Federal Identity, Credentialing, and Access Management

Identity Metasystem Interoperability 1.0 Profile

Version 1.0.1

Release Candidate

November 18, 2009

Document History

Status	Release	Date	Comment	Audience
Template	0.0.0	7/15/09	Initial Draft	Internal
Release Candidate	1.0.0	9/18/09	Revised per internal review	General Distribution
Release Candidate	1.0.1	11/18/09	Revised per ICAM AWG comments	AWG

Editors

Matt Tebo	Dave Silver	Terry McBride
John Bradley		

Executive Summary

Identity Metasystem Interoperability (IMI) 1.0 as described in this document has completed the scheme adoption process and has been adopted by ICAM for the purpose of Level of Assurance (LOA) 1-3 identity authentication. Proper use of this Profile ensures 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 authentication experience at a Federal Government site.

This Profile does not alter the IMI standard, but rather specifies which areas of the standard can be used for technical interoperability with government applications, and how they will be used.

The objective of this document is to fully define the ICAM IMI 1.0 adopted scheme so that persons implementing this adopted scheme, or otherwise managing or supporting an implementation, fully and correctly understand its use in ICAM transaction flows.

The IMI 1.0 specification, ratified by OASIS in July 2009, is the core of the IMI protocol. IMI 1.0 is based on a set of protocol specifications that facilitate portable identity through open standards such as Web Services Security (WS-Security), Web Services Trust (WS-Trust), and SOAP.

IMI 1.0 can be used to conduct both low and higher-risk transactions with the Federal Government. At this time, IMI 1.0 is suitable for LOA 1-3 authentication only. No modifications to IMI 1.0 are necessary to attain these levels. An increase in the LOA is dependant on factors outside of this Profile such as identity proofing and credential issuance. See [NIST SP 800-63] for more information.

IMI 1.0 is a framework that allows end users to manage their digital identity, and employ it at different Relying Parties (RPs) for the purpose of accessing online resources. In IMI 1.0, a digital identity is represented by claims[1] about an end user (e.g., gender, age). Sets of claims are represented in Information Cards. End users may possess one or more Information Cards containing different sets of claims from different Identity Providers (IdPs). As such, an end user may have a portfolio of Information Cards analogous to the cards they have in their physical wallet (e.g., credit card, driver's license).

A key component of IMI 1.0 is the Card Selector, which is software installed on the end user's computer that is tightly coupled with the end user's browser. The Card Selector is a virtual wallet for managing the end user's digital identity.

IMI 1.0 supports various types of Information Cards. However, this Profile allows only Managed Cards, which are issued by an external IdP. Claims are communicated by an IdP to an RP in a digitally signed security token (token). IMI 1.0 supports different token types depending on RP requirements. However,

[1] "Claim" is an IMI term. Other identity management frameworks use the term "attribute"

this Profile only allows the exchange of a Security Assertion Markup Language (SAML) 1.1 assertion token (assertion).

Section 2 provides a high-level overview of the adopted scheme, including use cases, and process flows. The section is intended to provide the context and understanding necessary to optimally implement and manage the adopted scheme. 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 guidance on how to implement the IMI 1.0 adopted scheme (i.e., send or receive IMI 1.0 messages within ICAM). It is assumed that the reader of this section is familiar with the IMI 1.0 specification [IMI 1.0].

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], 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]. These authentication schemes ensure that the end user does not have to create a new identity at every Relying Party (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 Identity Provider (IdP). The adoption process includes assessment of the scheme for compliance with [NIST SP 800-63] and other privacy and security requirements.

Identity Metasystem Interoperability (IMI) 1.0 as described in this document has completed the scheme adoption process and has been adopted by ICAM for the purpose of Level of Assurance (LOA) 1-3 identity authentication. Proper use of this Profile ensures 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 does not alter the IMI standard, but rather specifies which areas of the standard can be used for technical interoperability with government applications, and how they will be used. Where this Profile does not explicitly provide IMI 1.0 guidance, one must implement in accordance with IMI 1.0 requirements as documented by the Organization for the Advancement of Structured Information Standards (OASIS) and the Information Card Foundation (ICF).

1.2 Objective and Audience

The objective of this document is to fully define the ICAM IMI 1.0 adopted scheme so that persons implementing this adopted scheme, or otherwise managing or supporting an implementation, fully and correctly understand its use in ICAM transaction flows. The definition includes:

1. A high-level overview of the ICAM IMI 1.0 adopted scheme and its features;
2. General requirements for IdPs and RPs that extend outside the reach of IMI 1.0 specifications (e.g., privacy, security, activation, governance).
3. An ICAM deployment profile of the IMI 1.0 specification.

Section 2 provides a high-level overview of the adopted scheme, and includes discussion of features, use cases, and process flows. The section is intended to provide the context and understanding necessary to optimally implement and manage the adopted scheme. 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 guidance on how to implement the IMI 1.0 adopted scheme (i.e., send or receive IMI 1.0 messages within ICAM). It is assumed that the reader of this section is familiar with the IMI 1.0 specification [IMI 1.0].

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].

2. SCHEME OVERVIEW

2.1 IMI 1.0 Overview

The IMI 1.0 specification, ratified by OASIS in July 2009, is the core of the IMI protocol. IMI 1.0 is based on a set of protocol specifications that facilitate portable identity through open standards such as Web Services Security (WS-Security), Web Services Trust (WS-Trust), and SOAP.

IMI 1.0 can be used to conduct both low and higher-risk transactions with the Federal Government. At this time, IMI 1.0 is suitable for LOA 1-3 authentication only. No modifications to IMI 1.0 are necessary to attain these levels. An increase in the LOA is dependant on factors outside of this Profile such as identity proofing and credential issuance. See [NIST SP 800-63] for more information.

IMI 1.0 is a framework that allows end users to manage their digital identity, and employ it at different RPs for the purpose of accessing online resources. In IMI 1.0, a digital identity is represented by claims[2] about an end user (e.g., gender, age). Sets of claims are represented in Information Cards. End users may possess one or more Information Cards containing different sets of claims from different IdPs. As such, an end user may have a portfolio of Information Cards analogous to the cards they have in their physical wallet (e.g., credit card, driver's license).

IMI 1.0 supports many types of Information Cards. However, this Profile allows only Managed Cards, which are issued by an external IdP. The Information Card itself is not an authentication token. Rather, the Information Card contains metadata about the IdP as well as supported claims and other information. Fields in the Information Card include:

1. A graphical representation for the issued Information Card;

[2] "Claim" is an IMI term. Other identity management frameworks use the term "attribute"

2. The name of the IdP who issued the Information Card;
3. A unique identifier for the Information Card;
4. The date the Information Card was issued and when it expires;
5. An ordered list of the IdP's service endpoints where tokens can be requested;
6. The list of claim types that are offered by the IdP;
7. The location of the privacy statement of the IdP; and
8. The list of token types that are offered by the IdP.

Claims are communicated by an IdP to an RP in a digitally signed security token (token). IMI 1.0 supports different token types depending on RP requirements. However, this Profile only allows the exchange of a Security Assertion Markup Language (SAML) 1.1 assertion token (assertion). See [IMI 1.0] Section 7.5 for the complete list of predefined claims. See Section 3.1 of this Profile for additional claims per LOA.

A key component of IMI 1.0 is the Card Selector, which is software installed on the end user's computer that is tightly coupled with the end user's browser. The Card Selector is a virtual wallet for managing the end user's digital identity. The Card Selector acts as an intermediary between the IdP, RP, and end user. In IMI 1.0, all protocol communications flow through the end user's browser and Card Selector. In addition, the Card Selector:

1. Provides a consistent user experience across RPs;
2. Virtually eliminates phishing;
3. Minimizes the impact on the RP's user interface;
4. Is supported by multiple browsers; and
5. Is currently available from commercial and open source vendors for most operating systems.

To indicate its token and claims requirements, an RP publishes a security policy via a HyperText Markup Language (HTML) OBJECT tag[3]. When an end user attempts to access an RP-protected resource, his or her browser responds to the OBJECT tag by passing the RP's security policy to the Card Selector. Upon receipt of the security policy, the Card Selector:

1. Reads the RP's security policy;
2. Determines which of the end user's Information Cards meet the security policy; and
3. Presents only those Information Cards to the end user for selection to use in the transaction.

Once the end user selects an Information Card from his or her virtual wallet, the Card Selector requests an authentication token from the IdP associated with the Information Card. Upon successfully obtaining an authentication token, the Card Selector forwards it through the browser to the RP, whereupon the RP makes access control decisions based on information in the assertion (i.e., decides whether to allow the end user to access the requested resource).

[3] See Section 3.2 of this document for details on the RP security policy.

2.1.1 Conceptual Diagrams

In IMI (and therefore in this Profile), a transaction starts when an end user attempts to access an RP's protected resource. Figures 1 and 2 illustrate the interaction between the end user, Card Selector, RP, and IdP in this use case.

Figure 1 IMI Use Case

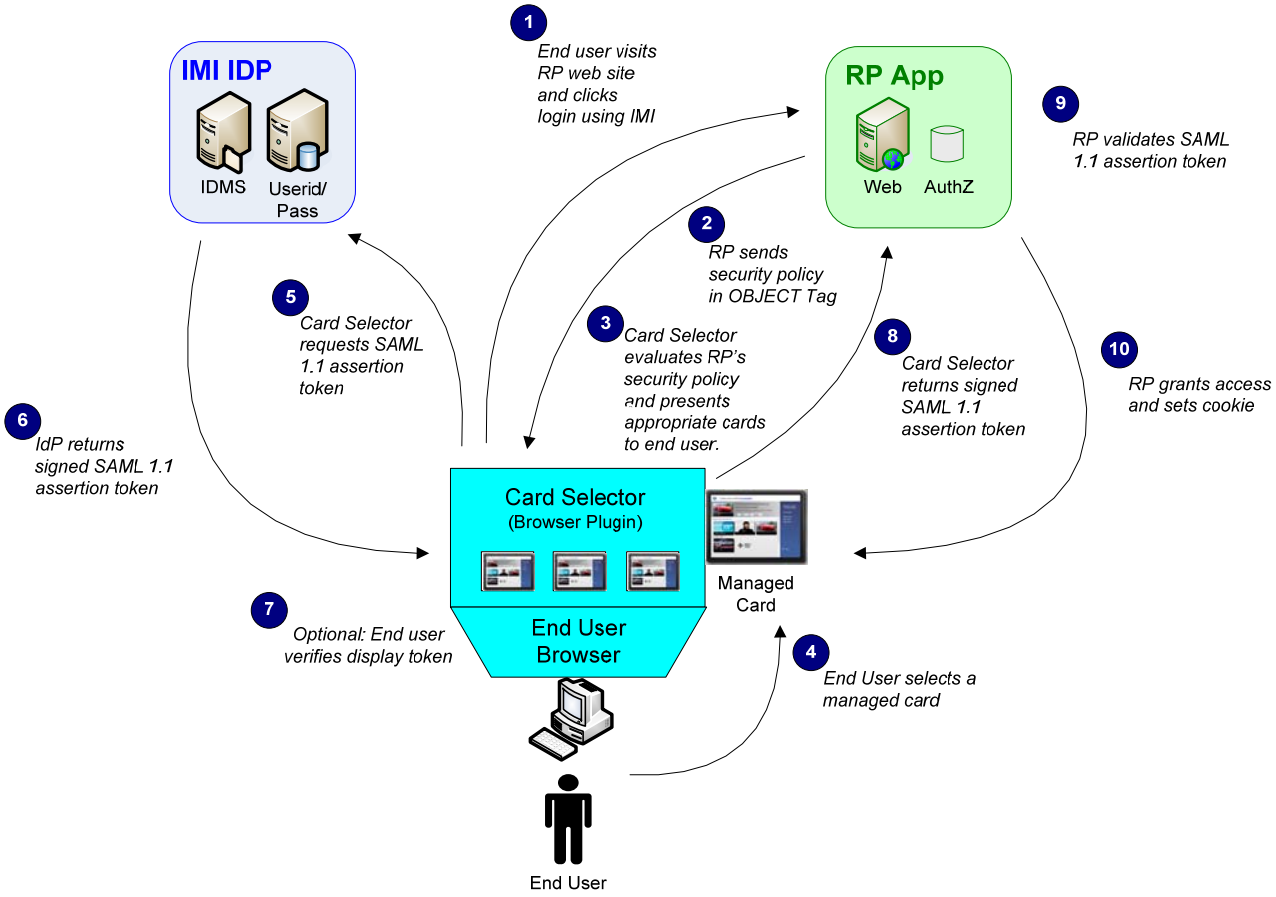
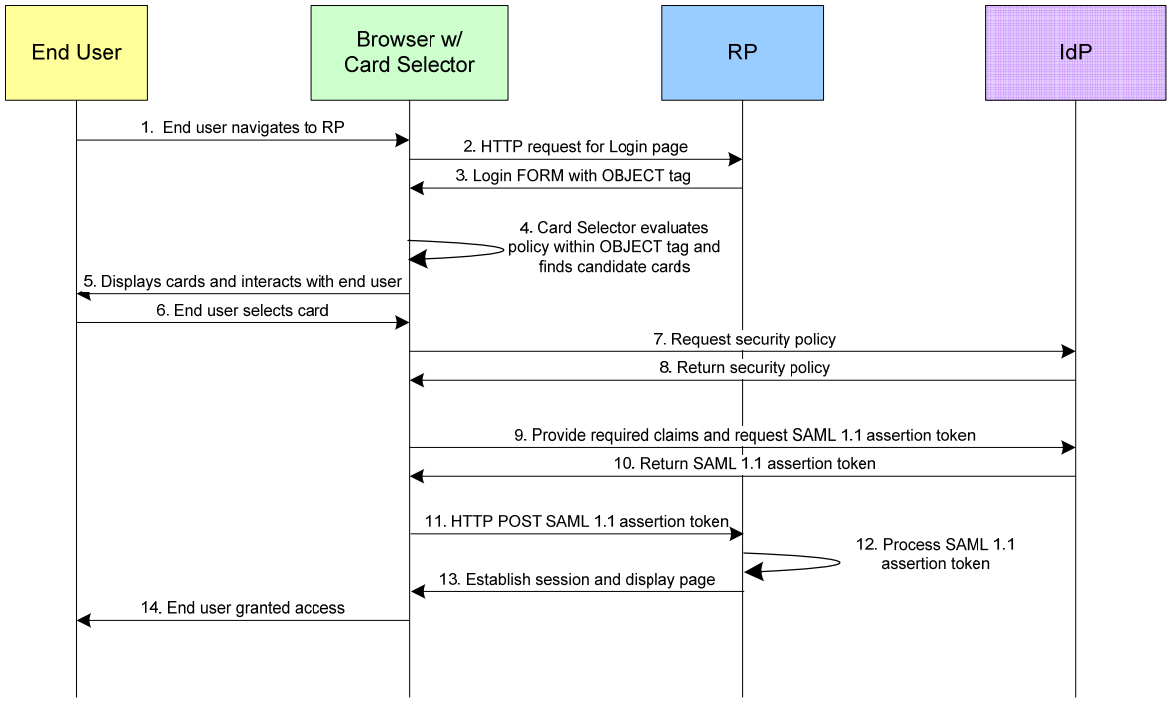


Figure 2 IMI Sequence Diagram



2.2 Privacy

Privacy is of paramount importance. *ICAM Trust Framework Provider Adoption Process (TFPAP) For Levels of Assurance 1, 2, and Non-PKI 3* [TFPAP] includes several privacy requirements. Those privacy requirements must be followed. Privacy requirements include, but are not limited to the following:

1. The RP must not request claims beyond what it needs (i.e., RP Application claim requests must be consistent with the data contemplated in their Privacy Impact Assessment).
2. Prior to any claim exchange:
   a. The end user must be notified of the claims to be exchanged; and
   b. The end user must consent to the exchange. An RP cannot require the end user to consent to claim exchange as a condition of accessing the RP. An alternative method for obtaining and verifying claim or of obtaining another credential must be provided.
3. The location of the IdP's privacy statement is included in the Information Card.

2.3 Security

This Profile includes the following high-level security measures for IMI 1.0 message transactions (see Section 3 for additional details):

1. The RP verifies that the IdP is an ICAM-authorized LOA 1, 2, or 3 IdP.
2. The IdP, RP, and Card Selector use either SSL/TLS, or WS-Security to positively identify one another and to secure all direct communication.
3. At the application layer, the IdP digitally signs and encrypts assertions to ensure integrity and confidentiality.

Note that at LOA 1, all claims contained in the assertion are considered to be self-asserted (i.e., provided by the end user without verification). Therefore, at LOA 1 RPs should not assume that this information is true. For LOA 2 and LOA 3, the RP may or may not be able to rely on the accuracy of the information provided. However, at LOA 2 and LOA 3, information verified by the IdP as part of the identity proofing process is generally considered reliable. In all cases, RPs should make a risk-based decision whether to use the information provided.

2.4 End User Activation

The first time an end user authenticates to an RP via IMI, the RP must perform end user activation. End user activation is the process an RP uses to associate a new or existing local identity record (i.e., account[4]) with the end user's identifier from the IdP.

While the IMI 1.0 token 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 IMI token. Other times, the information can be retrieved directly from the end user and verified through an RP-determined process (e.g., knowledge-based questions and answers). The RP determines the need for activation and facilitates it when necessary. There are two primary use cases for activation: 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 IMI 1.0 token. For instance, the Social Security Administration (SSA) has records for all U.S. citizens, many of whom it has not conducted business with online. By correlating the claims in the IMI 1.0 token 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 IMI 1.0 token and from 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 IMI 1.0 token. 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 A provides an example activation process.

2.4.1 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 IMI 1.0 token (i.e., claims) to automatically link the identifier in the IMI 1.0 token with the existing account. If the information in the IMI 1.0 token 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 IMI 1.0 token is linked to the account,

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

subsequent visits by the end user with a IMI 1.0 token should gain them immediate access to the RP application.

2.4.2 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. 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 a IMI 1.0 token should gain them immediate access to the RP application.

2.5 Programmed Trust

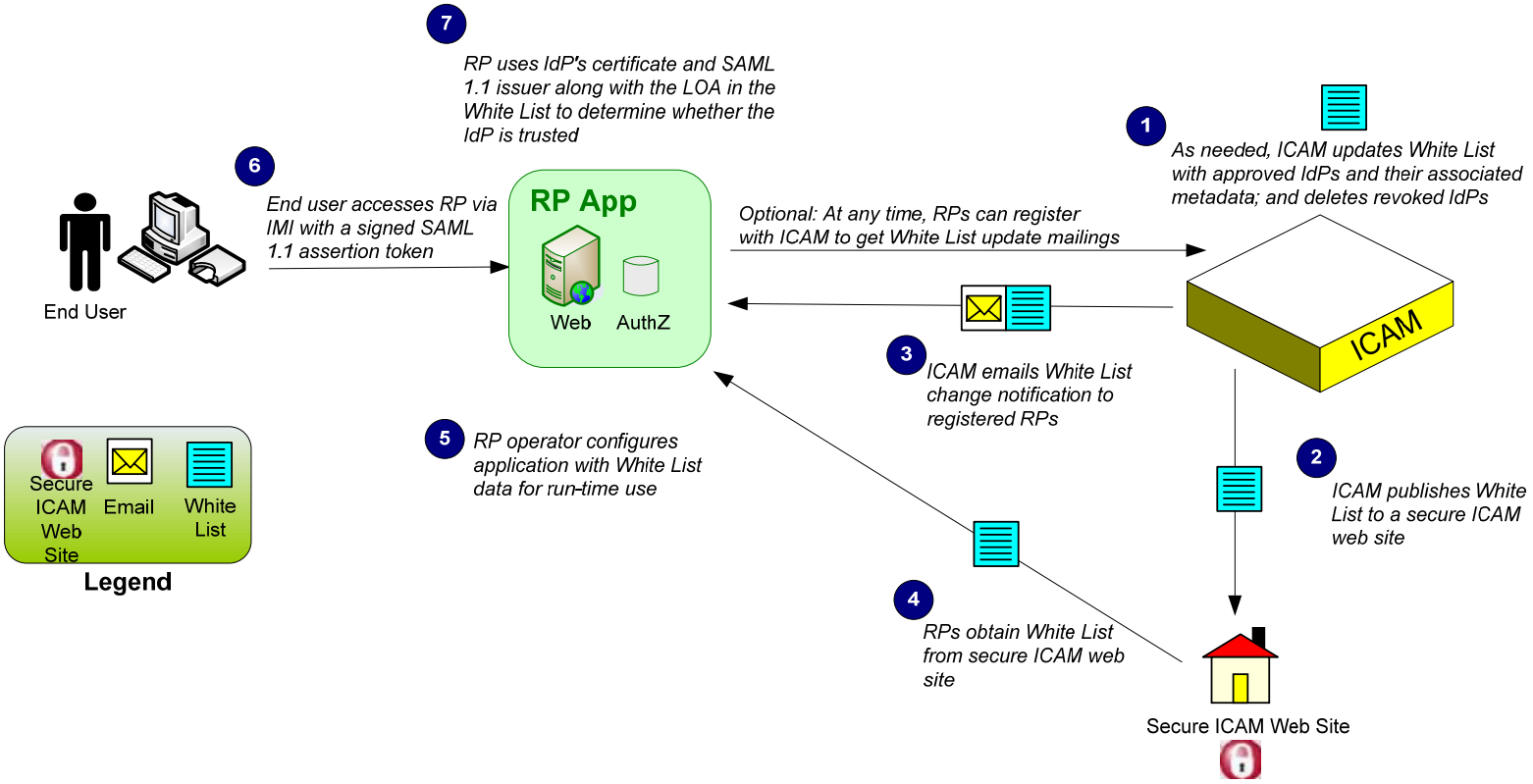
In addition to the governance outlined in [TFPAP], each ICAM adopted scheme must provide some mechanism to indicate to RPs which IdPs are approved for use within ICAM[5]. For the IMI 1.0 adopted scheme, ICAM maintains and distributes a White List containing metadata for each approved IdP. The metadata consists of (a) issuer-id, (b) issuer X.509 certificate, (c) assurance level, and (d) optional claim information.

During IMI 1.0 token validation, the RP must confirm that the IdP is on the White List. In order to do this, RPs must use both the `issuer` field and X.509 certificate from the assertion to find a positive match in the White List. If the IdP from whom the RP has received an assertion is not on the White List, the RP must reject the token. If a matching IdP entry is found, the RP must verify that the IdP's LOA in the White List meets the LOA in the assertion.

The IMI 1.0 White List is posted on a secure ICAM website. In addition, change notifications are delivered by email to RPs registered to receive White List updates. When ICAM revokes an IdP, it immediately updates the White List, posts it to its secure web site, and emails notification to registered RPs. Therefore, RPs (especially unregistered RPs) are encouraged to check the White List frequently. Figure 3 illustrates the high-level programmed trust process flow for the end user starts at the RP use case.

[5] An approved IdP has passed applicable [TFPAP] requirements, and whose assertions can therefore be relied upon (trusted) by RPs of an LOA equal to or lower than the trusted IdP.

Figure 3 High-level Programmed Trust Process Flow



3. TECHNICAL PROFILE

3.1 General

1. This profile is restricted to the exchange of SAML 1.1 assertion token types.
    a. The IdP MAY support other token types. However, the exchange of those tokens is outside the scope of this profile.
2. SSL/TLS or WS-Security [WSS] MUST be used to protect all protocol endpoints.
3. It is RECOMMENDED that Extended Validation (EV) certificates be used to secure protocol endpoints.[6]
4. The RP SHOULD perform Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) checks for certificates used to perform digital signing if available.
5. Managed Cards are supported for LOA 1 through 3 only.
6. All other types of Information Cards (e.g. Personal Cards) are out of scope for this Profile.
7. The use of display tokens (see [IMI 1.0]) is RECOMMENDED.
8. This profile defines the following assurance level claims that indicate trust per [TFPAP] at the corresponding LOA:
    a. LOA 1
    `http://idmanagement.gov/icam/2009/09/imi_1.0_profile#assurancelevel1`
    b. LOA 2
    `http://idmanagement.gov/icam/2009/09/imi_1.0_profile#assurancelevel2`
    c. LOA 3
    `http://idmanagement.gov/icam/2009/09/imi_1.0_profile#assurancelevel3`
9. The value of the LOA claim MUST be the White List URL (see Section 2.5 of this document for additional detail).

3.2 SAML 1.1 Token Claim Encoding

In this Profile, IMI 1.0 claim names and values are encoded as SAML 1.1 `Attributes`.

1. Claim names MUST be a URL containing a path separated by a forward slash.
    a. The last character of the URL MUST NOT be a forward slash.
2. In the SAML 1.1 assertion token, the IdP MUST split the claim name so that:
    a. The final component of the URL MUST be encoded as the SAML 1.1 `AttributeName`.
    b. All components before the final slash MUST be encoded as the SAML 1.1 `AttributeNamespace`.

The following is an example of valid SAML 1.1 `Attribute` for the claim `http://idmanagement.gov/icam/2009/09/imi_1.0_profile#assurancelevel2`:

[6] The recommendation for EV certificate Distinguished Names (DN) content guarantees a consistent private personal identifier (PPID) when certificates expire or are rolled over.

```
<saml:Attribute
  AttributeName="imi_1.0_profile#assuranclevel2"
  AttributeNamespace="http://idmanagement.gov/icam/2009/09">
      <saml:AttributeValue>https://idmanagement.gov/EXAMPLE/WHITELIST/URL
      </saml:AttributeValue>
</saml:Attribute>
```

3.3 Relying Party

1. The RP SHOULD reject SAML 1.1 assertion tokens containing claims and/or token types not expressed in their security policy.[7]
2. The RP MUST include exactly one `assurancelevel[1-2-3]` required claim type (See Section 3.1) in its security policy, equal to the RP's required LOA.
3. For all other claim types, it is RECOMMENDED that the RP security policy include only claim types registered with the ICF Schemas Working Group [ICF SWG].
    a. Other claim types MAY be requested depending on the RP's policy.
4. When requesting a token for authentication, the RP MUST include the Private Personal Identifier (PPID) as a required claim in its security policy.
    a. PPID `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier`
5. Requested token types MUST be SAML 1.1
6. The claim name MUST be constructed from a SAML 1.1 assertion token by concatenating the following three items: AttributeNamespace, "/", and AttributeName.
7. The RP's X.509 certificate Distinguished Name (DN) MUST include Common Name (CN).
8. The RP MAY use an RP Secure Token Server (RP/STS).
9. It is Recommended that issuer be omitted from the RP's security policy.
10. The RP MUST verify that the IdP is an ICAM-authorized IdP through verification of issuer-ids and server certificates against a White List.

[7] Unsolicited claims may indicate a Denial of Service (DOS) or other type of attack.

The following is a sample OBJECT tag for conveying the RP's security policy.

```
<OBJECT type="application/infocard" name="xmlToken">
 <PARAM Name="tokenType" Value="urn:oasis:names:tc:SAML:1.0:assertion">
 <PARAM Name="requiredClaims" Value="
   http://idmanagement.gov/icam/2009/09/imi_1.0_profile#assuranclevel2
   http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier
 "/>
 <PARAM name="optionalClaims" Value="
    http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirth
  "/>
</OBJECT>
```

3.4 Information Card

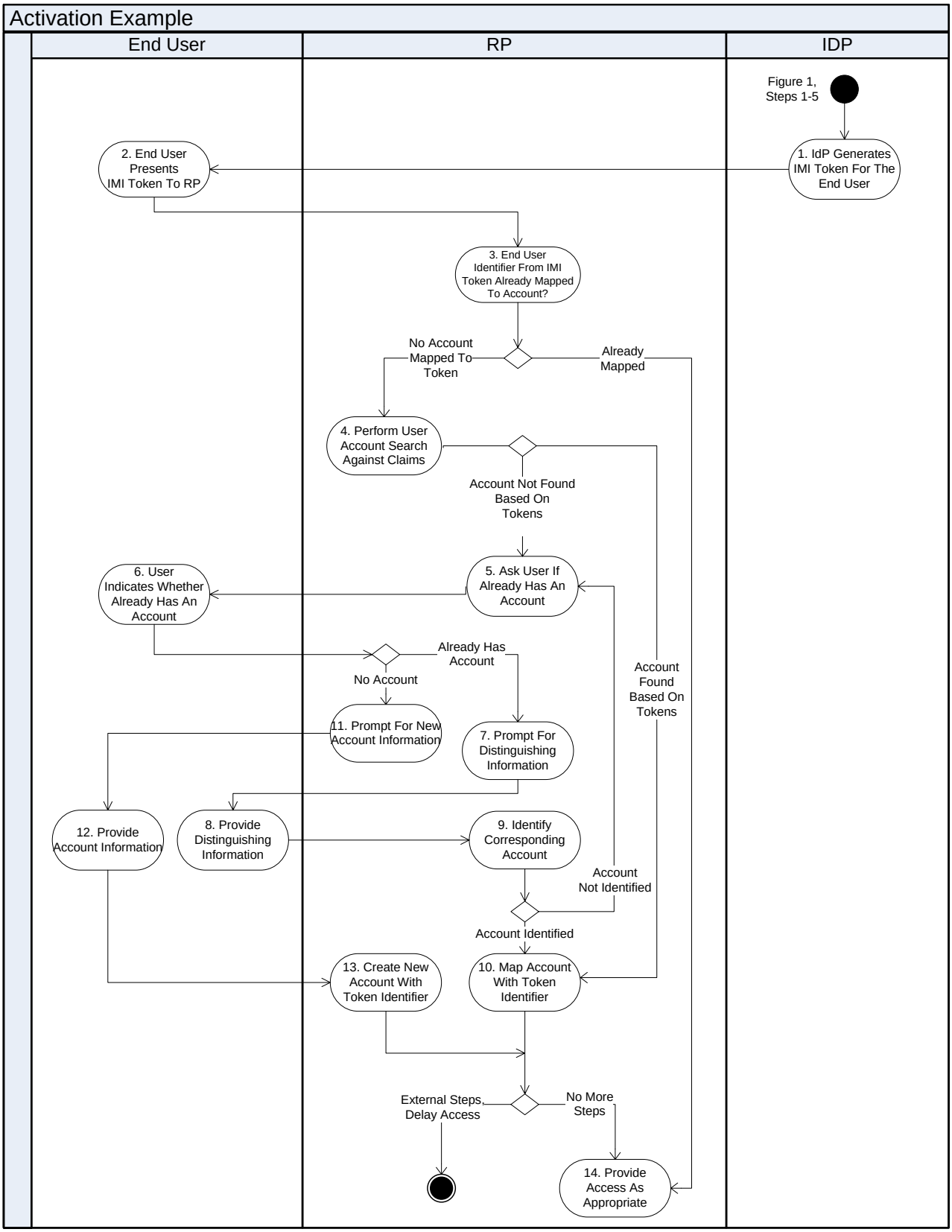
1. The Card Selector MUST send the appropriate credential (e.g. card-id) in the Request for Security Token (RST) to obtain a token. See [IMI 1.0] for additional details.
2. The Information Card `ic:SupportedTokenTypeList` field MUST include the SAML 1.1 assertion token type.
    a. Additional token types MAY be supported.
3. The Information Card MUST include the following Attributes:
    a. `ic07:RequireStrongRecipientIdentity` Attribute. This guarantees the RP has an X.509 certificate. If the RP doesn't have an X.509 certificate, the Card Selector won't present a given Information Card when this Attribute is set to true.
    b. `ic:RequireAppliesTo` Attribute. This forces the Card Selector to include the RP's X.509 certificate in the RST. This certificate is used by the IdP to encrypt the SAML 1.1 assertion token and to populate the `saml:AudienceRestrictionCondition` field in the SAML 1.1 assertion token (see Section 3.5 of this document).
    c. `ic:PrivacyNotice` Attribute. This provides the location of the IdP's privacy statement.
4. The Information Card MUST include at least one of the LOA claims listed in Section 3.1.
5. The Information Card MUST include all of the LOA claims for which it qualifies (e.g., an LOA 3 Information Card MUST contain LOA 2 and LOA 1 claims).
6. It is RECOMMENDED that other claim types in the Information Card be registered with the ICF Schemas Working Group [ICF SWG].
    a. Additional claim types MAY be supported.
    b. There are no restrictions on additional claim types.[8]

[8] Presence of a claim in an Information Card does not mean it will be included in the SAML 1.1 assertion token. End users may decline to send claim values.

3.5 Identity Provider/Secure Token Service

1. This Profile requires `wsp:AppliesTo` to be present in the RST (see `ic:RequireAppliesTo` in Section 3.4). In response:
    a. The IdP MUST encrypt SAML 1.1 assertion tokens using the public key of the RP.
    b. The IdP MUST include a `saml:AudienceRestrictionCondition` element restricting the SAML 1.1 assertion token to the scope indicated by the `wsp:AppliesTo` element in the RST message.
2. The IdP MUST use its private key to digitally sign SAML 1.1 assertion tokens.
3. The IdP MUST send only those claims explicitly requested by the RP.
4. The IdP MUST include its certificate in the `X509Certificate` element of the SAML signature.

APPENDIX A – END USER ACTIVATION EXAMPLE



APPENDIX B – GLOSSARY

Term	Definition
Assertion (SAML 1.1 Assertion Token)	A statement from a Verifier to a Relying Party that contains identity information about a Subscriber. Assertions may also contain verified attributes.
Card Selector	An end user controls her Information Cards through a software interface referred to as a Card Selector.
Claim	Information about an end user (e.g., gender, age).
Display token	A display token contains a representation of the claims carried in the issued token that can be displayed in a user interface.
Information Card	A rapidly-developing, Web 2.0-friendly method for shared light authentication, Information Cards let people authenticate themselves on multiple web sites without maintaining passwords for each site.
OBJECT Tag	In HTML, the <object> tag is used to include objects such as images, audio, videos, Java applets, ActiveX, PDF, and Flash.
Personally Identifiable Information (PII)	Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
Security Assertion Markup Language (SAML)	XML-based standard for exchanging authentication and authorization data between security domains, that is, between an *identity provider* (a producer of assertions) and a *service provider* (a consumer of assertions). SAML is a product of the OASIS Security Services Technical Committee.
SOAP	Protocol specification for exchanging structured information in the implementation of Web Services in computer networks. It relies on Extensible Markup Language (XML) as its message format, and usually relies on other Application Layer protocols (most notably Remote Procedure Call (RPC) and HTTP) for message negotiation and transmission.
White List	List containing ICAM-approved IdPs, and associated metadata.
WS-Security	Communications protocol providing a means for applying security to web services.
WS-Trust	A WS-* specification and OASIS standard that provides extensions to WS-Security, specifically dealing with the issuing, renewing, and validating of security tokens, as well as with ways to establish, assess the presence of, and broker trust relationships between participants in a secure message exchange.

APPENDIX C – ACRONYMS

Acronym	Definition
CN	Common Name
CRL	Certificate Revocation List
DN	Distinguished Name
DOS	Denial of Service
EV	Extended Validation
GSA	General Services Administration
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICAM	Identity, Credential, and Access Management
ICF	Information Card Foundation
IETF	Internet Engineering Task Force
IdP	Information Card Identity Provider
IMI	Identity Metasystem Interoperability
LOA	Level of Assurance
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OGP	Office of Governmentwide Policy
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PPID	Private Personal Identifier
RFC	Request for Comment
RP	Relying Party
RST	Request for Security Token
SAML	Security Assertion Markup Language
SSL	Secure Sockets Layer
STS	Secure Token Server
TLS	Transport Layer Security
URI	Uniform Resource Identifier
WS	Web Services
XML	Extensible Markup Language

APPENDIX D – DOCUMENT REFERENCES

[ICF SWG] Information Card Foundation Schemas Working Group
https://wiki.informationcard.net/index.php/Schemas_WG

[IMI 1.0] Identity Metasystem Interoperability 1.0, Organization for the Advancement of Structured Information Standards
http://docs.oasis-open.org/imi/identity/v1.0/cs/identity-1.0-spec-cs-01.doc

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

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

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

[SOAP] SOAP version 1.2
http://www.w3.org/TR/soap/

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

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

[WSS] Web Services Security, Organization for the Advancement of Structured Information Standards
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss