E-Authentication
Interface Specifications
for the SAML Artifact Profile

Version 1.0.0
June 28, 2004

Executive Summary

As part of the President's Management Agenda, the E-Authentication initiative has been established to enable trust and confidence in E-Government transactions via the establishment of an integrated policy and technical infrastructure for electronic authentication. The result is the Authentication Service Component (ASC). The ASC is a federated architecture that is strategically designed to support different identity assurance schemes simultaneously. By integrating with the ASC, an application owner no longer needs to build or maintain an authentication structure. Rather, they use one of the standard authentication schemes supported by the ASC. Each scheme has its own specification for use. Therefore, an ASC Interface Specification is required for each scheme detailing how that scheme integrates into the ASC.

Security Assertion Markup Language (SAML) 1.0 Artifact Profile is one of the schemes supported by the ASC. SAML supports assertion-based authentication, and is predicated on the exchange of a SAML Artifact and a SAML Assertion between endpoints. In E-Authentication, an agency application (AA) and a credential service (CS) are the endpoints. This interface specification provides guidance on how to use SAML 1.0 Artifact Profile specifically for E-Authentication purposes. This interface specification does not revise or extend SAML 1.0 Artifact Profile; it simply details how SAML 1.0 Artifact Profile must be used for E-Authentication purposes. Where this specification does not explicitly provide SAML guidance, the E-Authentication participant must implement in accordance with SAML 1.0 Artifact Profile requirements as documented by the OASIS standards body.

This document presents the transaction-processing specifications for CSs and AAs in separate sections, so each is stand-alone for the target audience. All transfers (also referred to as "hand-offs") between components, and transfer parameters are discussed. For a CS, the following specifications are detailed: (1) hand-off from the E-Authentication Portal, (2) single sign-on, (3) testing in production, and (4) exception handling. For an AA, the following specifications are detailed: (1) hand-off from the CS, (2) testing in production, and (3) exception handling. Detailed specifications for interfacing with the E-Authentication Portal are provided because it plays a fundamental role in single sign-on and error processing. Error codes to be included in transfers, as necessary, are listed. Guidance regarding personally identifiable information (PII) is provided.

The ASC rules for SAML Assertion composition (i.e., what values need to be in what fields) are specified. This ensures common expectation between the CS and AA. Code samples of both a SAML Assertion and a SAML Artifact are provided to further enhance an engineer's understanding of how to integrate SAML 1.0 Artifact Profile into their application for E-Authentication purposes.

Administration of the ASC using SAML 1.0 Artifact Profile is also addressed. The E-Authentication Governing Authority issues client and server certificates, and Certificate Revocation Lists (CRLs) to trusted endpoints, to secure the channel of communication between the two endpoints during SAML Artifact and SAML Assertion exchange. The E-Authentication Program Management Office (PMO) manages system configuration metadata, which is general information ASC partners need in order to interoperate when using the SAML 1.0 Artifact Profile scheme. An example of metadata is identifiers that uniquely identify AAs and CSs. Metadata is available to E-Authentication partners via download from the E-Authentication Portal and must be used to configure their SAML services before operating.

Table of Contents

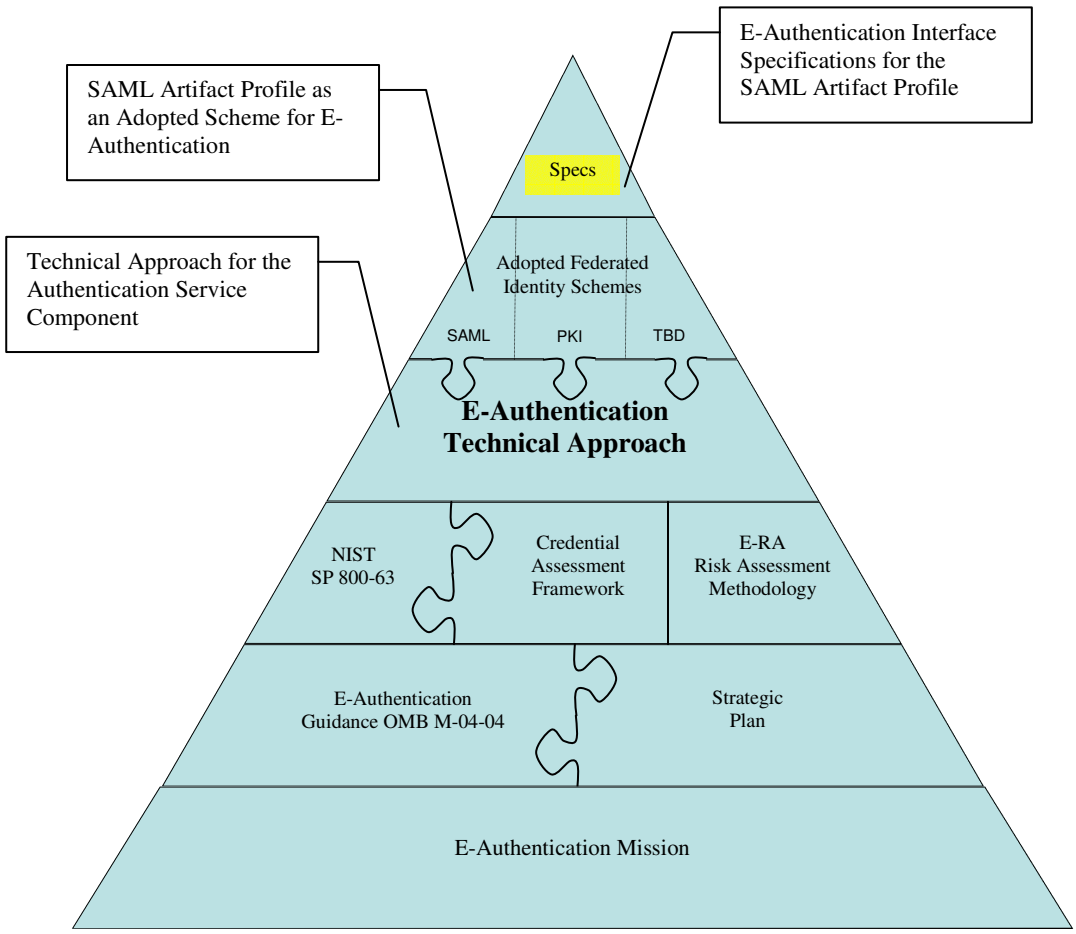
1 Introduction

This document provides the interface specifications for the Security Assertion Markup Language (SAML 1.0) Artifact Profile for use with the E-Authentication Initiative. The SAML 1.0 is one of the adopted schemes within the E-Authentication architectural framework. By integrating with the Authentication Service Component (ASC), an application owner can use a standard approach for authentication, rather than having to build or maintain an authentication structure. To integrate an application with the ASC there are two components: SAML and Public Key Infrastructure (PKI). While PKI allows for certificate-based authentication, SAML allows for assertion-based authentication.

This document is part of the ASC technical suite, which also includes the Technical Approach for the Authentication Service Component and the SAML Artifact Profile As an Adopted Scheme for E-Authentication. For complete comprehension, this document should be read after the Technical Approach and Adopted Scheme documents respectively. Figure 1 shows the documentation relationships for E-Authentication, and current versions of these documents are available on the E-Authentication website at http://www.cio.gov/eauthentication/.

Specifications for Agency Applications (AAs) and Credential Services (CSs) are both included in this document.

Figure 1: E-Authentication Document Hierarchy



1.1 Document References

[1] "Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)", OASIS Standard, 5 November 2002. Oasis-sstc-saml-bindings-1.0.
[2] "Assertions and Protocol for the OASIS Security Markup Language (SAML)", OASIS Standard, 5 November 2002. Oasis-sstc-saml-core-1.0.
[3] "Simple Object Access Protocol (SOAP) 1.1", W3C, W3C Note 08 May 2000, NOTE-SOAP-20000508.
[4] "RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile", Internet RFC/STD/FYI/BCP Archives).
[5] "Liberty Metadata Description and Discovery Specification", Version 1.0-10, Liberty Alliance

1.2 Reference Links

Topic	Link
SAML	http://www.w3.org http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security http://www.oasis-open.org/committees/security/docs
SOAP	http://schemas.xmlsoap.org/soap/envelope http://schemas.xmlsoap.org/soap/encoding
XML	http://www.w3.org/1999/XMLSchema-instance http://www.w3.org/1999/XMLSchema
X.509	http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1779.html#sec-2.3 http://www.faqs.org/rfcs/rfc2459.html
Metadata	http://www.projectliberty.org/specs/draft-lib-arch-metadata-v1.0-10.pdf. http://lists.oasis-open.org/archives/security-services/200304/msg00169.html

1.3 General Approach

This interface specification is based upon SAML 1.0 and provides guidance on how to use SAML 1.0 specifically for E-Authentication purposes. The specification does not revise or extend SAML 1.0. Where this specification does not explicitly provide SAML guidance, the E-Authentication participant must implement in accordance with SAML 1.0 requirements. The SAML browser Artifact Profile must be used. For details regarding SAML Artifact Profile, see "Bindings and Profiles for the OASIS Security Assertion Markup Language", section 4.

Authentication between the SAML Requester and the SAML Responder must be implemented by the following methods, as described in "Bindings and Profiles for the OASIS Security Assertion Markup Language", section 3.1.3.2, item 4:

- Hyper Text Transfer Protocol (HTTP) over Secure Sockets Layer (SSL) 3.0 or Transport Layer Security (TLS) 1.0 client authentication with a client-side certificate[1]

The E-Authentication Initiative Governing Authority will issue the client and server certificates, and AAs and CSs are required to process Certificate Revocation Lists (CRLs) issued by the Governing Authority. For additional information regarding Governing Authorities visit the E-Authentication website at http://www.cio.gov/eauthentication/.

All CSs and AAs will be issued identifiers by the E-Authentication Program Management Office (PMO). These identifiers are referred to as <CSid> and <AAid> respectively. The identifiers are used as keys to reference metadata, such as inter-site transfer Uniform Resource Locators (URLs) for each component, and will be made available for download by all CSs and AAs. See section 4 for more information on metadata.

[1] HTTP over SSL 3.0 or TLS 1.0 client authentication with a client-side certificate is mutually authenticated (i.e., client and server side certificates are required).

2 Credential Service Interface Specification

2.1 Hand-off From E-Authentication Portal

The end user will be redirected from the E-Authentication Portal (Portal) to the CS with an <AAid> in the query string. If an <AAid> is passed, the CS must authenticate the end user, then initiate a hand-off to the AA via the SAML Artifact Profile.

If the <AAid> is not included in the query string, then the end user has not selected an AA from the Portal and must be redirected to the Application Selection Service at the Portal with the CSid included on the query string: http://eauth.firstgov.gov/service/select?csid=<CSid>

Additionally, AAs may request a session reset in order to freshen end user credentials prior to authorization of activities. This request will be sent to the Portal, which will then relay the request to the CS via the inclusion of a specific query string parameter. An example of this is included below:

http://www.yourCS.com/signon.html?sessionreset=1&aaid=<AAid>

CSs receiving <sessionreset> on the query string must require the end user re-authenticate before initiating the hand-off to the AA.

For diagrams illustrating the hand-off from the Portal, please refer to the Technical Approach for the Authentication Service Component section 3.1.

Authentication between the SAML Requester and the SAML Responder must be implemented by the following methods, as described in "Bindings and Profiles for the OASIS Security Assertion Markup Language", section 3.1.3.2, items 2 and 4:

- HTTP over SSL 3.0 or TLS 1.0 client authentication with a client-side certificate

The E-Authentication Initiative will issue the client and server certificates.

For details regarding SAML Artifact, see "Bindings and Profiles for the OASIS Security Assertion Markup Language", section 4.1.1. Details regarding the assertion are discussed in section 5. Authentication of the end user is done according to the methods assessed by the PMO for approval as an E-Authentication CS.

2.2 Single Sign-on

Seamless single sign-on must be supported. When the Portal hands-off an end user who is already authenticated, the CS must immediately hand-off the end user to the AA without end user interaction. For privacy considerations, the end user must be required to take an explicit action to opt into single sign-on. The duration of the authentication session is at the discretion of the CS, subject to the methods assessed by the PMO for approval as an E-Authentication CS.

2.3 Testing

The CS must support test processing in the production environment. The CS must implement several test accounts within their system, with each test account being assigned an assurance level

= Test. All test accounts and passwords must be made available to the PMO, and should not be modifiable using test credentials.

Additionally, assertions at the test level may be sent with test Governing Authority's Certification Authority (CA) certificates.

2.4 Exception Handling

The Portal includes the ability to assist AAs and CSs in the graceful handoff of end users upon encountering error conditions that may prevent further end user interaction. This is accomplished by providing a special URL that includes query string parameters for the AAid, CSid, an error code, and a debug message. When encountering an exception, AAs and CSs are required to redirect the end user to the Portal's dedicated URL and communicate the nature of the exception to the Portal. Communication occurs via a pre-defined set of error codes such that end users can be properly advised and any necessary actions taken to continue their interaction with the Government.

AAs and CSs may also choose to include a brief debug message to facilitate error tracing by E-Authentication personnel and impacted participants. Debug messages should be brief but descriptive, and not include any personally identifiable information (PII) references. The debug message will not be displayed to the end user, but is transmitted in the open and is viewable via the address bar in the browser.

The Portal's exception handling URL is:

http://eauth.firstgov.gov/service/error?aaid=<AAid>&csid=<CSid>&errcode=<Error Code>&msg=<MESSAGE>

Error Code	Usage
10	AA Unavailable
20	CS Unavailable
30	AA Invalid
40	CS Invalid
50	CS assurance level does not meet AA's assurance level
60	CS refused to issue Identity Assertion
70	Hand-off error
90	Unknown Exception

3 Agency Application Interface Specification

3.1 Hand-off From Credential Service

The end user is passed to the AA from the CS. If attempting to access the AA directly, the end user should be redirected to the Portal CS Selection Service with <AAid> included on the query string: http://eauth.firstgov.gov/service/select?aaid=<AAid>

The end user is handed off from the CS using the SAML Artifact Profile. For details, see "Bindings and Profiles for the OASIS Security Assertion Markup Language", section 4. See section 5 for further specification of the assertion.

Authentication between the SAML Requester and the SAML Responder must be implemented by the following methods, as described in "Bindings and Profiles for the OASIS Security Assertion Markup Language", section 3.1.3.2, items 2 and 4:

- HTTP over SSL 3.0 or TLS 1.0 client authentication with a client-side certificate

The E-Authentication Initiative will issue the client and server certificates.

If the hand-off fails, the AA must redirect the end user to the Portal via:
http://eAuth.firstgov.gov/service/error?aaid=<AAid>&errcode=70[&msg=descriptive%20message]

If the AssuranceLevel attribute in the Assertion has a value less than is required by the AA, the AA must display a page indicating that the assurance level is insufficient for the end user to access the application and include a link that transfers the end user to the Portal:
http://eAuth.firstgov.gov/service/error?csid=<CSid>&aaid=<AAid>&errorcode=50&[msg=descriptive%20message]

AAs may request fresher (more recent) authentication[2] of an end user by using the <sessionreset> parameter when redirecting the end user to the Portal. This option is designed into the architecture to empower agencies to set more restrictive authorization controls. To trigger an authentication session reset, AAs should redirect end users to the following URL:
http://eauth.firstgov.gov/service/select?aaid=<AAid>&csid=<CSid>&sessionreset=1

For diagrams illustrating the hand-off from the CS, please refer to the Technical Approach for the Authentication Service Component section 3.3.

[2] The Authentication Instant field of the assertion provides authentication timestamp, which is different from the assertion timestamp.

3.2 Testing

The AA must support test processing in the production environment. The AA must inspect the AssuranceLevel attribute in the Assertion for an AssuranceLevel = "Test". If found, the AA must display a page to the end user indicating the test was successful. The page should include the <commonName> attribute from the assertion, the name of the CS, and the name of the AA. The test end user should not be granted access to any protected resources.

The page must also contain the following status text:

```
test with <commonName> from <CSid> to <AAid> <status>
```

where <status> contains either "successful" or "failed"

The status text may be hidden from the end user.

3.3 Exception Handling

The Portal includes the ability to assist AAs and CSs in the graceful hand-off of end users upon encountering error conditions that may prevent further end user interaction. This is accomplished by providing a special URL that includes query string parameters for the AAid, CSid, an error code, and a debug message. When encountering an exception, AAs and CSs are required to redirect the end user to the Portal's dedicated URL and communicate the nature of the exception to the Portal. Communication occurs via a pre-defined set of error codes such that end users can be properly advised and any necessary actions taken to continue their interaction with the Government.

AAs and CSs may also choose to include a brief debug message to facilitate error tracing by E-Authentication personnel and impacted participants. Debug messages should be brief but descriptive, and not include any PII references. The debug message will not be displayed to the end user, but is transmitted in the open and is viewable via the address bar in the browser.

The Portal's exception handling URL is:

http://eauth.firstgov.gov/service/error?aaid=<AAid>&csid=<CSid>&errcode=<Error Code>&msg=<MESSAGE>

Error Code	Usage
10	AA Unavailable
20	CS Unavailable
30	AA Invalid
40	CS Invalid
50	CS assurance level does not meet AA's assurance level
60	CS refused to issue Identity Assertion
70	Hand-off error
90	Unknown Exception

4 Configuration Metadata

SAML interoperability requires partners to have some information about other sites, including:

- Location of the SOAP Responders
- Issuer attribute
- AssuranceLevel attribute

Metadata is managed by the PMO. It will be available to E-Authentication partners via download from the Portal. The metadata is expressed according to the "Liberty Metadata Description and Discovery Specification".

Both the CS and the AA must download E-Authentication configuration metadata, and auto-configure their SAML services accordingly.

For a configuration metadata example, see Appendix A of this document.

5 Rules for the SAML Assertion

1 The <Assertion> Issuer attribute is approved by the E-Authentication Initiative.

2 The <NameIdentifier> value MUST be in X.509v3 SubjectName format. See "RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile". Note that the Format attribute of this element is optional, however if present it MUST be set to urn:oasis:names:tc:SAML:1.0:assertion#X509SubjectName.

3 The <NameIdentifier> value MUST contain a Relative Distinguish Name (RDN) with the name end user identifier (Uid) such that no two subscribers within a CS can share the same uid.

4 The <AttributeStatement> MUST exist and contain the following <Attribute> and respective <AttributeValue> elements:

   a. CSid (e.g.s, "CA2439879", "24")
      i. MUST contain the CSid of the CS or certification authority that issued the end user's credentials. The combination of CSid and Uid (see item 2.) insure a unique Uid.
   b. commonName (e.g., "John H. William Smith III")
      i. SHOULD contain surname and given name if known. Otherwise, must contain the end user's pseudonym or Uid.
   c. assuranceLevel (e.g., "2")
      i. MUST be one of the following valid values: 1, 2, 3, 4, or Test.
   d. No other attributes can be included except when explicitly approved by the PMO.

5 The AttributeNamespace MUST be set to http://eauthentication.gsa.gov/federated/attribute.

6 Other than the personal information explicitly cited in this specification, assertions MUST NOT contain any other personal information.

Appendix A: Examples

1 Sample SOAP-Wrapped SAML Request

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:xsi="http://www.w3.org/1999/XMLSchema-
instance"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/1999/XMLSchema"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
      <SOAP-ENV:Body>
            <samlp:Request
            xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
            MinorVersion="0" MajorVersion="1" RequestID="3234487234324"
            xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
            IssueInstant="2003-10-22T16:35:40Z">
      <samlp:AssertionArtifact>AAHJwitt2KE3M/msiV5vz4QwxqVRlcZNX0AP3mPt
      ROrMmic5+DVJCzAx</samlp:AssertionArtifact>
            </samlp:Request>
      </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

2 Sample SOAP-Wrapped SAML Assertion

```
soap-env:Envelope
xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">
<soap-env:Body>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
ResponseID="UCIwfB7OKt0L1ChV4JGuf7Ke/so=" InResponseTo="3234487234324"
MajorVersion="1" MinorVersion="0" IssueInstant="2003-10-22T17:19:19Z"
>
<samlp:Status>
<samlp:StatusCode Value="samlp:Success">
</samlp:StatusCode>
</samlp:Status>
<saml:Assertion  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
MajorVersion="1" MinorVersion="0"
AssertionID="Tnw9QeaqJFn3lmCjK+eRdTGAkmI=01"
Issuer="http://testlab.enspier.com:58080"
IssueInstant="2003-10-22T17:19:17Z" >
<saml:Conditions  NotBefore="2003-10-22T17:14:17Z"
NotOnOrAfter="2003-10-22T17:21:17Z" >
</saml:Conditions>
<saml:AuthenticationStatement
AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password"
AuthenticationInstant="2003-10-22T17:19:14Z">
<saml:Subject>
<saml:NameIdentifier
NameQualifier="dc=enspier,dc=com">uid=michael,ou=People,o=Website,dc=en
spier
,dc=com</saml:NameIdentifier>
<saml:SubjectConfirmation>
<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:artifact-
01</saml:Co
nfirmationMethod>
</saml:SubjectConfirmation>
</saml:Subject>
<saml:SubjectLocality  IPAddress="151.196.49.222"
/></saml:AuthenticationStatement>
<saml:AttributeStatement >
<saml:Subject>
<saml:NameIdentifier
NameQualifier="dc=enspier,dc=com">uid=michael,ou=People,o=Website,dc=en
spier
,dc=com</saml:NameIdentifier>
<saml:SubjectConfirmation>
<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:artifact-
01</saml:Co
nfirmationMethod>
</saml:SubjectConfirmation>
</saml:Subject>
<saml:Attribute AttributeName="assuranceLevel"
AttributeNamespace="http://eauthentication.gsa.gov/federated/attribute"
>
<saml:AttributeValue>2</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute AttributeName="commonName"
AttributeNamespace="http://eauthentication.gsa.gov/federated/attribute"
>
```

```
<saml:AttributeValue> John H. William Smith III</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute AttributeName="csid"
AttributeNamespace="http://eauthentication.gsa.gov/federated/attribute"
>
<saml:AttributeValue> CA2439879</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
</soap-env:Body>
</soap-env:Envelope>
```

3 *Sample Configuration Metadata*

```
<?xml version="1.0" encoding="UTF-8"?>

<lmeta:EntitiesDescriptor xmlns:lmeta="urn:liberty:metadata:2003-08"
xmlns:saml="urn:oasis:names:tc:SAML:1.1:assertion"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:eAuth="http://eauthentication.gsa.gov/xml/saml1.0-Art/meta-
extension.xsd">
<!-- Agency Application - SP -->
    <lmeta:EntityDescriptor providerID="http://entity1.gov/PMO-issued">
        <lmeta:SPDescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.0:protocol">
            <lmeta:AssertionConsumerServiceURL id="1"
isDefault="true">https://entity1.gov/saml-
artifact/receiver</lmeta:AssertionConsumerServiceURL>
            <lmeta:AuthnRequestSigned>false</lmeta:AuthnRequestSigned>
            <lmeta:Extension>
<eAuth:AgencyApplicationProvider>

                    <eAuth:RequesterX509SubjectName>CN=www.entity1.gov,
OU=SAML Requesters, O=GSA, C=US</eAuth:RequesterX509SubjectName>
                    <eAuth:AssuranceLevel>2</eAuth:AssuranceLevel>
                     <eAuth:AgencyApplication>
                         <eAuth:AAid>127</eAuth:AAid>

<eAuth:Target>http://www.entity1.gov/myEntity1</eAuth:Target>
                    </eAuth:AgencyApplication>
                     <eAuth:AgencyApplication>
                         <eAuth:AAid>132</eAuth:AAid>
<eAuth:Target>http://www.entity1.gov/orders</eAuth:Target>
                    </eAuth:AgencyApplication>

                </eAuth:AgencyApplicationProvider>

            </lmeta:Extension>
        </lmeta:SPDescriptor>
    </lmeta:EntityDescriptor>

    <!-- Credential Service - IdP -->
    <lmeta:EntityDescriptor providerID="http://entity2.com/PMO-issued">
        <lmeta:IDPDescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.0:protocol">
<lmeta:SingleSignOnServiceURL>https://entity2.com/saml/responder</lmeta
:SingleSignOnServiceURL>

<lmeta:SingleSignOnProtocolProfile>urn:oasis:tc:SAML:1.0:profiles:artif
act</lmeta:SingleSignOnProtocolProfile>
            <lmeta:Extension>
                <eAuth:CredentialServiceProvider>
                    <eAuth:AssuranceLevel>2</eAuth:AssuranceLevel>
                    <eAuth:CredentialService>

      <eAuth:NameQualifier>dc=entity2,dc=com</eAuth:NameQualifier>
                        <eAuth:CSid>8030</eAuth:CSid>
                    </eAuth:CredentialService>
                </eAuth:CredentialServiceProvider>
```

```
            </lmeta:Extension>
        </lmeta:IDPDescriptor>
    </lmeta:EntityDescriptor>

    <!-- translator - accepts other protocols (Liberty?) and translates
to SAML1.0 -->
    <lmeta:EntityDescriptor providerID="http://entity3.gov/PMO-issued">

        <lmeta:IDPDescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.0:protocol">

<lmeta:SingleSignOnServiceURL>https://entity3.com/SamlOUTResponder</lme
ta:SingleSignOnServiceURL>

<lmeta:SingleSignOnProtocolProfile>urn:oasis:tc:SAML:1.0:profiles:artif
act</lmeta:SingleSignOnProtocolProfile>
            <lmeta:Extension>

                <eAuth:CredentialServiceProvider>
                    <eAuth:AssuranceLevel>1</eAuth:AssuranceLevel>
                    <eAuth:CredentialService>
<eAuth:NameQualifier>EAuthentication</eAuth:NameQualifier>
                        <eAuth:AssuranceLevel>1</eAuth:AssuranceLevel>
                    </eAuth:CredentialService>
                </eAuth:CredentialServiceProvider>

            </lmeta:Extension>
        </lmeta:IDPDescriptor>

         <lmeta:SPDescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.0:protocol">
            <lmeta:AssertionConsumerServiceURL id="2"
isDefault="true">https://entity3.gov/saml-
artifact/INReceiver</lmeta:AssertionConsumerServiceURL>
            <lmeta:AuthnRequestSigned>false</lmeta:AuthnRequestSigned>
            <lmeta:Extension>

                <eAuth:AgencyApplicationProvider>
                     <eAuth:RequesterX509SubjectName>CN=entity3.gov,
OU=SAML Requesters, O=GSA, C=US</eAuth:RequesterX509SubjectName>
                     <eAuth:AssuranceLevel>1</eAuth:AssuranceLevel>
                     <eAuth:AgencyApplication>
                         <eAuth:AAid>146</eAuth:AAid>

<eAuth:Target>http://www.entity3.gov/translator-
throughput</eAuth:Target>
                     </eAuth:AgencyApplication>
                </eAuth:AgencyApplicationProvider>

            </lmeta:Extension>
        </lmeta:SPDescriptor>

    </lmeta:EntityDescriptor>

</lmeta:EntitiesDescriptor
```

Appendix B: Glossary and Acronyms

Term	Definition
Agency Application (AA)	An online service provided by a government agency that requires a end user to be authenticated.
Assurance Level	Level of trust, as defined by the OMB Memorandum 04-04 Guidance for E-Authentication.
Certificate	X.509v3 digital certificates in a Public Key Infrastructure (PKI) for authentication, and can be used at any assurance level.
Certificate Revocation List (CRL)	The CRL is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release. When a potential end user attempts to access a server, the server allows or denies access based on the CRL entry for that particular end user.
Certification Authority (CA)	A certification authority is an authority in a network that issues and manages security credentials and public keys for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate. Depending on the public key infrastructure implementation, the certificate includes the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner.
Claimant	A party whose identity is to be verified using an authentication protocol.
Credential	Digital documents used in authentication and access control that bind an identity or an attribute to a claimant's token or some other property, such as an end user's current network address. Note that this guidance distinguishes between credentials, and tokens while other documents may lump tokens with credentials.
Credential Service (CS)	A service of a Credential Service Provider (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.
Credential Service Provider (CSP)	An organization that offers one or more Credential Services. Sometimes known as an ECP.
E-Authentication Portal (Portal)	A website that helps an end user locate the CSs and AAs needed for completing transactions. The Portal also maintains information about CSs and AAs referred to as metadata, which includes technical interface data as well as descriptive information. When the end user opts into single sign-on, the Portal assigns a session a cookie.
Governing Authority	Established by the government to issue certificates that allow Agency Applications to retrieve SAML assertions from Credential Services over a client and server authenticated SSL channel, effectively controlling which entities can participate.

Term	Definition
Project Management Office (PMO)	The PMO is the organization that handles E-Authentication program management, administration, and operations.
SAML Artifact	A SAML artifact of "small" bounded size 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.
SAML Artifact Profile	The browser/artifact profile of SAML relies on a reference to the needed assertion traveling in a SAML artifact, which the destination site must dereference from the source site in order to determine whether the end user is authenticated.
SAML Assertion	A piece of data produced by a SAML authority regarding either an act of authentication performed on a subject, attribute information about the subject, or authorization permissions applying to the subject with respect to a specified resource.
Scheme	Schemes, such as SAML and Liberty, specify protocols and standards for federated identity mechanisms for different entities to share identities without requiring the end user to manage multiple accounts.
Security Assertion Markup Language (SAML)	XML-based framework for ensuring that transmitted communications are secure. SAML defines mechanisms to exchange authentication, authorization and nonrepudiation information, allowing single sign-on capabilities for Web services.
Single Sign-on	After initial authentication with a CS during a browser session, the end user is seamlessly logged into any other AA of equal or lower authentication levels. For privacy considerations, the end user is required to take an explicit action to opt into single sign-on.
Simple Object Access Protocol (SOAP)	Lightweight XML-based messaging protocol used to encode the information in Web service request and response messages before sending them over a network. It consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses. SOAP messages are independent of any operating system or protocol and may be transported using a variety of Internet protocols, including MIME and HTTP.
Token	Something that the claimant possesses or knows (typically a key or password) that can be used to remotely authenticate the claimant's identity. Technically, the token includes an end userid and password that ensures token uniqueness within a credential domain.

Acronym	Abbreviation For
AA	Agency Application
AAid	Agency Application Identifier

Acronym	Abbreviation For
ASC	Authentication Service Component
AWG	Architecture Working Group
CA	Certification Authority
CRL	Certificate Revocation List
CS	Credential Service
CSid	Credential Service Identifier
E-RA	Electronic Risk & Requirements Analysis
HTTP	Hyper Text Transfer Protocol
NIST	National Institute for Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PMO	Project Management Office
RA	Registration Authority
RC	Release Candidate
RDN	Relative Distinguish Name
RFC	Request For Comments
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
SP	Special Publication
SSL	Secure Sockets Layer
TBD	To Be Determined
TLS	Transport Layer Security
Uid	End user Identifier
URL	Uniform Resource Locator
UTF	Universal Transformation Format
XML	Extensible Markup Language

Appendix C: Document History

Document History

Status	Release	Date	Comment	Audience
Draft	0.1.0	11/03/03	Initial Draft for distribution	Limited
RC1	1.0.0	05/17/04	1) Added text for describing session reset. (AWG Bullet 18) 2) Added sentence describing "explicit opt-in". (AWG Bullet 57) 3) Spelling of e-Authentication changed to E-Authentication. 4) Added Glossary section to describe document terms. (AWG Bullet 12 & 64)	Limited
RC2	1.0.0	05/26/04	1) Section 2.1 was reworded for organizational purposes. 2) http://www.cio.gov/E-Authenticatioin link changed to http://www.gio.gov/eauthentciation. 3) Inserted an additional paragraph into section 1 to introduce SAML and PKI as the two components for authentication. 4) Added document reference callouts to the documents diagram in section 1. 5) Added exception handling to both AA and CS Interface Specification sections. 6) Added document reference callouts to the documents diagram in section 1.1. 7) Added an acronym list to Appendix B.	Limited
RC3	1.0.0	06/28/04	1) Reformatted document for consistency. 2) Added attribute namespace to sample configuration metadata. 3) Added text referring to the Tech Approach for viewing diagrams that illustrate the Portal and CS hand-off. 4) Added hand-off error code to AA and CS exceptional handling error code tables. 5) Certification Authority added to acronym list. 6) Document titles (NIST SP 800-63, OMB M-04-04) added to the document diagram. 7) Sentence added describing that AAs and CSs are	Limited

required to process CRLs.

8) Sentence added describing that test level may be sent with test Governing Authority's CA certificates.

9) Certificate Revocation List (CRL) definition reworded in the glossary.

10) Certification Authority (CA) definition added to the glossary.