ICAM

Identity, Credential,
& Access Management

Federal Identity, Credentialing, and Access Management

Security Assertion Markup Language (SAML) 2.0
Web Browser Single Sign-on (SSO)
Profile

Version 1.0.2

December 16, 2011

Document History

Status	Release	Date	Comment	Audience
Final Release Candidate	1.0.0	9/27/10	Initial version for posting to IDManagement.gov.	Public
Final	1.0.1	11/15/11	1. Section 3.1 item #8 and Section 3.2 item 8b, revised the unspecified URI.(3rd bullet) from "SAML:2.0" to "SAML:1.1" 2. Section 3.1 item #9, changed to indicate that the RP MUST use HTTP-REDIRECT or HTTP-POST binding. 3. Section 3.2 item #4, deleted LOA reference to make it general rule. 4. Section 3.2, combined item #4 and item #5. 5. Section 3.3.1, item #2c, changed to "If the RP uses Assertion encryption,, <md:SPSSODescriptor> MUST contain at least one <md:KeyDescriptor>." 6. Section 3.3.1, item #3c bullet, changed from just HTTP-Redirect binding to HTTP-Redirect or HTTP-POST binding.	Public
Final	1.02	12/16/11	1. In general: changes regarding protecting against Assertion Disclosure threat – consistent with NIST Special Publication 800-63-1. 2. Section 2.6, revised end of paragraph to use language consistent with NIST Special Publication 800-63-1 (protected session), and to clarify its meaning in context of this Profile. 3. Section 3.2 item #4, revised to use language consistent with NIST Special Publication 800-63-1 (protected session), and to clarify its meaning in context of this Profile. 4. Section 3.4, added "protected session" guideline. 5. Appendix A comments column, revised Assertion bullets to indicate protected session and that Assertion may be encrypted. 6. Appendix C, added definition of "protected session", per NIST Special Publication 800-63-1. 7. Appendix E, revised NIST Special Publication 800-63-1 reference definition to cite December 2011 version.	Public

Editors

Terry McBride	Matt Tebo	John Bradley
Dave Silver	Tim Baldridge	

Executive Summary

Security Assertion Markup Language (SAML) 2.0 Profile as described in this document has been adopted by Federal Identity, Credential, and Access Management (ICAM) for the purpose of Level of Assurance (LOA) 1, 2, and 3 identity authentication, as well as holder-of-key assertions for binding keys or other attributes to an identity at LOA 4. Proper use of this Profile ensures that implementations:

- Meet Federal standards, regulations, and laws;
- Minimize risk to the Federal government;
- Maximize interoperability; and
- Provide end users (e.g., citizens) with a consistent context or user experience at a Federal Government site.

This Profile is a deployment profile based on the Organization for the Advancement of Structured Information Standards (OASIS) SAML 2.0 specifications [SAML2 *], and the Liberty Alliance eGov Profile v.1.5 [eGov Profile]. This Profile relies on the SAML 2.0 Web Browser SSO Profile [SAML2 Profiles] to facilitate end user authentication.

This Profile does not alter these standards, but rather specifies deployment options and requirements to ensure technical interoperability with Federal government applications. Where this Profile does not explicitly provide guidance, the standards upon which this Profile is based take precedence. In addition, this Profile recognizes the [eGov Profile] conformance requirements[1], and to the extent possible reconciles them with other SAML 2.0 Profiles.

The objective of this document is to define the ICAM SAML 2.0 Web Browser SSO Profile so that persons deploying, managing, or supporting an application based upon it can fully understand its use in ICAM transaction flows.

In general, the SAML 2.0 protocol facilitates exchange of SAML messages (requests and/or responses) between endpoints. For this Profile, messages pertain primarily to the exchange of an identity assertion that includes authentication and attribute information. Message support for additional features is also available. In ICAM, the endpoints are typically the Relying Party (RP) and the Identity Provider (IdP).

SAML 2.0 Profile defined herein includes the following features: single sign-on, session reset, and attribute exchange. In addition, this Profile defines two main SAML 2.0 use cases: the end user starting at the RP, and the end user starting at the IdP. Use case diagrams and sequence diagrams are provided to illustrate the use cases. Privacy, security, and end user activation are also discussed. Programmed trust (a mechanism to indicate to RPs which IdPs are approved for use within ICAM) is also discussed, and a high-level process flow diagram is provided to illustrate the concept.

The Profile concludes with detailed technical guidance that scopes SAML 2.0 Web Browser SSO for ICAM purposes. Like most specifications, SAML 2.0 provides options. Where necessary, ICAM specifies or removes options in order to enhance security, privacy, and interoperability. The Technical Profile section addresses the authentication request and response, metadata, and transaction security.

[1] A deployment profile outlines requirements for using SAML software in a given context, whereas a conformance (or product) profile describes the requirements for a software implementation.

Table of Contents

Figures

1. INTRODUCTION

1.1 Background

In December 2003, the Office of Management and Budget (OMB) issued memorandum M-04-04, *E-Authentication Guidance for Federal Agencies* [OMB M-04-04], which established four levels of identity assurance (LOA) for the authentication of electronic transactions. The four (4) M-04-04 LOA are:

Level 1: Little or no confidence in the asserted identity's validity.
Level 2: Some confidence in the asserted identity's validity.
Level 3: High confidence in the asserted identity's validity.
Level 4: Very high confidence in the asserted identity's validity.

M-04-04 also tasked the National Institute of Standards and Technology (NIST) with providing technical standards for each LOA. Consequently, NIST developed Special Publication 800-63-1, *Electronic Authentication Guideline* [NIST SP 800-63-1], as the standard agencies must use when conducting electronic authentication.

The General Services Administration's (GSA) Office of Governmentwide Policy (OGP) is responsible for government-wide coordination and oversight of Federal Identity, Credential, and Access Management (ICAM). These activities are aimed at improving access to electronic government services internally, with other government partners, with business partners, and with the American citizen constituency. Toward that end, the ICAM Subcommittee assesses identity authentication schemes under consideration for adoption by the Federal Government in accordance with the ICAM Identity Scheme Adoption Process [Scheme Adopt]. The adoption process includes assessment of the scheme for compliance with [NIST SP 800-63-1] and other privacy and security requirements.

The Security Assertion Markup Language (SAML) 2.0 Profile as described in this document has been adopted by ICAM for the purpose of LOA 1, 2 and 3 identity authentication, as well as holder-of-key assertions for binding keys or other attributes to an identity at LOA 4. Proper use of this Profile ensures that implementations:

- Meet Federal standards, regulations, and laws;
- Minimize risk to the Federal government;
- Maximize interoperability; and
- Provide end users (e.g., citizens) with a consistent context for credential use at a Federal Government site

This Profile is a deployment profile based on the Organization for the Advancement of Structured Information Standards (OASIS) SAML 2.0 specifications [SAML2 *], and the Liberty Alliance eGov Profile v.1.5 [eGov Profile]. This Profile does not alter these standards, but rather specifies deployment options and requirements to ensure technical interoperability with Federal government applications. Where this Profile does not explicitly provide guidance, the standards upon which this Profile is based take precedence. In addition, this Profile recognizes the [eGov Profile] conformance requirements[2], and to the extent possible reconciles them with other SAML 2.0 Profiles.

[2] A deployment profile outlines requirements for using SAML software in a given context, whereas a conformance (or product) profile describes the requirements for a software implementation.

1.2 Objective and Audience

The objective of this document is to define the ICAM SAML 2.0 Profile so that persons deploying, managing, or supporting an application based upon it can fully understand its use in ICAM transaction flows. The definition includes:

1. A high-level overview of the ICAM SAML 2.0 Profile and its features;
2. General requirements for Identity Providers (IdPs)[3] and Relying Parties (RPs) that extend outside the reach of SAML 2.0 specifications (e.g., privacy, security, activation, governance).
3. An ICAM deployment profile of the SAML 2.0 Profile specification [SAML2 Profiles].

Section 2 provides a high-level overview of the Profile, and includes discussion of features, use cases, and process flows. The section provides the context and understanding necessary to implement and manage an ICAM SAML 2.0 application. The audience for this section includes both technical personnel (e.g., designers, implementers) and non-technical personnel (e.g., senior managers, project managers).

Section 3 provides technicians with normative guidance on how to implement the ICAM SAML 2.0 Profile (i.e., send or receive SAML 2.0 messages within ICAM). It is assumed that readers of section 3 are familiar with the SAML 2.0 specification [SAML2 Core].

1.3 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].

Conventional XML namespace prefixes are used throughout the listings in this specification to stand for their respective namespaces as follows:

Prefix	**XML Namespace**
saml:	urn:oasis:names:tc:SAML:2.0:assertion
samlp:	urn:oasis:names:tc:SAML:2.0:protocol
md:	urn:oasis:names:tc:SAML:2.0:metadata
ds:	http://www.w3.org/2000/09/xmldsig#

2. SCHEME OVERVIEW

2.1 SAML 2.0 Overview

In general, the SAML 2.0 protocol facilitates exchange of SAML messages (requests and/or responses) between endpoints. For this Profile, messages pertain primarily to the exchange of an identity assertion that includes authentication and attribute information. Message support for additional features is also available (see Section 2.3). In ICAM, the endpoints are typically the Relying Party (RP) and the Identity Provider (IdP).

[3] Some make a distinction between Identity Provider (IdP) as the entity that credentials the end user, and Credential Service Provider (CSP) as the entity that authenticates the end user and provides assertions to relying parties.

The ICAM SAML 2.0 Profile can be used to conduct transactions with the Federal government. At this time, SAML 2.0 is suitable for LOA 1, 2 and 3 identity authentication, as well as holder-of-key assertions for binding keys or other attributes to an identity at LOA 4. See Appendix A for a summary of message transactions supported by this Profile.

This Profile relies on the SAML 2.0 Web Browser SSO Profile [SAML2 Profiles] to facilitate end user authentication.

2.2 SAML 2.0 Bindings

Each SAML 2.0 profile uses one or more SAML 2.0 bindings. SAML bindings are frameworks for embedding and conveying SAML protocol messages. That is, a SAML binding is a specific means of conveying SAML protocol messages using standard transport protocols (e.g., HTTP POST). The SAML bindings used for this Profile are:

- **HTTP POST binding** – the communication mechanism for an IdP to pass a SAML assertion to an RP. The HTTP POST binding defines a mechanism by which SAML protocol messages are transmitted within the base64-encoded content of an HTML form control. Advantages of this binding include (1) ease of implementation because no firewall reconfigurations are required; (2) scalability because HTTP POST is stateless (i.e., having no information about what occurred previously) and requires fewer hardware resources; and (3) HTTP POST is less complex and expensive to deploy than SAML Artifact based binding.
- **HTTP Redirect binding** – the communication mechanism for an RP to pass a SAML authentication request to an IdP. The HTTP Redirect binding defines a mechanism by which SAML protocol messages are embedded within an HTTP URL. Advantages of the HTTP Redirect binding are similar to those offered by the HTTP POST binding.

2.3 Use Cases

The usual portable identity model includes three main actors: the end user, the IdP, and the RP. In the main use cases within this model, the following always occurs:

1. The end user chooses to use an identity that he or she establishes with the IdP to interact with the RP;
2. The end user authenticates (e.g., enters a username and password) to the IdP;
3. The IdP asserts the identity of the end user to the RP via a SAML assertion; and
4. The RP relies on the identity information from the assertion to identify the end user.

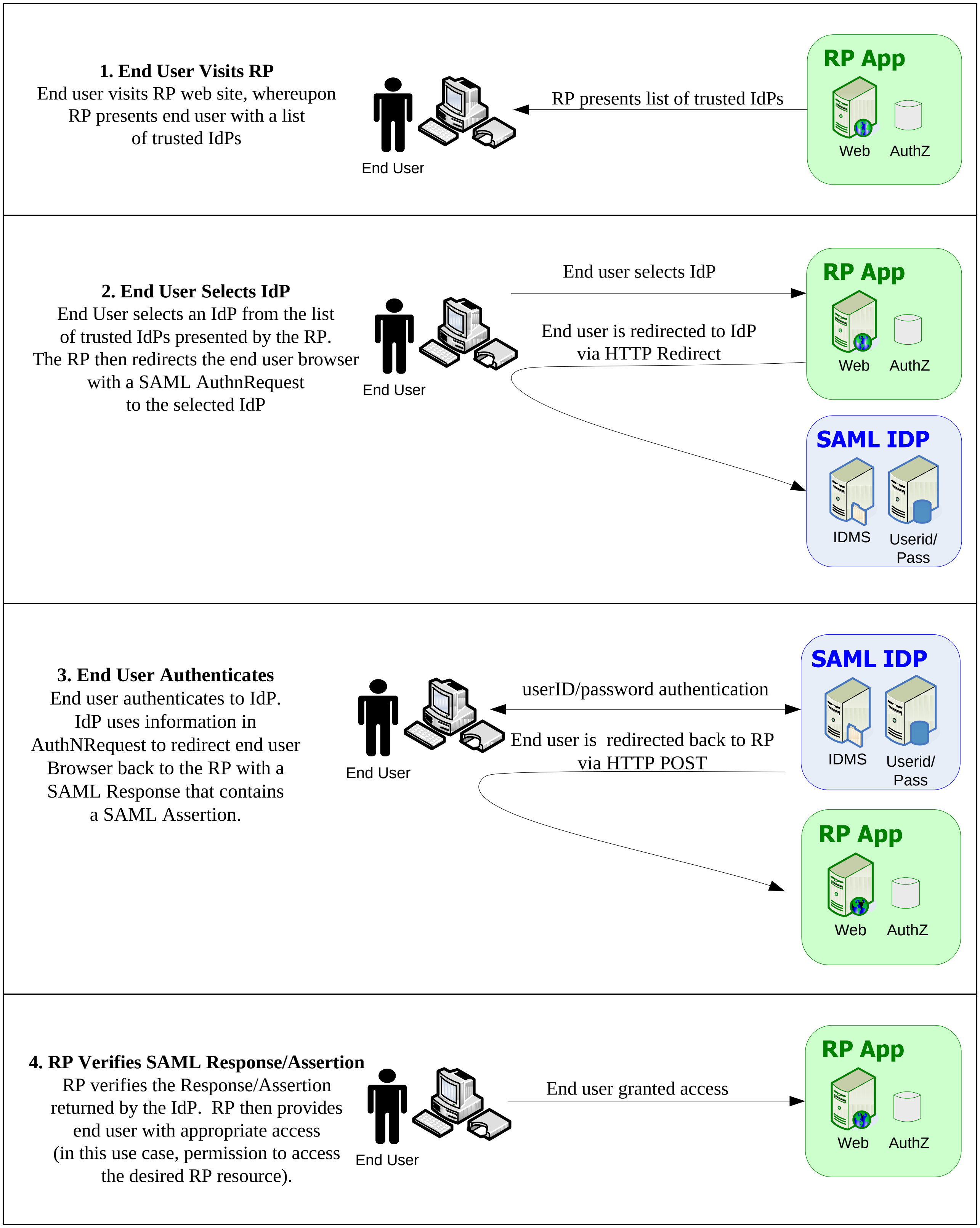
In this model, the end user does not have to create a new identity at every RP with which he or she interacts. In addition, the RP does not have to integrate credential management features (e.g., identity proofing, password reset) because those features are “outsourced” to the IdP.

This Profile defines two main SAML 2.0 use cases[4]: (1) end user starts at the RP, and (2) end user starts at the IdP. All features defined in this Profile (e.g., SSO, session reset) derive from the two main use cases.

[4] This Profile implicitly supports other use cases, including Enterprise RP/STS use cases.

1. **End User starts at the RP** –. The RP requests an assertion from the IdP. The RP request uses the HTTP Redirect binding, while the IdP response uses the HTTP POST binding. Figures 1 and 2 illustrate this use case.

Figure 1 Starting at the RP Use Case



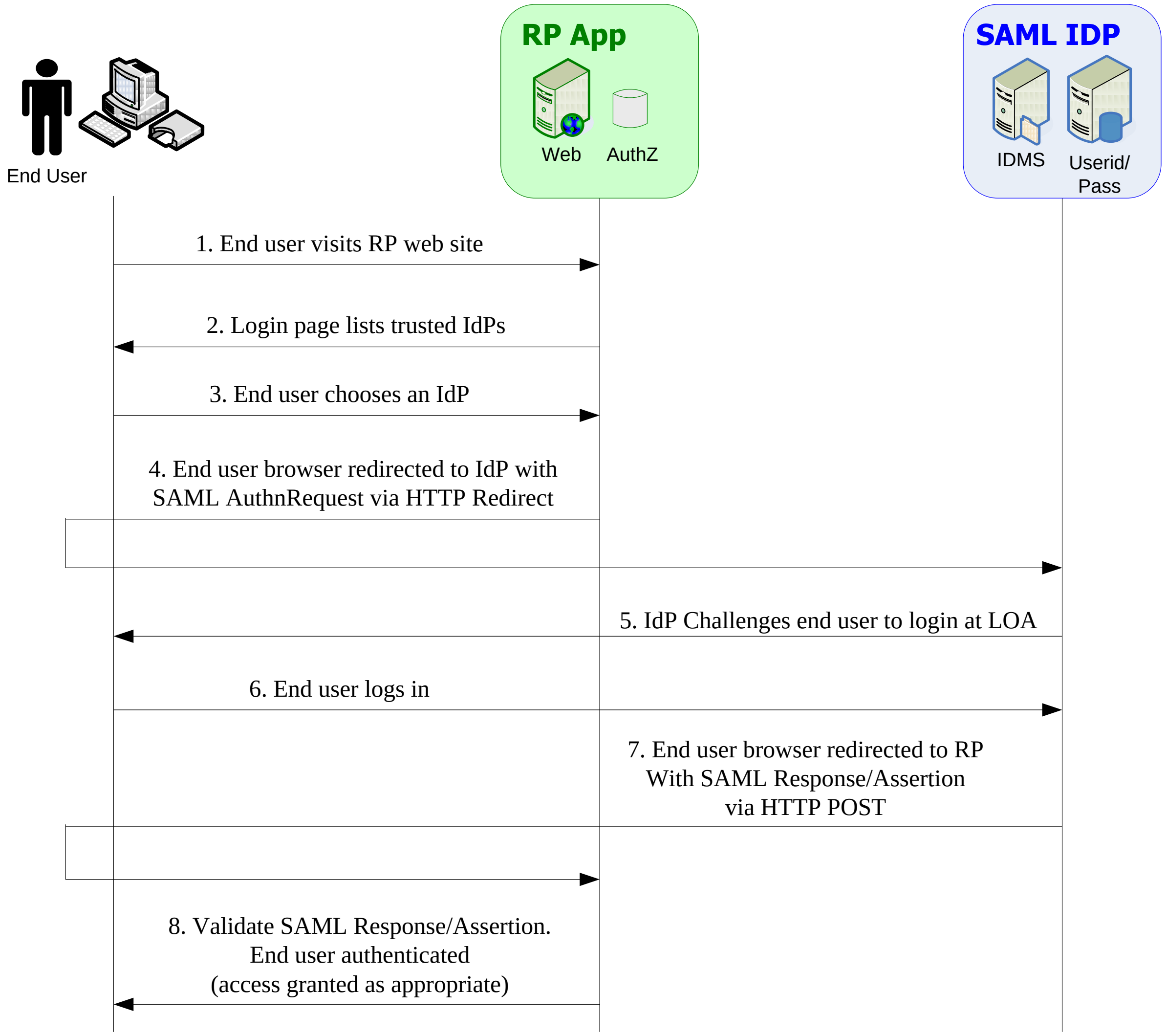
1. End User Visits RP
End user visits RP web site, whereupon RP presents end user with a list of trusted IdPs

2. End User Selects IdP
End User selects an IdP from the list of trusted IdPs presented by the RP. The RP then redirects the end user browser with a SAML AuthnRequest to the selected IdP

3. End User Authenticates
End user authenticates to IdP. IdP uses information in AuthNRequest to redirect end user Browser back to the RP with a SAML Response that contains a SAML Assertion.

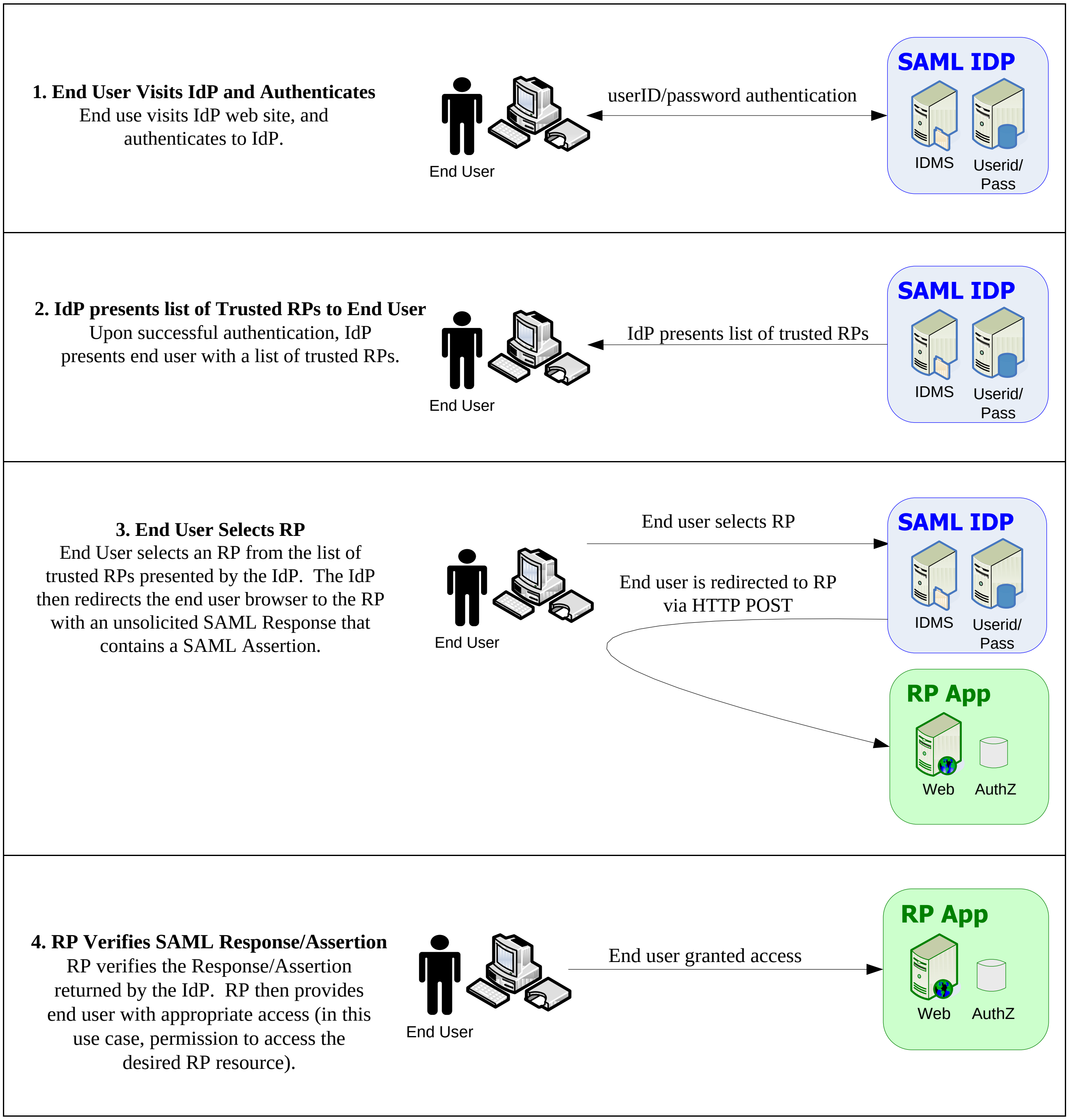
4. RP Verifies SAML Response/Assertion
RP verifies the Response/Assertion returned by the IdP. RP then provides end user with appropriate access (in this use case, permission to access the desired RP resource).

Figure 2 Starting at the RP Sequence Diagram


RP App
Web
AuthZ
SAML IDP
IDMS
Userid/
Pass
End User
1. End user visits RP web site
2. Login page lists trusted IdPs
3. End user chooses an IdP
4. End user browser redirected to IdP with
SAML AuthnRequest via HTTP Redirect
5. IdP Challenges end user to login at LOA
6. End user logs in
7. End user browser redirected to RP
With SAML Response/Assertion
via HTTP POST
8. Validate SAML Response/Assertion.
End user authenticated
(access granted as appropriate)

2. **End User starts at the IdP** – This is considered an unsolicited transaction because the RP does not request an assertion. Only HTTP POST binding is used. Figures 3 and 4 illustrate this use case.

Figure 3 Starting at the IdP Use Case



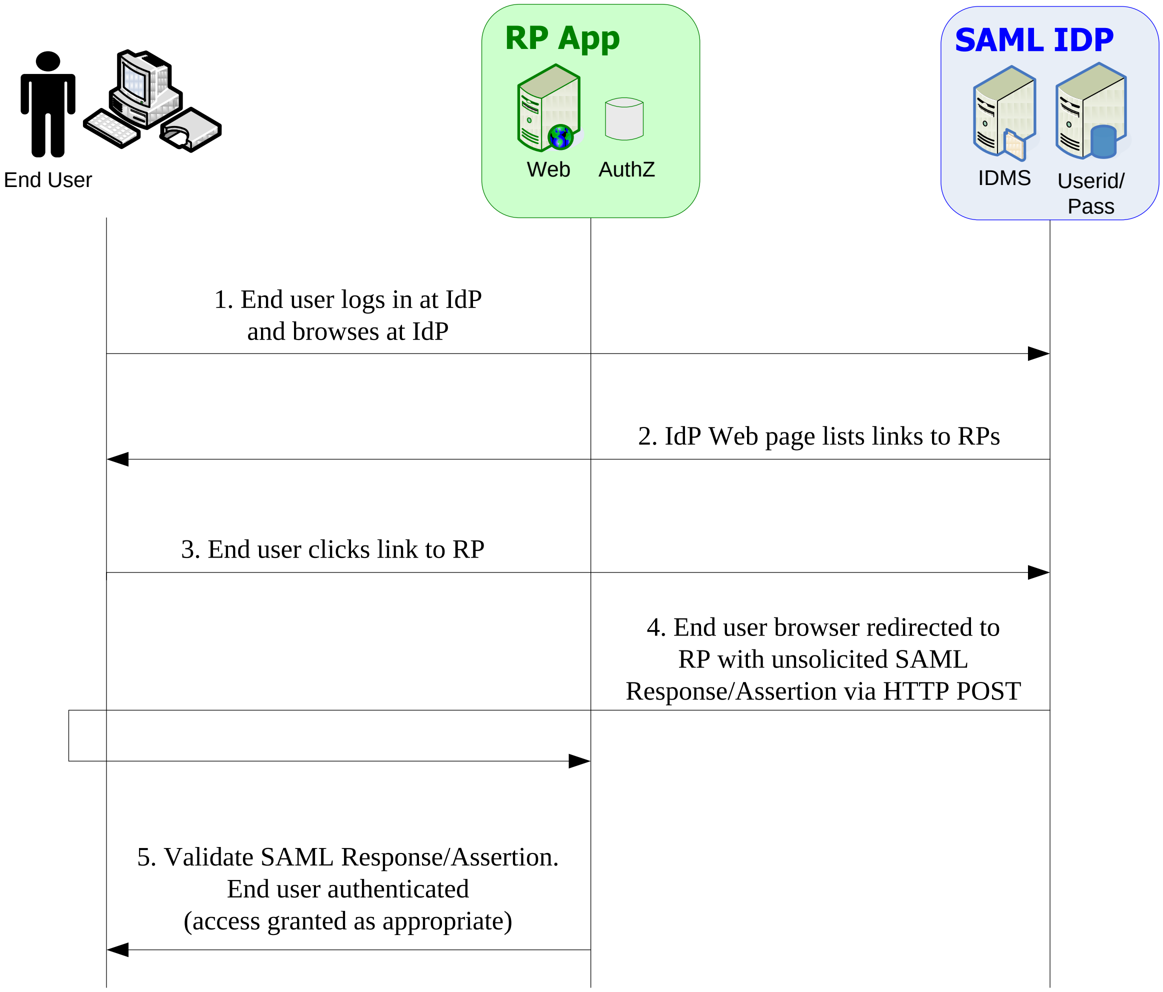
1. End User Visits IdP and Authenticates
End use visits IdP web site, and authenticates to IdP.

2. IdP presents list of Trusted RPs to End User
Upon successful authentication, IdP presents end user with a list of trusted RPs.

3. End User Selects RP
End User selects an RP from the list of trusted RPs presented by the IdP. The IdP then redirects the end user browser to the RP with an unsolicited SAML Response that contains a SAML Assertion.

4. RP Verifies SAML Response/Assertion
RP verifies the Response/Assertion returned by the IdP. RP then provides end user with appropriate access (in this use case, permission to access the desired RP resource).

Figure 4 Starting at the IdP (Unsolicited Assertion) Sequence Diagram


RP App
Web
AuthZ
SAML IDP
IDMS
Userid/
Pass
End User
1. End user logs in at IdP
and browses at IdP
2. IdP Web page lists links to RPs
3. End user clicks link to RP
4. End user browser redirected to
RP with unsolicited SAML
Response/Assertion via HTTP POST
5. Validate SAML Response/Assertion.
End user authenticated
(access granted as appropriate)

2.4 Features

The following sections describe the features included in this Profile.

2.4.1 Single Sign-on

Single Sign-on (SSO) can be achieved when the end user has recently authenticated and has an active session with the IdP. If policy permits, the end user is not prompted to log in (re-authenticate) when another RP accessed by the end user requests a SAML assertion. In other words, the end user is seamlessly logged into any other RP that interoperates with the IdP.

2.4.2 Session Reset

Session reset allows an RP to force end user re-authentication in order to obtain a fresh identity assertion. Reasons include, but are not limited to the following:

1. RP policy requires end user authentication to the IdP even when SSO is in effect;
2. The end user has been idle for a while, and the RP wants to confirm that the end user is still there;
3. The end-user wants to initiate a transaction deemed sensitive by the RP; and
4. The RP has a policy for maximum RP session duration.

The RP requests a session reset by sending a SAML `AuthnRequest` with the `ForceAuthn` attribute set to 'true' to the IdP responsible for the end user's current authentication session. Upon receipt, the IdP re-authenticates the end user, even if SSO is in effect or the IdP's own policies do not require re-authentication at that time (i.e., the end user's authentication session has not yet expired).

2.4.3 Attribute Exchange

This profile does not require the inclusion of any attributes in authentication assertions and does not prescribe attribute names. Communities of Interest should establish attribute naming conventions and/or use attribute names from well-known registries. An RP that requires attributes in authentication assertions must publish the required attributes via metadata. IdPs must also publish attributes they support via metadata.

This Profile does not preclude attribute exchange in accordance with the Backend Attribute Exchange Architecture and Interface Specification [BAE]. Readers should refer to BAE for guidance on implementing attribute exchange outside the context of web SSO between citizens and government.

2.4.4 Single Logout

Single Logout (SLO) is near-simultaneous logout of an end user from a specific authentication session and all active RP sessions associated with the authentication session. Therefore, SLO occurs within the context of SSO. The end user initiates SLO by selecting a link displayed by an RP or IdP.

SLO offers many challenges to agencies and organizations who choose to implement it. Foremost among these challenges are inconsistencies in SLO COTS product implementations that can result in interoperability issues, and usability concerns that can result in a poor end user experience. Due to these concerns, this Profile does not require the use of SLO, but does make recommendations as to its use (see Section 3.5).

2.5 Privacy

Privacy is of paramount importance. Section 3.3 of the *ICAM Trust Framework Provider Adoption Process (TFPAP) For Levels of Assurance 1, 2, and Non-PKI 3* [TFPAP] includes several privacy requirements which apply to this profile. Implementers are encouraged to follow these privacy requirements many of which can be accomplished outside the scope of SAML.

2.6 Security

IdPs and RPs must use approved cryptographic modules per [FIPS 140]. In accordance with [SAML2 Security], this Profile includes high-level security measures for SAML 2.0 message transactions (see Section 3 of this Profile for additional details). Section 3.3 of this Profile requires all SAML requests and assertions be validated against metadata. RPs should digitally sign <samlp:AuthnRequest>s. IdPs must always digitally sign the entire SAML assertion contained within a SAML response message. To address assertion disclosure threats, the SAML Assertion must be sent via a protected session (i.e., SSL/TLS)[5], and may be in encrypted form. Security benefits are as follows:

1. Digitally signing messages allows the message recipient to authenticate the sender as a trusted party. The recipient does not further process the received message until such positive verification;
2. Digitally signing message allows the message recipient to determine whether anyone or anything has tampered with the message (i.e., compromised message data integrity). The recipient does not further process a tampered message;
3. Digitally signing messages ensures non-repudiation (i.e., the sender cannot later deny that they sent the message); and
4. Digitally encrypting a SAML assertion ensures only intended recipients can read the contents of the SAML assertion, which contains personally identifiable information (i.e., confidential information).

2.7 End User Activation

The first time an end user authenticates to an RP via assertion, the RP will likely have to perform end user activation. End user activation is the process whereby an RP associates a new or existing local identity record (i.e., account[6]) with the end user's identifier from the IdP.

While the SAML 2.0 identity assertion provides the RP with a unique end user identifier, the RP often needs additional information about the end user before it can associate him/her with a local account and conduct a transaction. Sometimes that information can be retrieved from the assertion. Other times, the information can be retrieved directly from the end user and verified through an RP-determined process (e.g., knowledge-based questions/answers). The RP determines the need for activation and facilitates it when necessary. There are many activation use cases. Two activation use cases of particular interest are: existing account linking and new account provisioning.

In existing account linking, the RP has existing end user records that it can link to the identifier in the assertion. For instance, the Social Security Administration (SSA) has records for all U.S. citizens, many of whom it has not conducted business with online. For example, by correlating the information it

[5] See Section 3.4 for implementation details.

[6] An account does not imply that the end user has local credentials.

receives from the assertion with information in their databases, SSA can link the end user’s credential at the IdP with an existing local account.

In new account provisioning, the RP has no prior knowledge of the end user and must establish an account for the end user. The RP uses information gathered from the assertion and other processes determined by the RP to establish the new account and associate it with credential at the IdP.

Both use cases are discussed further below. In either case, the RP application does not have to allow access to its services immediately after receiving the assertion. For example, the RP may delay end user access if additional steps are required (e.g., out-of-band review and approval of some or all data entered by the end user). Appendix B provides an example activation process.

2.7.1 Existing Account Linking

If the end user already has an account with the RP, the RP may be able to use the information contained in the assertion (i.e., attributes) to automatically link the identifier in the assertion with the existing account. If the information in the assertion is insufficient to definitively identify the end user, the RP application could ask the end user to answer questions based on information contained in their existing records in order to verify that they are the person in question (i.e., knowledge-based authentication). Other processes can be defined by the RP to collect and verify information about the end user. The processes can be online or out-of-band. For example, the RP can mail a special code to the end user to verify the end user's address. Once the identifier from the assertion is linked to the account, subsequent visits by the end user with an assertion should result in immediate access to the RP application.

Note that an authentication assertion exchanged using SAML 2.0 must never be used to give an end user access to an application with a higher LOA requirement than is present in the assertion, even if the accounts are linked.

2.7.2 New Account Provisioning

The first time an end user visits an RP application, the application may not have an account for the end user. In this case, the RP needs to establish an account and associate the end user's identifier from the IdP with the new account. The RP usually needs some information about the end user in order to establish the account. This information can be supplied by the end user through interactive prompting of the end user, or by the IdP through backend attribute exchange. The RP must determine the information it needs and the process for collecting and verifying the needed information. Once the account is provisioned, subsequent visits by the end user with an assertion should result in immediate access to the RP application.

2.8 Programmed Trust

In addition to the governance outlined in [TFPAP], some mechanism to indicate which RPs and IdPs are approved for use must be provided. For the ICAM SAML 2.0 Profile, ICAM issues and distributes metadata to each ICAM member. In addition, ICAM must approve the certificate used by ICAM members to sign their metadata prior to publication[7].

[7] See section 3.3.1.1.d for more information.

2.8.1 Metadata

SAML 2.0 message exchange between two ICAM-approved systems requires each to have specific knowledge about the other prior to trusted technical interoperation. One example of metadata is the URL of the service with which other systems will deliver SAML messages. Without such knowledge, other ICAM-approved systems do not know where to send SAML messages. Metadata describes and conveys such information. In general:

1. Metadata is the primary means of trust within ICAM. Therefore, it must be updated and consumed frequently[8].
2. Signed metadata is used to bind ICAM members to their digital signature and encryption keys.
3. Prior to run time, trust of ICAM members' signing and encryption certificates is determined when metadata is configured into the ICAM member system.
4. At run time, ICAM members must validate that the key used to sign inbound assertions matches the message sender's key in metadata.

ICAM maintains and distributes metadata for all ICAM members. All ICAM members must produce and submit (and should publish) their own metadata, and consume the metadata of others as appropriate:

- Federal ICAM members:
  a. Must produce a metadata file with an `<md:EntityDescriptor>` element formed in accordance with Section 3.3.1 of this Profile.
  b. Must digitally sign the `<md:EntityDescriptor>` element using an ICAM-approved certificate.
  c. Should publish the most recent version of their signed metadata via HTTPS.
  d. Must immediately update and re-submit metadata to ICAM and if applicable, re-publish metadata when their metadata information changes.
  e. Must verify metadata for correctness and completeness prior to consumption.
  f. Should check for and consume new or revised metadata on a periodic basis as prescribed by ICAM.
- Non-Federal ICAM members:
  a. Produce metadata as required by their TFP.
  b. Submit metadata to their TFP as required by their TFP.
     i. The TFP consolidates its members' `<md:EntityDescriptor>`s into an `<md:EntitiesDescriptor>`.
     ii. The `<md:EntitiesDescriptor>` must be signed using a key that is negotiated with ICAM.
  c. Consume metadata published by ICAM.

Failure to consume and configure metadata completely and correctly can preclude technical interoperation, or result in unexpected consequences or negative impacts to any number of ICAM member systems. ICAM Members should only consume metadata that is published or approved by ICAM.

It should be noted that section 3.3 of this Profile directly incorporates elements of the OASIS SAML 2.0 Metadata Interoperability Profile V.2 [IOP] currently in committee draft.

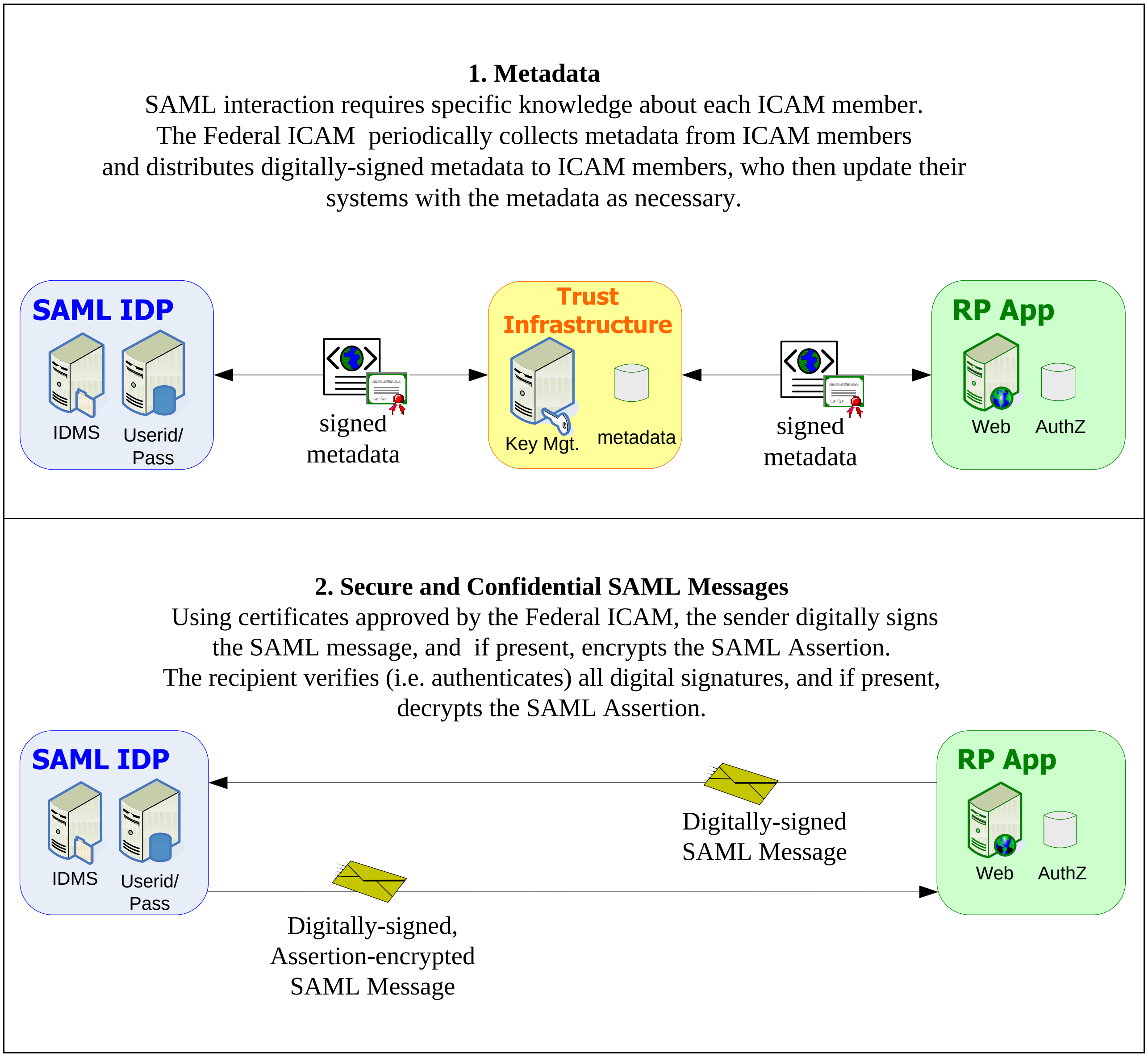
[8] Frequent publication and consumption of metadata serves a similar purpose to that of certificate revocation lists and should be treated with equal importance.

Despite its role in facilitating metadata distribution, ICAM is not involved in authentication transaction processing. ICAM members use the metadata to interact directly with each other for authentication transactions purposes. This Profile addresses metadata in accordance with [SAML2 Metadata], which includes:

1. Standards-based, XML encoded metadata files; and
2. Digitally signed metadata for the following purposes:
    a. Authenticate the metadata owner as a trusted participant; and
    b. Ensure metadata integrity (i.e., no tampering has occurred).

Figure 5 illustrates the high-level programmed trust process flow for applicable to all SAML 2.0 uses cases.

Figure 5 High-level Programmed Trust Process Flow



1. Metadata

SAML interaction requires specific knowledge about each ICAM member. The Federal ICAM periodically collects metadata from ICAM members and distributes digitally-signed metadata to ICAM members, who then update their systems with the metadata as necessary.

2. Secure and Confidential SAML Messages

Using certificates approved by the Federal ICAM, the sender digitally signs the SAML message, and if present, encrypts the SAML Assertion. The recipient verifies (i.e. authenticates) all digital signatures, and if present, decrypts the SAML Assertion.

SAML IDP
IDMS
Userid/ Pass
Digitally-signed SAML Message
RP App
Web
AuthZ
Digitally-signed, Assertion-encrypted SAML Message

3. TECHNICAL PROFILE

Like most specifications, SAML 2.0 provides options. Where necessary, the Federal government may further specify or remove an option in order to achieve better security, privacy, or interoperability. The following sections outline the Federal ICAM Profile for the SAML 2.0 specification.

3.1 Authentication Request

1. The `<samlp:AuthnRequest>` MUST include a `<saml:Issuer>` element matching the `EntityID` in the metadata of the RP.
    a. The `EntityID` MUST be a URL that is in the RP's control.
2. Omitting `<saml:Subject>` and `<saml:Conditions>` from `<samlp:AuthnRequest>` is RECOMMENDED.
    a. Conditions are useful for delegation scenarios. However, delegation is out of scope for this Profile. If Federation partners wish to use `<saml:Conditions>`, they SHOULD establish an agreement as to its use.
3. Omitting `<saml:Scoping>` from `<samlp:AuthnRequest>` is RECOMMENDED.
    a. `<saml:Scoping>` and the extensions necessary to enable it are out of scope for this Profile. If Federation partners wish to use `<saml:Scoping>`, they SHOULD establish an agreement as to its use.
4. `ForceAuthn` MUST be supported.
    a. `ForceAuthn` MAY be used to require the IdP to force the end user to authenticate.
5. `isPassive` MUST be supported.
    a. If `isPassive` is true, the IdP MUST NOT take control of the end user interface (i.e., browser).
6. IdPs MUST use the `AssertionConsumerServiceURL` in metadata.
    a. If `AssertionConsumerServiceURL` is present in `<samlp:AuthnRequest>`, the IdP SHOULD compare the `AssertionConsumerServiceURL` with the requestor's metadata, and MUST end the transaction if there is no match.
7. `<samlp:AuthnRequest>` MUST include `<samlp:RequestedAuthnContext>` with one or more `<saml:AuthnContextClassRef>s` .
    a. The value of the `Comparison` operator MUST be set to "`exact`" unless RP and IdP have previously negotiated the use of other operators.
    b. The value of at least one `<saml:AuthnContextClassRef>` element MUST be one of the following ICAM LOA URLs:
        - http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel1
        - http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel2
        - http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel3
        - http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel4
        - Other ICAM-approved LOA URL value
8. `<samlp:NameIDPolicy> Format` MUST be present.
    a. For Authentication transactions between citizens and government the value for `<samlp:NameIDPolicy> Format` MUST be set to one of the following:
        - urn:oasis:names:tc:SAML:2.0:nameid-format:persistent[9]

[9] The persistent `<NameID>` format requires a pseudonymous identifier that is unique to an IdP/RP pair for the end user.

- urn:oasis:names:tc:SAML:2.0:nameid-format:transient[10]
- urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

1. The use of pseudonyms (persistent identifiers) is strongly RECOMMENDED

9. The `<samlp:AuthnRequest>` issued by the RP MUST be communicated to the IdP using the HTTP-REDIRECT or HTTP-POST binding.
10. For compatibility reasons, `<samlp:AuthnRequest>` SHOULD be signed.
11. If present, `<samlp:AuthnRequest> ProtocolBinding` MUST be set to `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`.
12. `AttributeConsumingServiceIndex` MAY be included in the `<samlp:AuthnRequest>` in order to indirectly indicate a set of attributes the RP desires.

3.2 Response[11]

1. An IdP MAY send unsolicited `<samlp:Response>`s .
   a. If received, RPs MUST process an unsolicited `<samlp:Response>` s.
   b. RPs SHOULD accept `<saml:Assertion>`s only from IdPs whose `EntityID`s are found in metadata.
2. The `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST` binding MUST be supported.
   a. Parties who wish to use any other SAML binding SHOULD negotiate its use. In addition, it is RECOMMENDED that the parties follow the directives in Section 2.6, Security.
3. The `<samlp:Response>` MUST include a `<saml:Issuer>` element whose value matches the `EntityID` for the IdP in metadata.
4. If the authentication request is successful,
   a. `<samlp:Response>` MUST contain exactly one `<saml:Assertion>` or one `<saml:EncryptedAssertion>`.
   b. `<samlp:Response>` MUST be sent via a protected session (i.e., SSL/TLS)[12].
5. The `<saml:Assertion>` MUST contain exactly one `<saml:AuthnStatement>`.
   a. `<saml:AuthnStatement>` SessionIndex parameter SHOULD be present.
   b. `<saml:AuthnStatement>` SessionNotOnOrAfter MAY be present.
6. `<saml:AuthnContext>` MUST be present with exactly one `<saml:AuthnContextClassRef>` elements.
   a. The value of `<saml:AuthnContextClassRef>` element MUST be set to one of the following ICAM LOA URLs:
      - http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel1
      - http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel2
      - http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel3
      - http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel4
      - Other ICAM-approved LOA URL value

[10] A transient identifier is used only one time.

[11] Further ICAM work on the governance of SAML IdPs is expected.

[12] See Section 3.4 for implementation details.

   b. The RP SHOULD compare the LOA in the Response with the LOA in the IdP's metadata, and end the transaction if the LOA in the Assertion is higher than the LOA for the IdP published in metadata.

7. The `<saml:Assertion>` MUST contain a `<saml:Subject>`.
   a. `<saml:Subject>` MUST contain a `<saml:NameID>`.
   b. For Authentication transactions between citizens and government, `<saml:NameID> Format` in the response MUST be either of the following:
      - urn:oasis:names:tc:SAML:2.0:nameid-format:transient
      - urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
      - urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
        1. The use of pseudonyms (persistent identifiers) is strongly RECOMMENDED
   c. `<saml:SubjectConfirmationData>` MUST be used per [SAML2 Profiles].
      - For holder-of-key assertions, the `Method` attribute of `<saml:SubjectConfirmationData>` MUST be urn:oasis:names:tc:SAML:2.0:cm:holder-of-key
8. The `<saml:Assertion>` MUST contain zero or one `<saml:AttributeStatement>`s.
   a. Each `<saml:AttributeStatement>` MUST contain one or more `<saml:Attribute>`s, which MAY contain any number of `<saml:AttributeValue>`s.
   b. The IdP MUST set the value of the `NameFormat` attribute to urn:oasis:names:tc:SAML:2.0:attrname-format:uri.
   c. `<saml:AttributeStatement>` MUST use `<saml:Attribute>` and MUST NOT use `<saml:EncryptedAttribute>`.
   d. The use of URI-formatted Attribute names from well known registries is RECOMMENDED.
   e. IdPs MUST NOT send attributes that are not requested by the RP.
   f. RPs SHOULD NOT accept `<saml:Assertion>`s containing attributes that have not been negotiated out of band or via metadata.
9. The `<saml:Assertion>` MUST include a `<saml:Conditions>`.
10. The `<saml:Assertion>` MUST be digitally signed.

3.2.1 LOA 4 Holder-of-key Assertion Requirements

At LOA 4, bearer assertions SHALL NOT be used solely to authenticate the end user to the RP. However, holder-of-key assertions made by the IdP MAY be used to bind keys or other attributes to an identity. Holder-of-key assertions may be used at LOA 4 provided that the following requirements are met[13]:

1. The end user MUST authenticate to the IdP using a certificate whose issuer is cross-certified with the Federal Bridge Certification Authority or issued under the Common Policy Framework Certification Authority at a certificate policy that meets the requirements of LOA 4 (See [FBCA CP] or [CPFCA CP]).
2. The IdP MUST generate a holder-of-key assertion that references the LOA 4 certificate that the end user used to authenticate to the IdP.
   a. The value of at least one `<saml:AuthnContextClassRef>` element MUST be:

[13] See [NIST SP 800-63-1] Section 10.3.2.4, Level 4.

- http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel4.

b. The value of the Method attribute of <saml:SubjectConfirmationData> MUST be urn:oasis:names:tc:SAML:2.0:cm:holder-of-key.
- The <saml:SubjectConfirmationData> element MUST include a <ds:KeyInfo> with one <ds:X509Certificate> element as a child of <ds:X509Data>.
- The <ds:X509Certificate> element MUST contain the certificate that the end user used to authenticate to the IdP.

3. The RP MUST verify that the end user possesses the private key to the certificate that is referenced in the holder-of-key assertion using a LOA 4 protocol as specified in [NIST SP 800-63-1] Section 9, Authentication Process. Furthermore the RP must validate that the certificate issuer is cross-certified with the Federal Bridge Certification Authority.

3.3 Metadata

3.3.1 Metadata Production

1. ICAM Member metadata MUST include at least one <md:EntityDescriptor> element.
   a. <md:EntityDescriptor> MUST contain a unique entity-id.
   b. <Organization> SHOULD be present and include OrganizationName or OrganizationDisplayName.
   c. validUntil and cacheDuration Attributes MUST be present and their values set using risk-based methods.
      - It is RECOMMENDED that cacheDuration not exceed 64800 seconds (18 hours).
   d. Prior to metadata distribution, the <md:EntityDescriptor> or <md:EntitiesDescriptor> MUST be digitally signed with an ICAM-approved certificate.
   e. <md:KeyDescriptor> MUST include a <ds:KeyInfo> with one <ds:X509Certificate> element as a child of <ds:X509Data>.
      - Other sub elements of <ds:KeyInfo> are permitted (e.g., <ds:KeyValue>) but they MUST all represent the same key.
2. RPs MUST include a <md:SPSSODescriptor> in their <md:EntityDescriptor> element.
   a. protocolSupportEnumeration MUST be present and MUST include urn:oasis:names:tc:SAML:2.0:protocol.
   b. WantAssertionsSigned MUST be set to true.
   c. If the RP uses Assertion encryption, <md:SPSSODescriptor> MUST contain at least one <md:KeyDescriptor>.
   d. <md:SPSSODescriptor> MAY contain <md:SingleLogOutService>.
   e. <md:SPSSODescriptor> MAY contain <md:AttributeConsumingService>.
      i. RPs wishing to request attributes in an <samlp:AuthnRequest> MUST publish one or more <md:AttributeConsumingService> in their metadata that includes the set of desired attributes.
3. IdPs MUST include <md:IDPSSODescriptor> in their <md:EntityDescriptor> element.

a. `protocolSupportEnumeration` MUST be present and MUST include `urn:oasis:names:tc:SAML:2.0:protocol`.

b. `<md:IDPSSODescriptor>` MUST contain at least one `<md:KeyDescriptor>`.

c. One or more `<md:SingleSignOnService>` MUST be present in `<md:IDPSSODescriptor>`.

- `Binding` MUST be set to urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect or urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST

d. `<md:IDPSSODescriptor>` MAY contain `<md:AttributeAuthorityDescriptor>`.

- IdPs SHOULD include `<Attribute>` for attributes they are capable of sharing.

e. `<md:EntityDescriptor>` MUST include the IdP's LOA expressed in accordance with OASIS *Expressing Identity Assurance in SAML 2.0,* Section 3 [Assurance]

- The LOAs expressed in metadata MUST contain the highest LOA the IdP is certified to assert.
- The IdP SHOULD list all the LOA's it is certified to assert in metadata.

3.3.2 Metadata Consolidation

1. ICAM MAY consolidate `<md:EntitiesDescriptor>` metadata files issued by other organizations into one `<md:EntitiesDescriptor>` file for ICAM use. Support for the use of nested `<md:EntitiesDescriptor>` elements in a single file is REQUIRED.

   a. The root element of consolidated metadata MUST be `<md:EntitiesDescriptor>`.

   - The root element MAY contain one or more `<md:EntitiesDescriptor>` elements.
   - The root element MAY also contain one or more `<md:EntityDescriptor>` elements.

   b. ICAM MUST digitally sign the root `<md:EntitiesDescriptor>` and all its contents.

   - Each `<md:EntitiesDescriptor>` within the root element MUST be signed by the issuing organization using an ICAM-approved certificate.

   c. `validUntil` and `cacheDuration` attributes MUST be present.

3.3.3 Metadata Consumption

1. ICAM member implementations MUST support at least one of the following metadata import mechanisms:

   a. Local file (e.g., obtained out of band).

   b. Remote resource at fixed location accessible via HTTP 1.1 [RFC 2616] over SSL v3 or TLS 1.1 (and higher) [RFC 2818].

   - In the case of HTTP resolution, ICAM member implementations SHOULD support use of the "ETag" header for cache management.
   - Other cache control support is OPTIONAL.
   - ICAM member implementations MAY import metadata from more than one source.

2. At consumption time, the metadata consumer MUST perform XML-signature verification at the root element level.

3. At consumption time, the metadata consumer MUST support one of the following mechanisms for establishment of signature key trust:

   a. Direct comparison against preconfigured keys.

   b. Path-based certificate validation against one or more trusted root certificates combined with either certificate revocation list (CRL) or OCSP.

4. The `validuntil` attribute in an `<md:EntityDescriptor>` or `<md:EntitiesDescriptor>` element MUST be honored. ICAM members MUST refresh the metadata before it is expired. If for some reason the metadata cannot be refreshed before it expires, the member MUST make a risk-based determination whether or not to continue transacting with the effected entities.
5. Metadata consumers SHOULD be capable of processing one or more consolidated metadata per section 3.3.2.

3.4 Security

1. SSL v3 or TLS 1.1 (and higher) MUST be used to protect all protocol endpoints.
   a. The use of TLS 1.2 is RECOMMENDED.
   b. It is RECOMMENDED that the TLS implementation conform to [NIST SP 800-52].
2. `<saml:Assertion>`s, and metadata MUST be digitally signed.
3. The RP MUST validate that the key used to sign the `<saml:Assertion>` matches the key in the metadata for that `entityID` in the `<saml:Assertion>`.
4. IdPs and RPs MUST use [FIPS 140] validated cryptographic modules and algorithms for XML signing and encryption.
5. The use of SHA1 hashes for signatures is NOT RECOMMENDED.
   a. The use of SHA256 is RECOMMENDED
6. AES128, ECDSA, and ECDH-ES are RECOMMENDED for signing and encryption.

3.5 Single Logout (SLO)

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 following are recommendations Communities of Interest who wish to utilize SLO SHOULD follow.

1. The RP SHOULD offer the end user a choice between simple logout (logging out only from the RP) and SLO.
   a. When SLO is initiated at the RP, the <LogoutRequest> SHOULD be communicated over SSL v3 or TLS 1.1 (and higher), and use the HTTP Redirect binding.
2. If the end user logs out while at an IdP resource, the IdP SHOULD terminate the end user's authentication session and SHOULD initiate SLO (i.e., terminate all RP sessions associated with that authentication session).
   a. Before proceeding, the IdP SHOULD inform the end user that he or she will be logged out of all active RP sessions, and the end user SHOULD confirm the request.

<Logout Request>

1. `<LogoutRequest>` SHOULD be signed.
2. Upon receiving `<LogoutRequest>`, an IdP SHOULD send `<LogoutRequest>` to every RP associated with the authentication session – except for the RP that submitted `<LogoutRequest>` to the IdP since that RP already logged out the end user.
3. Upon receiving `<LogoutRequest>`, an RP SHOULD terminate the end user's RP session.
4. The IdP SHOULD log the end user out locally (i.e., terminate the authentication session) and send a `<LogoutResponse>` to the originating RP to indicate SLO completion.

<LogoutResponse>

1. `<LogoutResponse>` MUST be communicated over SSL v3 or TLS 1.1 (and higher), and SHOULD use the HTTP Redirect binding.

2. `<LogoutResponse>` SHOULD be signed.
3. If the Status of a `<LogoutResponse>` is not urn:oasis:names:tc:SAML:2.0:status:Success, the recipient of `<LogoutResponse>` SHOULD 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.
    a. Otherwise, the recipient of `<LogoutResponse>` SHOULD inform the end user that he or she has logged out successfully

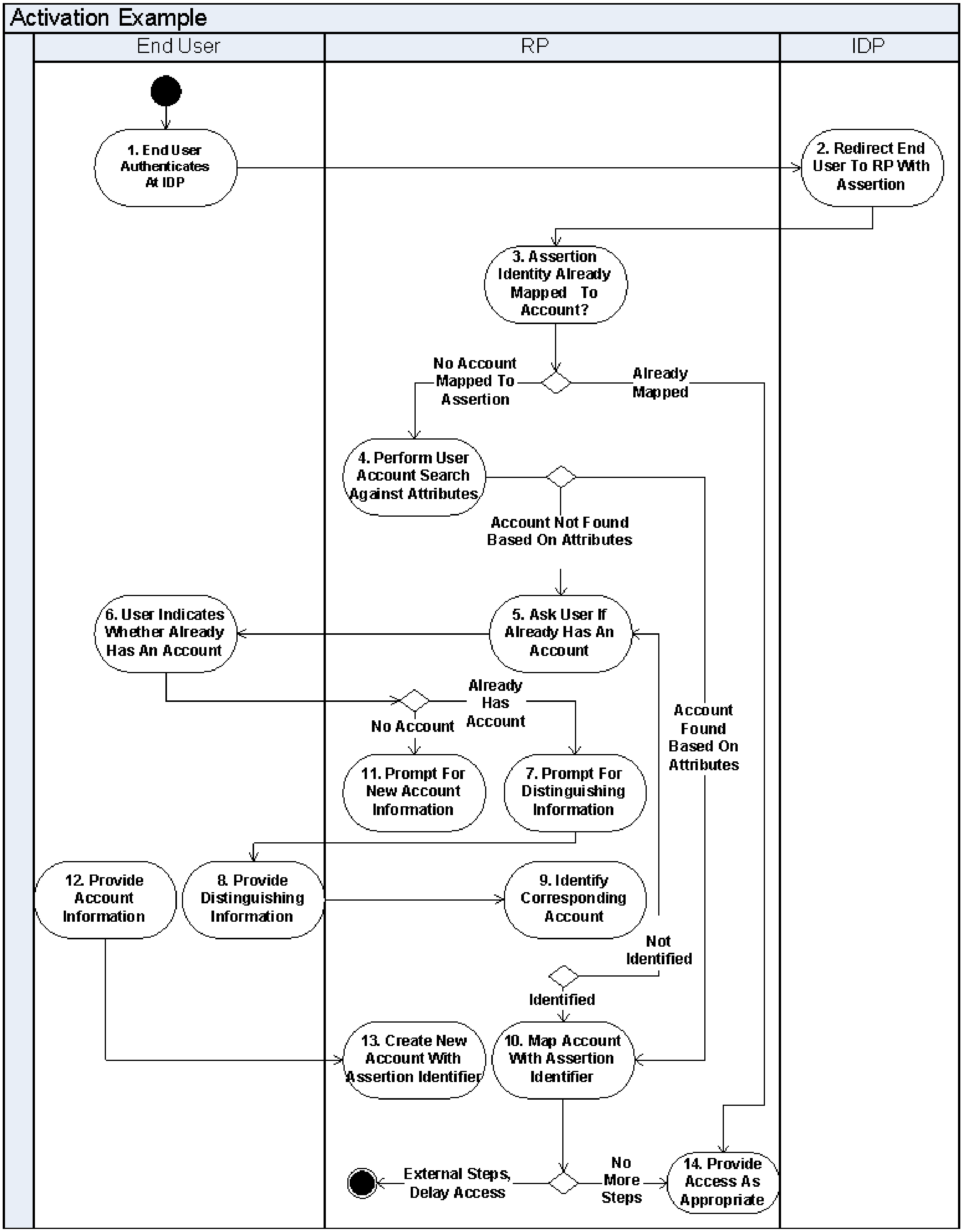
3.6 IdP Discovery

1. IdP Discovery using Common Domain Cookie (CDC) MAY be implemented. Communities of Interest SHOULD define their own common domain.

APPENDIX A – SAML 2.0 WEB SSO PROFILE MESSAGE SUMMARY

SAML Use Case	SAML Request Message	SAML Response Message	Comments
Starting at the RP (Single Sign-on)	AuthnRequest	Response	▪ HTTP Redirect for AuthnRequest ▪ HTTP POST for Response ▪ Protected session (SSL/TLS) ▪ Assertion may be in encrypted form ▪ Signed Assertion
Starting at the IdP (Unsolicited Assertion)	None	Response	▪ No AuthnRequest because end user starts at the IdP ▪ HTTP POST for Response ▪ Protected session (SSL/TLS) ▪ Assertion may be in encrypted form ▪ Signed Assertion
Session Reset	AuthnRequest	Response	▪ HTTP Redirect for AuthnRequest ▪ AuthnRequest ForceAuthn attribute set to true ▪ HTTP POST for Response ▪ Protected session (SSL/TLS) ▪ Assertion may be in encrypted form ▪ Signed Assertion

APPENDIX B – END USER ACTIVATION EXAMPLE


Activation Example
End User
RP
IDP
1. End User Authenticates At IDP
2. Redirect End User To RP With Assertion
3. Assertion Identity Already Mapped To Account?
No Account Mapped To Assertion
Already Mapped
4. Perform User Account Search Against Attributes
Account Not Found Based On Attributes
Account Found Based On Attributes
5. Ask User If Already Has An Account
6. User Indicates Whether Already Has An Account
Already Has Account
No Account
11. Prompt For New Account Information
7. Prompt For Distinguishing Information
12. Provide Account Information
8. Provide Distinguishing Information
9. Identify Corresponding Account
Not Identified
Identified
13. Create New Account With Assertion Identifier
10. Map Account With Assertion Identifier
External Steps, Delay Access
No More Steps
14. Provide Access As Appropriate

APPENDIX C – GLOSSARY

Term	Definition
Account	An account is used to associate transactional records with an end user or organization. Presence of an account does not necessarily mean that there are credentials (e.g., username and password) associated with the account.
Approved	Acceptance by ICAM to technically interoperate with other ICAM members.
Assert	To make a statement about the properties of a user or user's act of authentication.
Authentication Session	Period of time that an end user remains trusted after the end user authenticates. That is because an IdP typically does not require an end user to re-authenticate for every page requested. Each IdP defines its own authentication session duration. If an end user returns to the IdP and an earlier authentication session has expired, the IdP 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.
Consolidated Metadata	Multiple <md:EntityDescriptor> or <md:EntitiesDescriptor> files into a single <md:EntitiesDescriptor> file.
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. In this Profile, encryption pertains to SSL v3 or TLS 1.1 (and higher), encryption and/or XML encryption, depending upon the Level of Assurance.
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 IdP and/or RP.
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).

Term	Definition
Holder-of-Key Assertion	A holder-of-key assertion contains a reference to a public key (corresponding to a private key) or a symmetric key possessed by the end user. The RP requires the end user to prove possession of the private key or secret that is referenced in the assertion. In proving possession, the end user also proves that he or she is the rightful owner of the assertion.
Identity Provider	A kind of service provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers (relying parties) within a federation, such as with web browser profiles.
Metadata	Information shared between endpoints (e.g., RP, IdP) necessary for technical interoperation.
Persistent	Ability to maintain data.
Protected Session	A session wherein messages between two participants are encrypted and integrity is protected using a set of shared secrets called session keys. A participant is said to be authenticated if, during the session, he, she or it proves possession of a long term token in addition to the session keys, and if the other party can verify the identity associated with that token. If both participants are authenticated, the protected session is said to be mutually authenticated. One way to implement a protected session is SSL/TLS, which is required for this Profile.
Pseudonymous Identifier	Private end user pseudonym that will only be used with one site. The site will always know it's you when you come back, but it won't be able to look up any other information about you, or correlate your profile with other sites.
Relying Party	A system entity (i.e., stand-alone system or group of applications that rely on a central authentication system) that decides to take an action based on information from another system entity. For example, a SAML Relying Party depends on receiving assertions from an asserting party (e.g., a SAML Identity Provider) about a subject. A Relying Party is also referred to as a Service Provider.
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.

Term	Definition
Security Token Service (STS)	An STS provides a standards-based method of converting security tokens across different formats.
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 Sign-on (SSO)	Once an end user has authenticated their identity at an IdP, he or she may, by their choice, move among RPs that interoperate with the IdP without re-authenticating. In other words, the end user is seamlessly logged into any other RP that interoperates with the IdP. For privacy considerations, end users must take explicit actions to opt-in to SSO. SSO applies to assertion based ICAM 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.

APPENDIX D - ACRONYMS

Acronym	Definition
CRL	Certificate revocation List
GSA	General Services Administration
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICAM	Identity, Credential, and Access Management
IdP	Identity Provider
IETF	Internet Engineering Task Force
LOA	Level of Assurance
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OGP	Office of Governmentwide Policy
OMB	Office of Management and Budget
RFC	Request for Comment
RP	Relying Party
SAML	Security Assertion Markup Language
SLO	Single Log-out
SSA	Social Security Administration
SSL	Secure Sockets Layer
SSO	Single Sign-on
STS	Security Token Service
TFPAP	Trust Framework Provider Application Process
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XML	Extensible Markup Language

APPENDIX E - DOCUMENT REFERENCES

[Assurance] Expressing Identity Assurance in SAML 2.0
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.pdf

[BAE] Backend Attribute Exchange Architecture and Interface Specficiation
http://www.idmanagement.gov/awg/documents/BackendArchitectureInterfaceSpec.pdf

[EGCA CP] "X.509 Certificate Policy for the E-Authentication Certification Authorities", Version 1.4, August 16, 2007
http://www.idmanagement.gov/fpkipa/documents/EGovCA-CP.pdf

[eGov Profile] Libery Alliance Project eGov Profile v1.5
http://www.projectliberty.org/liberty/content/download/4711/32210/file/Liberty_Alliance_eGov_Profile_1.5_Final.pdf

[FIPS 140] Federal Information Processing Standards Publication 140-2; Security Cryptographic Modules
http://csrc.nist.gov/publications/nistpubs/

[IOP] OASIS Committee Specification, SAML V2.0 Metadata Interoperability Profile Version 2.0, Working Draft 1, Mar 2010
http://www.oasis-open.org/committees/download.php/36645/draft-sstc-metadata-iop-2.0-01.pdf

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

[NIST SP 800-63-1] Electronic Authentication Guideline; National Institute of Science and Technology (NIST Special Publication 800-63-1, December 2011
http://csrc.nist.gov/publications/nistpubs/

[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

[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

[RFC 2119] Request for Comments 2119, Key words for use in RFCs to Indicate Requirement Levels.
http://www.ietf.org/rfc/rfc2119.txt

[RFC 2616] Hypertext Transfer Protocol.
http://www.ietf.org/rfc/rfc2616.txt

[RFC 2218] HTTP Over TLS
http://www.ietf.org/rfc/rfc2818.txt

[RFC 3339] Date and Time on the Internet: Timestamps
http://www.ietf.org/rfc/rfc3339.txt

[SAML2 *] All the SAML2 document reference that immediately follow.
All available at http://docs.oasis-open.org/security/saml/v2.0

[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 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 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 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 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

[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 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

[Scheme Adopt] ICAM Identity Scheme Adoption Process
http://www.idmanagement.gov/documents/IdentitySchemeAdoptionProcess.pdf

[TFPAP] ICAM Trust Framework Provider Adoption Process (TFPAP) For Levels of Assurance 1, 2, and Non-PKI 3
http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf

[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/