.1 Required Attributes

Table 1-1 lists attributes that MUST be present whenever <AuthnStatement> accompanies <AttributeStatement>.

Table 1-1 Federation Required Attributes

Name (URI)	Description	Format	Datatype
us:gov:e-authentication:basic:assuranceLevel	The confidence level of the end user's identity proofing and authentication mechanism	MUST be one of 1, 2, 3, 4, or test	xs:string
urn:oid:2.5.4.3	The displayable full name of the end user. In the case of assurance level 1 this may be a pseudonym.	First name followed by optional middle name or initial followed by last name delimited by spaces. MUST be <=256 characters in length.	xs:string
us:gov:e-authentication:basic:specVer	The version of the interface specification	MUST be "2.0" for this interface specification	xs:string

1.7.3.4.2 Optional Attributes

The Federation takes a dynamic approach to optional attributes to provide a richer attribute set to end users. Table 1-2 shows Federation optional elements. Optional attributes MAY be set with blank values.

Table 1-2 Federation Optional Attributes

Name (URI)	Description	Format	Datatype
urn:oid:2.5.4.4	The last name of the end user	MUST be <=128 characters in length	xs:string
urn:oid:2.5.4.42	The first name of the end user	MUST be <=128 characters in length	xs:string
urn:oid:1.3.6.1.4.1.1466.101.120.34	The middle name of the end user	MUST be <=128 characters in length	xs:string
urn:oid: 2.5.4.44	The end user's generation qualifier (e.g., "Jr.", "3rd", "IV")	MUST be <=20 characters in length	xs:string
us:gov:e-authentication:basic:PSSN	The last four digits of the end user's social security number	MUST be 4 digits	xs:integer
us:gov:e-authentication:basic:birthMonth	The month of the end user's birth	MUST be 2 digits MUST contain a value in the range of 01 - 12	xs:integer
us:gov:e-authentication:basic:birthDay	The day of the end user's birth	MUST be 2 digits MUST contain a value in the range of 01 – 31, as appropriate for birthMonth	xs:integer
us:gov:e-authentication:basic:birthYear	The year of the end user's birth	MUST be 4 digits (yyyy)	xs:integer
us:gov:e-authentication:basic:address1	The first line of the end user's physical address of record	MUST be <= 50 characters in length	xs:string
us:gov:e-authentication:basic:address2	The second line of the end user's physical address of record	MUST be <= 50 characters in length	xs:string
urn:oid:2.5.4.7	The end user's city for the physical address of record	MUST be <= 28 characters in length	xs:string
urn:oid:2.5.4.8	The end user's state for the physical address of record	MUST be 2 character length state code	xs:string
urn:oid:2.5.4.17	The end user's zip code for the physical address of record	MUST be either 5 digit format or 5digit-4digit (including the dash) format	xs:string
us:gov:e-authentication:basic:Sid	Session Identifier established by the CS to identify the end user's session at the CS	MUST be <= 128 characters in length	xs:string

1.8 IdP Discovery Profile (Single Sign On)

- As IdP Discovery Profile uses a common domain, RPs and CSs MUST have access to a common domain cookie (CDC)[6].
- All Federation members MUST have a CDC Service within the eauthentication.gsa.gov domain.
- The CS MUST redirect the end user to its CDC writing service prior to transferring the end user to an RP.
- The CDC MUST NOT persist past the closing of the end user's browser.
- As it is possible that an end user uses more than one CS, the CDC MAY indicate more than one CS. See [SAML2 Profiles] for more detail.
- When an unauthenticated end user arrives at an RP, the RP MUST redirect the end user to its CDC read service.
  - If a CDC exists, the RP MUST present a tailored list of compatible CSs featuring, at a minimum, compatible CS(s) in the CDC.
  - If no CDC exists, the end user MAY select a link whereupon the RP MUST present a list of compatible CSs.

1.9 Single Logout Profile

The SLO protocol provides a means by which an authentication session and all associated RP sessions (i.e., initiated through that authentication session) can be terminated near-simultaneously.

- The RP MUST offer the end user a choice between simple logout (logging out only from the RP) and SLO.
- If the end user logs out while at a CS resource, the CS MUST terminate the end user's authentication session and MUST initiate SLO (i.e., terminate all RP sessions associated with that authentication session).
  - Before proceeding, the CS MUST inform the end user that he or she will be logged out of all active RP sessions, and the end user MUST confirm the request.

1.9.1 <Logout Request>

- `<LogoutRequest>` MUST be communicated over TLS 1.0, and use the HTTP Redirect binding.
- `<LogoutRequest>` MUST be signed.
- `Version` attribute MUST be set to "2.0".
- Upon receiving `<LogoutRequest>`, a CS MUST send `<LogoutRequest>` to every RP associated with the authentication session – except for the RP that submitted `<LogoutRequest>` to the CS since that RP already logged out the end user.
- Upon receiving `<LogoutRequest>`, an RP MUST terminate the end user's RP session.
- The CS MUST log the end user out locally (i.e., terminate the authentication session) and send a `<LogoutResponse>` to the originating RP to indicate SLO completion.

1.9.2 <LogoutResponse>

- `<LogoutResponse>` MUST be communicated over TLS 1.0, and use the HTTP Redirect binding.
- `<LogoutResponse>` MUST be signed.

[6] [SAML2 Profiles], Section 4.3

- `Version` attribute MUST be set to "2.0".
- If the Status of a `<LogoutResponse>` is not urn:oasis:names:tc:SAML:2.0:status:Success, the recipient of `<LogoutResponse>` MUST inform the end user that he or she may still have an active RP session, and instruct the end user to close his or her web browser. Otherwise, the Federation member system MUST inform the end user that he or she has logged out successfully.

1.10 Security

To establish trust and secure communications this interface specification relies heavily on X.509v3 cryptographic key pairs. This section outlines the different certificates that are required as well as specifics on their use.

1.10.1 E-GCA Certificates

The Federal PKI Operation Authority operates a certificate authority on behalf of the PMO to provide trust and security to the Federation. Possession of a valid certificate issued by the E-GCA demonstrates membership in the Federation. The E-GCA issues two certificates to each RP (one used for digital signature and one used for encryption), and one certificate to each CS (used for digital signature).

- These certificates MUST be maintained in compliance with the Subscriber responsibilities stipulated in [EGCA CP].

1.10.2 Digital Signature

All SAML messages, or parts thereof, MUST be signed by the sender using the E-GCA signature certificate that was issued to them. The signature allows the recipient of the message to authenticate the sender, and confirm that the message has not been altered since the time of signature.

- The recipient MUST authenticate the sender and verify the signature upon receipt of the message.
- The recipient MUST verify the revocation status of the sender certificate used to sign the message. Federation member systems SHOULD use one of the following methods for revocation verification:
  - *CDP Extension* – the signature certificate will include a Certificate Revocation List (CRL) Distribution Point extension point.
  - *OCSP* – The OCSP URI is available via the `AuthorityInformationAccess` extension.
  - *CRL* – the CRL location (in the directory or web site) can be statically configured into the software, and CRL downloaded periodically. See [EGCA CP] for details regarding distinguished name location and directory hostname.
- If certificate revocation status cannot be determined, the Federation member system MUST reject the message.

1.10.3 Encryption

Encryption ensures that only the intended recipient can decipher the message and gain access to confidential information.

- All confidential information in a SAML message MUST be encrypted.
- Encryption MUST use the public key of the intended recipient's E-GCA issued encryption certificate.

1.10.4 TLS web sites

This interface specification relies on the use of HTTP over TLS 1.0 (HTTPS) to transport messages.

- Any HTTPS site managed by a Federation member MUST be secured using a certificate trusted by default by commercially available browsers including Internet Explorer, Mozilla, Firefox, and America Online.

1.11 Metadata

This interface specification uses [SAML2 Metadata] to ease software configuration and communication. The PMO maintains and distributes current metadata. To terminate Federation member use of non-current metadata, the PMO stops distributing it. In addition, the PMO may revoke a certificate in the metadata file for reasons including, but not limited to terminating a Federation member's participation, certificate compromise, and key changes.

1.11.1 Security

1.11.1.1 Signature

- Federation members MUST sign their metadata using the signing certificate issued by the E-GCA.
- At consumption time, the Federation member relying upon the metadata MUST check the revocation status of the certificate used to sign the metadata. See Section 1.10.2 for possible methods for checking the revocation status.

1.11.1.2 Trust

- In order to establish metadata trust, each Federation member MUST sign their metadata using the signing certificate issued by the E-GCA
- The Federation member MUST submit the resulting XML metadata document to the PMO.

1.11.2 <EntityDescriptor>

- Each metadata file MUST contain metadata for one Federation member.
- The root of every metadata file within the Federation MUST be `<EntityDescriptor>`.

`entityID`

- `entityID` MUST be agreed upon by the entity and the PMO.
- `entityID` MUST be unique within the Federation.

`<Organization>`

- It is RECOMMENDED that `<Organization>` be present and include either `OrganizationName` or `OrganizationDisplayName`.

`<ContactPerson>`

- It is RECOMMENDED that the `<ContactPerson>` be present and include either `EmailAddress` or `TelephoneNumber` at a minimum.

<Signature>

- A valid signature enveloped within <EntityDescriptor> MUST be included.

1.11.3 <IDPSSODescriptor> Element

The <IDPSSODescriptor> Element describes CS metadata.

WantAuthnRequestsSigned

- WantAuthnRequestsSigned MUST be set to true.

protocolSupportEnumeration

- protocolSupportEnumeration MUST be urn:oasis:names:tc:SAML:2.0:protocol.

<KeyDescriptor>

- <KeyDescriptor> MUST be present to indicate the E-GCA signing certificate used by the CS.
- Use attribute MUST bet set to signing.
- <X509Data> MUST include the <X509Certificate> element populated with the certificate.

<SingleLogoutService>

- There MUST be exactly one <SingleLogoutService>.
- <SingleLogoutService> MUST be set to urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect.
- The port specified in the location URL MUST be 443.

<SingleSignOnService>

- Exactly one <SingleSignOnService> MUST be present.
- Binding MUST be set to urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect.
- The port specified in the location MUST be 443.

1.11.4 <SPSSODescriptor> Element

The <SPSSODescriptor> Element describes RP metadata.

AuthnRequestsSigned

- AuthnRequestsSigned MUST be set to true.

WantAssertionsSigned

- WantAssertionsSigned MUST be set to true.

protocolSupportEnumeration

- protocolSupportEnumeration MUST be set to urn:oasis:names:tc:SAML:2.0:protocol.

<KeyDescriptor>

- Two <KeyDescriptor> elements MUST be present.
- One of the <KeyDescriptor> elements MUST indicate the E-GCA signing certificate used by the RP
    - Use attribute MUST indicate signing.

- The other `<KeyDescriptor>` element MUST indicate the E-GCA encryption certificate used by the RP
  - `Use` attribute MUST indicate encryption.
- `<X509Data>` within each `<KeyDescriptor>` MUST include the `<X509Certificate>` element populated with the certificate.

`<SingleLogoutService>`

- Exactly one `<SingleLogoutService>` MUST be present.
- `<SingleLogoutService>` MUST be set to urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect.
- The port specified in the location MUST be 443.

`<AssertionConsumerService>`

- Exactly one `<AssertionConsumerService>` MUST be present.
- `Binding` MUST be set to urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST.
- The port specified in the location MUST be 443.

1.12 Exception Handling

Table 1-3 lists errors that the Federation member SAML service MUST handle gracefully. This is not a complete list of all possible errors (see the Federation Style Guide for more details as referenced in [FMD]). The table categorizes errors by SAML event. When these errors occur, the Federation member's help desk SHOULD be able to tie the end user session to the event that occurred given the approximate time of the error, the Federation members involved, and the end user.

Table 1-3 Possible Errors

• Error Processing <Response> o Incorrect/Unknown <Issuer> o Incorrect Version o Unrecognized InResponseTo o Unacceptable IssueInstant o Status not Success	• Error Processing <Assertion> o Signature Invalid o Signature Certificate Revoked o Cannot determine revocation status o <Assertion> Time Invalid o Cannot Decrypt <Assertion> o Incorrect Recipient o Incorrect Version
• Error Processing <AuthnRequest> o Unknown <Issuer> o Signature Invalid o Signature Certificate Revoked o Cannot determine revocation status	• Error processing SLO Request o Unknown <Issuer> o Signature Invalid o Signature Certificate Revoked o Cannot determine revocation status
• Error processing SLO <Response> o Unknown <Issuer> o Signature Invalid o Unknown status o Signature Certificate Revoked o Cannot determine revocation status	• Error reading CDC o Invalid Format

1.13 Testing

1.13.1 Test Assertions

- Each CS MUST have one account per assurance level at the CS that is used to produce an `<Assertion>` with us:gov:e-authentication:basic:assuranceLevel set to test.
- Test accounts MAY be used to monitor the RP-CS connection.
- Upon receiving `<Assertion>` with us:gov:e-authentication:basic:assuranceLevel set to "test", the RP MUST display a page containing at least the following message:

test with <display the urn:oid:2.5.4.3 attribute value> successful

1.13.2 Test Certificates

For unit, system, and acceptance testing, the Federation member will be issued test E-GCA certificate(s). The Federation member SHOULD consider use of the test certificates when planning the development and deployment of their system, particularly regarding test CRL LDAP directories and OCSP responders.

1.13.3 Conformance with Federation Reference Documents

This document does not represent the complete set of Federation requirements. Other documents MAY apply including business and policy documents (e.g., [FMD]), laws and regulations (e.g., [FISMA], [NIST SP 800-63]), and applicable technology standards (e.g., XML standards]).

1.13.4 Attribute Testing

Handling of attributes is subject to policies, laws, and regulations because they may contain confidential information. As the Federation MUST ensure RPs correctly manage missing, blank, and optional attributes, testing focuses on handling of received attributes. In particular, tests will check RP behavior when an unexpected set of attributes is received.

- Prior to testing, an RP MUST identify in writing all attributes essential to its operation.
- Prior to testing, an RP MUST identify in writing all attributes it will not accept from a CS.

1.14 Minimum Required Algorithms

The following are the minimum algorithms required for this adopted scheme.

- Encryption algorithm MUST be AES with 128 bit keys.
- Signature algorithm MUST be SHA1withRSA or SHA256withRSA.
- Federation member MAY use stronger algorithms if compliant with FIPS 140-2 and prior arrangements are made with the PMO and partners.

1.15 Examples

1.15.1 Sample SAML Authentication Requests

1.15.1.1 Redirect Query String

SAMLRequest=nZTRb9owEMbf%2B1dEfk%2FihADFAiQGmobUrRnJ9rCXySSX1VJs
Zz6Hdv997ZQyqlY88Hq5O%2F%2B%2B7z5ljly2HVv19kHt4G8PaIPgSbYK2fBlQXqj
mOYokCkuAZmtWLH6esfSiLLOaKsr3ZKb7WZBML3NZhnN6mzU0OY2yaY8baZJ0n
Ca0gmMZvv9pOYzSCgJfoJBodWCuDUk2CL2sFVoubKuROk0pGmYjMtkzEYTlo5%2
FkWDj0ITidph6sLZDFseeMaUhnUYVbyLgTkYECjsBJlJgWZaNYttgvN3kRXH%2F24
On7r3P2lQwaF6QhrcIHiHniOIAp0p%2BFPdJqFqoP5ed2L80IftSlnmY3xclCVaIYDzvW
ivsJZgCzEFU8GN3d6agi7BXUaXlAMulmzmAiV9nYgmWr1rB0bWS5c3cS2aDYebsUJ
fp%2BCsJWf5%2Fbx6frTou7tg3N%2Bzc0q2o%2Fl2TBO%2Bt5PZyt6%2BIOmyGVtb5
LKAFZUlQ5B7ge89b0bgjulCdeJ2hbasf1wa4dVeypgeyfBHxFvuk5RhoqIdTO0ctPNlrNK
217LgR6KMnhRKyl%2B7pwb7z1evWGb2D5pq7XGyrWOVXu7IP6aM2tQ8nVE5aabjL
uzb2eM6PeE4ufWiIsyt%2B%2FxdYPgM%3D&RelayState=s2849404d43f0f8147a2f711
fa0206e39bb6da9e10

1.15.1.2 SAML Message

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
Destination="https://saml20.caf.eauth.enspier.net/idp/SSO"
ID="R0F161211723111AFD135227D35B5CC7C5B6D14F0" IssueInstant="2007-02-
08T20:52:42Z" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Version="2.0">
        <saml:Issuer>https://saml20.caf.eauth.enspier.net:443/SP</saml:Issuer>
        <samlp:NameIDPolicy AllowCreate="true"
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"/>
</samlp:AuthnRequest>
```

1.15.2 Sample Authentication <Response>

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="ide5543476c7bec6d89a0551dcfa505c45f67a4a7"
InResponseTo="s2f2e4125ad08136b30ae49893a1ae86c154f451e4" IssueInstant="2007-
02-15T19:21:59.000Z" Version="2.0">
        <saml:Issuer
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://saml20.caf.eauth.e
        nspier.net:443/IDP</saml:Issuer>
        <samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
                <samlp:StatusCode
                Value="urn:oasis:names:tc:SAML:2.0:status:Success"
                xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"/>
        </samlp:Status>
        <saml:EncryptedAssertion
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                <xenc:EncryptedData
                xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                Type="http://www.w3.org/2001/04/xmlenc#Element">
                        <xenc:EncryptionMethod
                        Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"
                        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"/>
                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <xenc:EncryptedKey
                        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                        <xenc:EncryptionMethod
                        Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"
                        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"/>
                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:X509Data
                        xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:X509Certificate
                        xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        MIIDTDCCArWgAwIBAgIBETANBgkqhkiG9w0BAQUFADA
                        3MQswCQYDVQQGEwJVUzEoMCYGA1UEChMf.....
                        </ds:X509Certificate>
                        </ds:X509Data>
                        </ds:KeyInfo>
                        <xenc:CipherData
                        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                        <xenc:CipherValue
                        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">Il2whq71M
                        1wn/RGb2Z+qyl1E8GnN8zXjXQdEq8slTFxelI/Txf453Ksapgwo
                        wFEE9ypeONnFEyj7.....
                        </xenc:CipherValue>
                        </xenc:CipherData>
                        </xenc:EncryptedKey>
```

```
                        </ds:KeyInfo>
                        <xenc:CipherData
                        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                        <xenc:CipherValue
                        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">B1MslYB1
                        yVzST+S48YsGId1GbExu2e2jNP/9f1oAotPxEmcKDHino8afpS
                        J+brgU6jiZVNkYz3cx.....
                        </xenc:CipherValue>
                </xenc:CipherData>
                </xenc:EncryptedData>
        </saml:EncryptedAssertion
</samlp:Response>
```

1.15.3 Sample SAML <Assertion>

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="i1a8cbc7ffe5e97f8c177792eefe1cd4b21109d93" IssueInstant="2007-02-
15T19:21:59.000Z" Version="2.0">
        <saml:Issuer
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://saml20.caf.eauth.e
        nspier.net:443/IDP</saml:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                <ds:CanonicalizationMethod
                Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                <ds:SignatureMethod
                Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                <ds:Reference URI="#i1a8cbc7ffe5e97f8c177792eefe1cd4b21109d93">
                <ds:Transforms>
                <ds:Transform
                Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
                c14n#">
                <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-
                exc-c14n#" PrefixList="xsd"/>
                </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod
                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>xy+yrYU6widLMZuHBJ4lSiVfDng=</ds:DigestValue
                >
                </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>
                RuYlMNva0n5cHyUBy3l4h7MLGffm71gxRbT58/1nyDB53osoKgTdMf
                EcwGlJp4U5kmogPa7Q1SbQ.....
                </ds:SignatureValue>
                <ds:KeyInfo>
                <ds:X509Data>
                <ds:X509Certificate>
                UEvocATzqEPnAtIkRCltvFCHbOG9ctZiS1QQIGcSR0te60PfAgMBAA
                GjgckwgcYwCQYDVR0TBAIw.....
                </ds:X59Certificate>
                </ds:X509Data>
                </ds:KeyInfo>
        </ds:Signature>
        <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
                format:persistent"
                NameQualifier="https://saml20.caf.eauth.enspier.net:443/IDP"
```

```
            SPNameQualifier="https://saml20.caf.eauth.enspier.net:443/SP"
            xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">a9c16e861688086
            0f837a58dc12b490376d8bffa</saml:NameID>
            <saml:SubjectConfirmation
            Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"
            xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:SubjectConfirmationData
            InResponseTo="s2f2e4125ad08136b30ae49893a1ae86c154f451e4"
            NotOnOrAfter="2007-02-15T19:31:59.000Z"
            Recipient="https://sp.relyingparty1.com:443/amserver/Consumer/metaAli
            as/sp" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>
            </saml:SubjectConfirmation>
      </saml:Subject>
      <saml:Conditions xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:AudienceRestriction
            xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:Audience>
            https://saml20.caf.eauth.enspier.net:443/SP</saml:Audience>
            </saml:AudienceRestriction>
      </saml:Conditions>
      <saml:AuthnStatement AuthnInstant="2007-02-15T19:21:55.000Z"
      SessionIndex="843AE7" SessionNotOnOrAfter="2007-02-16T05:21:55.000Z"
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:AuthnContext
            xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"><saml:AuthnCont
            extClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtected
            Transport</saml:AuthnContextClassRef>
            <saml:AuthnContextDeclRef>https://saml20-
            07.caf.eauth.enspier.net:443/tfs/SAML20PasswordProtectedTransportStat
            ement.xml</saml:AuthnContextDeclRef>
            </saml:AuthnContext>
      </saml:AuthnStatement>
      <saml:AttributeStatement xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:Attribute xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            Name="us:gov:e-authentication:basic:assuranceLevel"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:AttributeValue
            xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
            xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xsi:type="xsd:string">2</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            Name="us:gov:e-authentication:2007:cn"
```

```
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                <saml:AttributeValue
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                xsi:type="xsd:string">2</saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                Name="us:gov:e-authentication:2007:cn"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                <saml:AttributeValue
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                xsi:type="xsd:string">Alice Adams</saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                Name="us:gov:e-authentication:2007:specVer"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                <saml:AttributeValue
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                xsi:type="xsd:string">2.0</saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                Name="us:gov:e-authentication:2007:PSSN"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                <saml:AttributeValue
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                xsi:type="xsd:string">5681</saml:AttributeValue>
                </saml:Attribute>
        </saml:AttributeStatement>
</saml:Assertion>
```

1.15.4 CS Metadata

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https:/saml20.caf.eauth.enspier.net:443/IDP">
<md:IDPSSODescriptor WantAuthnRequestsSigned="1"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
            <md:KeyDescriptor use="signing">
                        <ds:KeyInfo xmlns:ds="http:/www.w3.org/2000/09/xmldsig#">
                        <ds:X509Data>
                        <ds:X509Certificate>
                      MIIDTDCCArWgAwIBAgIBDTANBgkqhkiG9w0BAQUFADA3MQsw
                      CQYDVQQGEwJVUzEoMCYGA1UEChMf.....
                        </ds:X509Certificate>
                        </ds:X509Data>
                        </ds:KeyInfo>
             </md:KeyDescriptor>
             <md:SingleLogoutService>
           Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
           Location="https:/saml.caf.eauth.enspier.net:443/-soap/IDPSOAP_SAML20"/>
             <md:SingleSignOnService>
           Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
           Location="https:/saml20.caf.eauth.enspier.net:443/IDPSSO_SAML20"/>
            </md:IDPSSODescriptor>
           <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:SignedInfo>
                        <ds:CanonicalizationMethod
                        Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        <ds:SignatureMethod
                        Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                        <ds:Reference URI="#i1a8cbc7ffe5e97f8c177792eefe1cd4b21109d93">
                        <ds:Transforms>
                        <ds:Transform
                        Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
                        c14n#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-
                        exc-c14n#" PrefixList="xsd"/>
                        </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod
                        Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>xy+yrYU6widLMZuHBJ4lSiVfDng=</ds:DigestValue
                        >
                        </ds:Reference>
                        </ds:SignedInfo>
                        <ds:SignatureValue>
```

```
                    RuYlMNva0n5cHyUBy3l4h7MLGffm71gxRbT58/1nyDB53osoKgTdMf
                    EcwGlJp4U5kmogPa7Q1SbQ.....
                    </ds:SignatureValue>
                    <ds:KeyInfo>
                    <ds:X509Data>
                    <ds:X509Certificate>
                    UEvocATzqEPnAtlkRCltvFCHbOG9ctZiS1QQIGcSR0te60PfAgMBAA
                    GjgckwgcYwCQYDVR0TBAIw.....
                    </ds:X59Certificate>
                    </ds:X509Data>
                    </ds:KeyInfo>
          </ds:Signature>
</md:EntityDescriptor>
```

1.15.5 RP Metadata

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://saml20.caf.eauth.enspier.net:443/SP">
<md:SPSSODescriptor AuthnRequestsSigned="1" WantAssertionsSigned="1"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
          <md:KeyDescriptor use="signing">
                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                    <ds:X509Data>
                    <ds:X509Certificate>
                  MIIDTDCCArWgAwIBAgIBDTANBgkqhkiG9w0BAQUFADA3MQsw
                  CQYDVQQGEwJVUzEoMCYGA1UEChMf.....
                    </ds:X509Certificate>
                    </ds:X509Data>
                    </ds:KeyInfo>
          </md:KeyDescriptor>
          <md:KeyDescriptor use="encryption">
                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                    <ds:X509Data>
                    <ds:X509Certificate>
                  MIIDTDCCArWgAwIBAgIBDTANBgkqhkiG9w0BAQUFADA3MQsw
                  CQYDVQQGEwJVUzEoMCYGA1UEChMf.....
                    </ds:X509Certificate>
                    </ds:X509Data>
                    </ds:KeyInfo>
          </md:KeyDescriptor>
          <md:SingleLogoutService>
          Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
          Location="https://saml20-07.caf.eauth.enspier.net:443/tfs-
          soap/SPSLOSAML20"/>
          <md:AssertionConsumerService>
          Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
          Location="https://saml20-07.caf.eauth.enspier.net:443/tfs/SPSSO_SAML20"
          index="1"/>
</md:SPSSODescriptor>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
          c14n#"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
          sha1"/>
          <ds:Reference URI="#i1a8cbc7ffe5e97f8c177792eefe1cd4b21109d93">
          <ds:Transforms>
```

```
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
        signature"/>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-
        c14n#" PrefixList="xsd"/>
        </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>xy+yrYU6widLMZuHBJ4lSiVfDng=</ds:DigestValue>
        </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
        RuYlMNva0n5cHyUBy3l4h7MLGffm71gxRbT58/1nyDB53osoKgTdMfEcwGlJ
        p4U5kmogPa7Q1SbQ.....
        </ds:SignatureValue>
        <ds:KeyInfo>
        <ds:X509Data>
        <ds:X509Certificate>
        UEvocATzqEPnAtIkRCltvFCHbOG9ctZiS1QQIGcSR0te60PfAgMBAAGjgckw
        gcYwCQYDVR0TBAIw.....
        </ds:X59Certificate>
        </ds:X509Data>
        </ds:KeyInfo>
</ds:Signature>
</md:EntityDescriptor>
```

1.15.6 <LogoutRequest>

```
<samlp:LogoutRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://saml20-07.caf.eauth.enspier.net:443/IDPSLO_SAML20"
ID="s25cdbdf71cd19644d070080a7b810c579ddddc284" IssueInstant="2007-02-
15T15:44:13Z" Version="2.0">
        <saml:Issuer
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://saml20.caf.eauth.e
        nspier.net:443/SP</saml:Issuer>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                <SignedInfo>
                <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
                exc-c14n#"/>
                <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
                sha1"/>
                <Reference URI="#s25cdbdf71cd19644d070080a7b810c579ddddc284">
                <Transforms>
                <Transform
                Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </Transforms>
                <DigestMethod
                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <DigestValue>AIUkj6nrRn6cFYsUj01+3xVY9mY=</DigestValue>
                </Reference>
                </SignedInfo>
                <SignatureValue>
                LIkR4kUciPVCuBKC9hchjtpnQsx2S4fpeKhSFaB3191HBmBbX+8sUZ
                79TOV2E7rCbz+N4pKCDwKb.....
                </SignatureValue>
        </Signature>
        <saml:NameID xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
        NameQualifier="https://saml20.caf.eauth.enspier.net:443/IDP"
        SPNameQualifier="
        https://saml20.caf.eauth.enspier.net:443/SP">a9c16e8616880860f837a58dc12b49
        0376d8bffa</saml:NameID>
        <samlp:SessionIndex>843AE7</samlp:SessionIndex>
</samlp:LogoutRequest>
```

1.15.7 <LogoutResponse>

```
<samlp:LogoutResponse xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Destination="https://saml20-
07.caf.eauth.enspier.net:443/SP/SPSLO_SAML20" ID="0110-1929-93ba-9e37cbd646a5"
InResponseTo="ic8c7b752867812bfa991778a77ef720f67d75ff4" IssueInstant="2007-02-
16T15:29:01Z" Version="2.0">
        <saml:Issuer> Format="urn:oasis:names:tc:SAML:2.0:nameid-
        format:entity">https://saml20.caf.eauth.enspier.net:443/IDP/saml:Issuer>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                <SignedInfo>
                <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
                exc-c14n#"/>
                <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
                sha1"/>
                <Reference URI="#s25cdbdf71cd19644d070080a7b810c579ddddc284">
                <Transforms>
                <Transform
                Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </Transforms>
                <DigestMethod
                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <DigestValue>AIUkj6nrRn6cFYsUj01+3xVY9mY=</DigestValue>
                </Reference>
                </SignedInfo>
                <SignatureValue>
                LIkR4kUciPVCuBKC9hchjtpnQsx2S4fpeKhSFaB3191HBmBbX+8sUZ
                79TOV2E7rCbz+N4pKCDwKb.....
                </SignatureValue>
        </Signature>
        <samlp:Status>
                <samlp:StatusCode
                Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        </samlp:Status>
</samlp:LogoutResponse>
```

2 INTERFACE SPEC: SAML 1.0 BROWSER ARTIFACT PROFILE

The PMO is planning to phase out this adopted scheme some time in 2007 in favor of a SAML 2.0 based adopted scheme (see Section 1). A migration plan will guide Federation members and COTS vendors through the transition.

For the interface specification for this adopted scheme, please see:
http://www.cio.gov/eauthentication/documents/SAMLspec.pdf

APPENDIX A: GLOSSARY

Term	Definition
Assertion	A piece of data produced by a CS regarding either an act of authentication performed on a principal (e.g., end user), attribute information about the principal, or authorization data applying to the principal with respect to a specified resource.
Authentication	The process of establishing confidence in user identities. Authentication is different from authorization. However, they are usually inextricably linked. Authentication precedes authorization. Authentication simply establishes identity, or in some cases verified personal attributes (e.g., zip code), but not what that identity is authorized to do or what access privileges he or she has; this is a separate decision. The RP can use the authenticated information provided by the identity verifier to make authorization or access control decisions. The Federation directly addresses authentication, and indirectly supports authorization.
Authentication Service Component Entity (ASC Entity)	The ASC comprises various entities that actively participate in the authentication process. An ASC entity can be a system, a person, or group of persons that has a distinct role. Examples include RPS, CSs, end users, and external sites (e.g., USA.gov or FORMS.gov) providing Federation discovery services.
Authentication Session	Period of time that an end user remains trusted after the end user authenticates. That is because a CS typically does not require an end user to re-authenticate for every page requested. Each CS defines its own authentication session duration. If an end user returns to the CS and an earlier authentication session has expired, the CS re-authenticates the end user – even if single sign-on is in effect.
Binding	Mappings of SAML request-response message exchanges onto standard messaging or communication protocols.
Common Domain	RP or CS internal service to access an end user's common domain cookie and perhaps facilitate end user discovery of a compatible CS; it has no confidential information and has no access to or knowledge of application domain processing; this internal service is included in the Federation common domain; common domains are coordinated with the Federation DNS.
Common Domain Cookie (CDC)	Browser cookie that tracks the CSs to which the end user has authenticated during a particular session. CSs read and update the CDC. RPs read the CDC.
Compatible	Two Federation Member systems may technically interoperate if: ▪ The CS has an equal or higher assurance level than the RP, ▪ The CS is can provide all optional attributes required by the RP, and ▪ The CS and RP use the same interface specification version, or a scheme translator is available

Term	Definition
Cookie	A message given to a web browser (e.g., end user's web browser) by an ASC entity. The web browser stores the message in a file that is accessible only to the entities within the domain where the message was provided. The ASC uses cookies to facilitate single sign-on, and to manage sessions (e.g., RP session, authentication session). In addition, the ASC only uses transient cookies, which are stored in temporary memory and erased when the end user closes their web browser. Cookies do not collect information from the end user's computer. Cookies typically store information in the form of a session identification that does not personally identify the end user.
Credential Service (CS)	A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential, then each one is considered a separate CS.
CS Cookie	Once a CS authenticates an end user, the CS assigns a session cookie to the end user's browser. Upon subsequent end user visits to the CS during the same browser session, the CS uses the CS cookie to determine the end user's identity, whereupon the CS can redirect the end user without any end user interaction (i.e., no authentication required since the end user authenticated earlier), thus completing the single sign-on sequence. Content and sensitivity of the CS cookie varies among CSs.
Digital Encryption	Private key data encryption that converts data into a form that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.
Digital Signature	An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection.
Discovery	Process of an end user finding a CS and/or RP.
E-Authentication Program Management Office (PMO)	The PMO is the organization that handles Federation program management, administration, and operations. The PMO is not involved in authentication of transactions.
E-Governance Certification Authorities (E-GCA)	Established by the government to issue certificates as applicable for the adopted scheme. Certificates that may be issued TLS authentication, digital signing, and digital encryption. E-GCA certificates effectively control which entities can participate in the Federation.
Extensible Markup Language (XML)	XML is a specification developed by the W3C that enables the definition, transmission, validation, and interpretation of data between applications and between organizations. In a nutshell, XML describes data and focuses on what data is. XML facilitates technical interoperability, and is used in identity management standards such as SAML (e.g., to convey information in a SAML assertion).
HTML Form Control	User interface control that serves as a point of user interaction HTML forms.
Hypertext Markup Language (HTML)	The basic language used to write web pages, which are read by browsers.
Hypertext Transfer Protocol (HTTP)	Underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. In the Federation, where appropriate, HTTP is used to redirect end users.

Term	Definition
Metadata	SAML 2.0 message exchange between two ASC entities requires each to have specific knowledge about the other. One example is the URL of each service with which an ASC entity technically interoperates. Without such knowledge, an ASC entity does not know where to send SAML related messages for processing. Metadata describes and conveys such information.
Name Qualifier	A string that disambiguates an end user name identifier in a federated environment.
Partner	From a technical standpoint, other Federation member systems with which a Federation member system technically interoperates. From a business standpoint, other Federation members with whom a Federation member has a relationship.
Private Key	The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.
Public Key	The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.
Public Key Certificate	A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key.
Public Key Infrastructure (PKI)	Using a combination of private (i.e., secret) key and public key cryptography, PKI enables a number of other security services including data confidentiality, data integrity, and non-repudiation. PKI is the combination of software, encryption technologies, and services that enables entities to protect the security of their communications and business transactions on networks. PKI integrates digital certificates, public key cryptography, and certification authorities into a complete network security architecture. A typical PKI encompasses the issuance of digital certificates to individual users and servers; end-user enrollment software; integration with certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.
Redirect	Transfer of an end user from one node (i.e., operation Federation member system) to another, as necessary. For example: • After authenticating an end user, the CS redirects the end user to the RP; • An end user that starts at an RP but has not yet been authenticated is redirected by the RP to a selected CS
Relying Party	An entity that relies upon the subscriber's credentials (i.e., requires an end user to be authenticated), typically to process a transaction or grant access to information or a system.
RP Session	The period of time an RP will trust an end user before issuing a session reset request to re-authenticate the end user (i.e., redirect the end user back to the CS). Since RPs do not have access to authentication session information, RPs must maintain their own session with an end user. The RP sets the time limit for the RP session.

Term	Definition
Security Assertion Markup Language (SAML)	The set of specifications describing security assertions that are encoded in XML, profiles for attaching the assertions to various protocols and frameworks, the request/response protocol used to obtain the assertions, and bindings of this protocol to various transfer protocols (for example, SOAP and HTTP). SAML addresses web single sign-on, web services authentication, attribute exchange, authorization, non-repudiation, and secure communications. SAML defines assertion message formats that are referenced in Liberty Alliance, Shibboleth, WS-Security, and other specifications. SAML has become the standard web SSO identity management solution. Several versions have been released to date, including SAML 1.0, SAML 1.1, and SAML 2.0. The Organization for the Advancement of Structured Information Standards (OASIS) oversees SAML.
Signature Verification	The process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.
Single Logout (SLO)	Near-simultaneous logout of a collection of related sessions on request. In ASC terms, it is the logout of an end user from all active RP sessions associated with a specific authentication session.
Single Sign-on (SSO)	Once an end user has authenticated their identity at a CS, he or she may, by their choice, move among RPs compatible with the CS without re-authenticating. In other words, the end user is seamlessly logged into any other RP compatible with the CS. For privacy considerations, end users must take explicit actions to opt-in to SSO. SSO applies to assertion based Federation member systems only. In addition, SSO is in effect only for the duration of the end user's current browser session and authentication session. An end user must opt-in to SSO each time he or she opens a new web browser session. The ASC supports SSO as a core aspect of the federated architecture.
Web Browser	Web browsers communicate with web servers primarily using HTTP (hypertext transfer protocol) to fetch web pages. HTTP allows web browsers to submit information to web servers as well as fetch web pages from them. Web pages are located by means of a URL (uniform resource locator), which is treated as an address. Cookies can be sent by a server to a web browser and then sent back unchanged by the browser.

APPENDIX B: ACRONYMS

Acronym	Definition
ASC	Authentication Service Component
CDC	Common Domain Cookie
CDP	CRL Distribution Point
CRL	Certificate Revocation List
CS	Credential Service
E-GCA	E-Governance Certification Authorities
E-RA	E-Authentication Risk Assessment
FMD	Federation Membership Documents
FIPS	Federal Information Processing Standards
GSA	General Services Administration
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ID	Identifier
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Science and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OMB	Office of Management and Budget
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMO	Program Management Office
RC	Release Candidate
RP	Relying Party
SAML	Security Assertion Markup Language
SLO	Single Logout
SP	Special Publication
SSO	Single Sign-on
TBD	To Be Determined
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locater
U.S.	United States
XML	Extensible Markup Language