ICAM

Identity, Credential,
& Access Management

Federal Identity, Credentialing, and Access Management

OpenID 2.0 Profile

Version 1.0.1
Release Candidate

November 18, 2009

Document History

Status	Release	Date	Comment	Audience
Release Candidate	1.0.0	9/3/09	Revisions per internal review	General Distribution
Release Candidate	1.0.1	11/18/09	Revised per ICAM AWG comments.	AWG

Editors

Terry McBride	Dave Silver	Matt Tebo
Chris Louden	John Bradley	

Executive Summary

OpenID 2.0 as described in this document has completed the scheme adoption process and has been adopted by Federal Identity, Credential, and Access Management (ICAM) for the purpose of Level of Assurance (LOA) 1 identity authentication (i.e., conducting low risk transactions with the Federal government). 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 does not alter the OpenID 2.0 standard, but rather specifies which areas of the standard can be used for technical interoperability of government applications, and how they will be used.

This document defines the ICAM OpenID 2.0 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. In addition, OpenID 2.0 provides end users (e.g., citizens) with a consistent context or user experience within a single Federal Government site or within multiple sites.

The OpenID 2.0 protocol facilitates exchange of OpenID messages (requests and/or responses) between endpoints. For this adopted scheme, messages pertain primarily to the exchange of an identity assertion that includes authentication and attribute information. In ICAM, the endpoints are typically the Relying Party (RP) and the Identity Provider (IdP).

OpenId 2.0 defined herein includes the following features: single sign-on, session reset, attribute exchange, pseudonymous identifiers, and authentication policy. In addition, this Profile defines two main OpenID 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 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.

The Profile concludes with detailed technical guidance that scopes OpenID 2.0 for ICAM purposes. Like most specifications, OpenID 2.0 provides options. Where necessary, ICAM specify or removes options in order to achieve better security, privacy, or interoperability.

Table of Contents

Figures

Tables

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]. The adoption process includes assessment of the scheme for compliance with [NIST SP 800-63] and other privacy and security requirements.

OpenID 2.0 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 identity authentication (i.e., conducting low risk transactions with the Federal government). 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 does not alter the OpenID 2.0 standard, but rather specifies which areas of the standard can be used for technical interoperability of government applications, and how they will be used. Where this Profile does not explicitly provide OpenID 2.0 guidance, one must implement in accordance with OpenID 2.0 requirements as documented by the OpenID Foundation.

1.2 Objective and Audience

The objective of this document is to define the ICAM OpenID 2.0 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 OpenID 2.0 adopted scheme and its features;

2. General requirements for Identity Providers (IdPs) and Relying Parties (RPs) that extend outside the reach of OpenID 2.0 specifications (e.g., privacy, security, activation, governance).
3. An ICAM deployment profile of the OpenID 2.0 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 OpenID 2.0 adopted scheme (i.e., send or receive OpenID 2.0 messages within ICAM). It is assumed that the reader of this section is familiar with the OpenID 2.0 specification [OpenID 2.0].

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 OpenID 2.0 Overview

The OpenID 2.0 protocol facilitates exchange of OpenID messages (requests and/or responses) between endpoints. For this adopted scheme, 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).

OpenID 2.0 authentication provides a way to prove that an end user controls an Identifier. It does this without the RP needing access to end user credentials such as a password or to other sensitive information such as an email address. Implementation-wise, OpenID is a set of protocol specifications that facilitate portable identity through the most open set of specifications and technologies possible.

OpenID was started by an open source community, and as such, is not owned by any organization or standards body. Subsequently, the OpenID Foundation was formed to assist the open source model by promoting and supporting expanded adoption of OpenID as well as by providing needed infrastructure.[1]

OpenID 2.0 provides end users (e.g., citizens) with a consistent context or user experience within a single Federal Government site or within multiple sites.

OpenID 2.0 can be used to conduct low-risk transactions with the Federal Government. At this time, OpenID 2.0 is suitable for LOA 1 authentication only.

[1] See http://openid.net/what/ for more information.

The OpenID Authentication 2.0 specification is the core of the OpenID protocol. The OpenID Authentication 2.0 specification outlines the communication flow, identifiers, security, and other features that allow systems to leverage the end user's portable identity in order to authenticate an end user to an RP via an assertion from the IdP. In addition to OpenID Authentication 2.0, there are two other specifications that support RP/IdP interoperability.

- **Provider Authentication Policy Extension (PAPE) 1.0** – used to communicate the policies required to perform authentication. For example, this Profile defines a PAPE 1.0 policy requiring adherence to the ICAM OpenID 2.0 Profile.
- **Attribute Exchange (AX) 1.0** – used to communicate end user attributes (e.g., date of birth) from the IdP to the RP.

OpenID 2.0 requires all OpenID protocol messages to be transferred over HTTP. However, this Profile extends OpenID 2.0 by additionally requiring SSL/TLS, effectively requiring HTTPS (see Sections 2.5 and 3.8). OpenID 2.0 defines two types of communication between the RP and IdP:

- **Direct Communication** – the RP makes a request directly to the IdP endpoint and the IdP responds directly to the request, or vice versa.
- **Indirect Communication** – the request is sent to the end user's browser with instructions for the browser to redirect the message, either through HTTP POST or HTTP response code (e.g., 302 redirect). The response is usually sent back to the requester the same way (i.e., indirect communication).

2.2 Use Cases

The usual portable identity model includes three main actors: the end user, the IdP, and the RP. In all 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; 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 OpenID 2.0 use cases. The use cases are differentiated by where the end user starts the OpenID transaction. All other use cases defined in this Profile (e.g., session reset) derive from those use cases. End user interaction with the IdP may be for different reasons (e.g., reviewing and permitting attribute exchange). Metadata is discussed in detail in Section 2.7.

1. **End User starts at the RP** – The RP requests an assertion from the IdP. Both Direct Communication and Indirect Communication are used. Figures 1 and 2 illustrate this use case.
2. **End User starts at the IdP** – This is considered an unsolicited transaction because the RP does not request an assertion. Both Direct Communication and Indirect Communication are used. Figures 3 and 4 illustrate this use case.

Figure 1 Starting at the RP Use Case

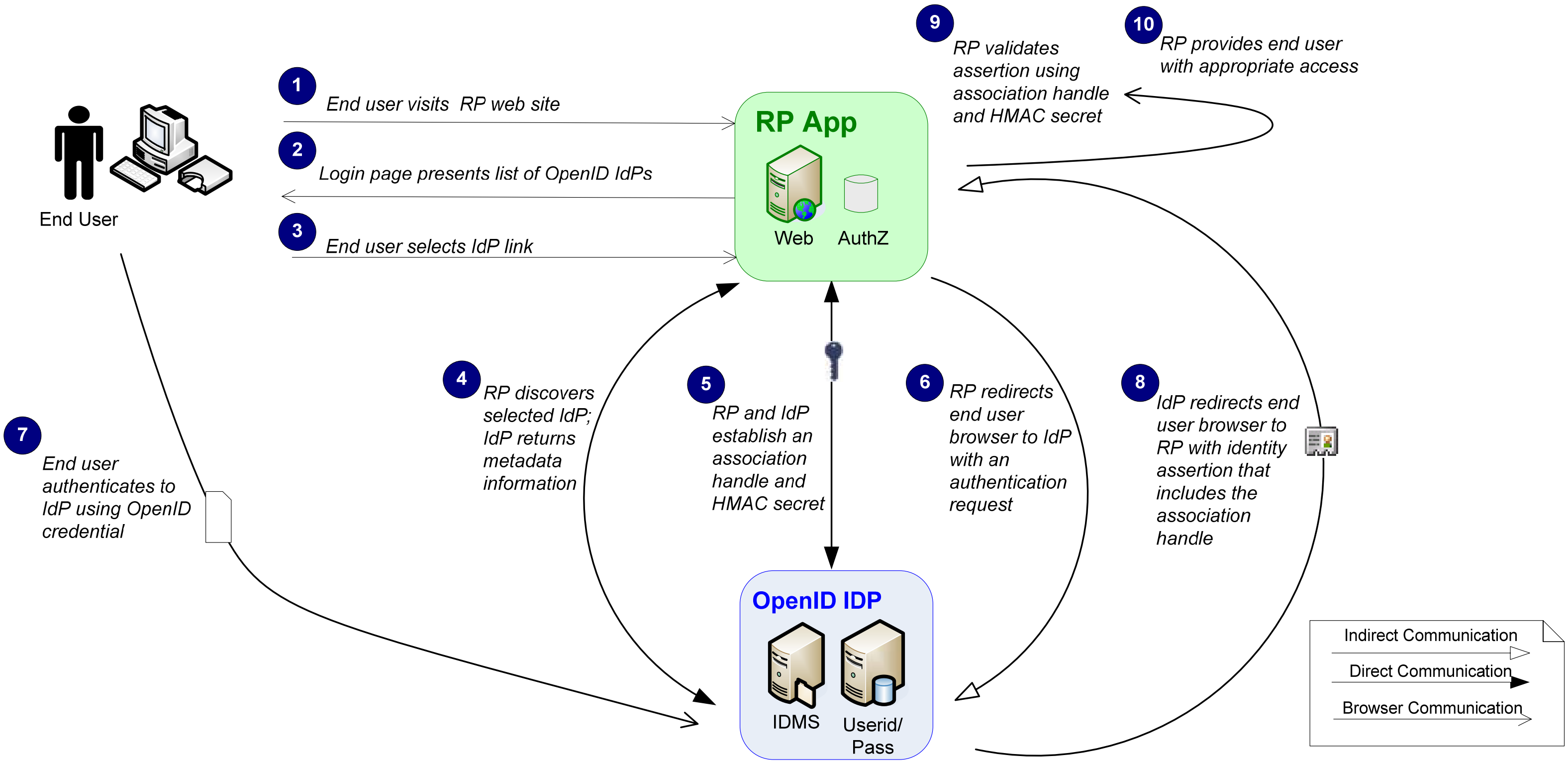

End User
1 End user visits RP web site
2 Login page presents list of OpenID IdPs
3 End user selects IdP link
RP App
Web
AuthZ
9 RP validates assertion using association handle and HMAC secret
10 RP provides end user with appropriate access
4 RP discovers selected IdP; IdP returns metadata information
5 RP and IdP establish an association handle and HMAC secret
6 RP redirects end user browser to IdP with an authentication request
7 End user authenticates to IdP using OpenID credential
8 IdP redirects end user browser to RP with identity assertion that includes the association handle
OpenID IDP
IDMS
Userid/ Pass
Indirect Communication
Direct Communication
Browser Communication

Figure 2 Starting at the RP Sequence Diagram

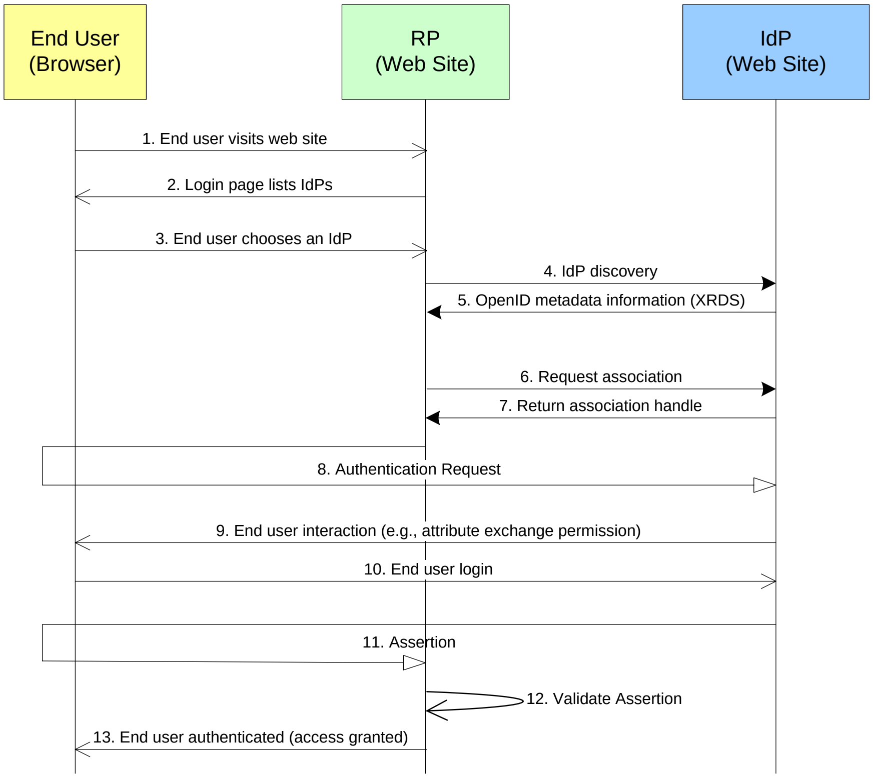

End User (Browser)
RP (Web Site)
IdP (Web Site)
1. End user visits web site
2. Login page lists IdPs
3. End user chooses an IdP
4. IdP discovery
5. OpenID metadata information (XRDS)
6. Request association
7. Return association handle
8. Authentication Request
9. End user interaction (e.g., attribute exchange permission)
10. End user login
11. Assertion
12. Validate Assertion
13. End user authenticated (access granted)

Figure 3 Starting at the IdP Use Case

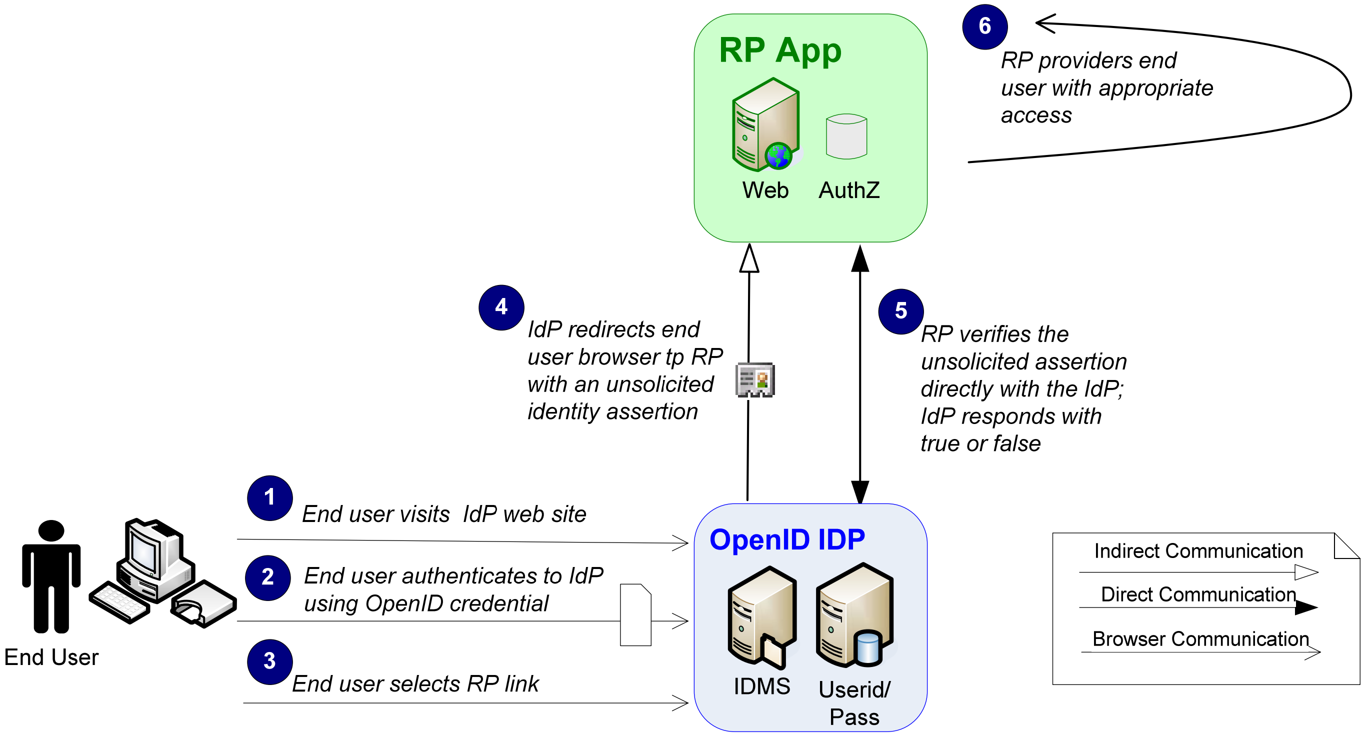
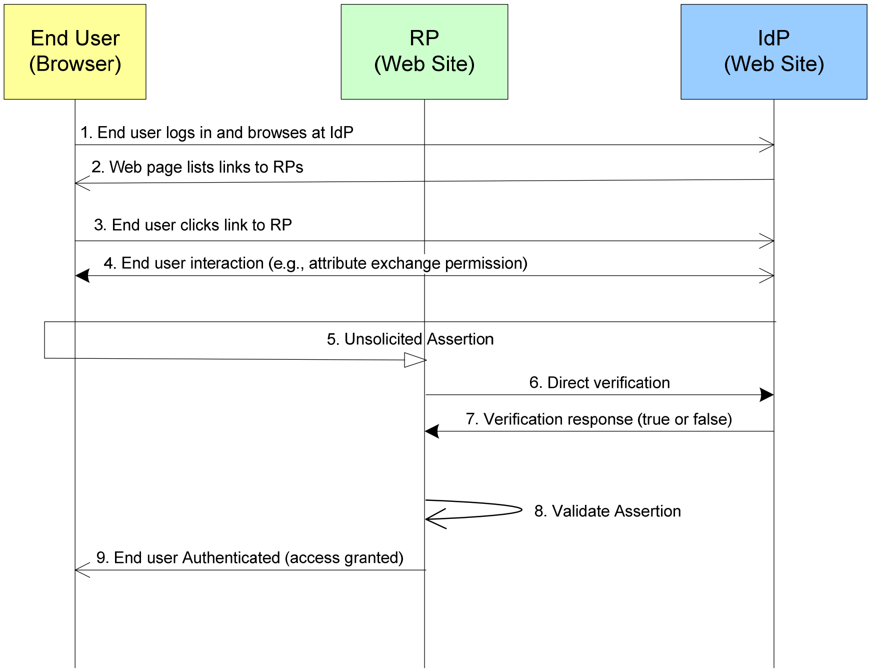

RP App
Web
AuthZ
6
RP providers end user with appropriate access
4
IdP redirects end user browser tp RP with an unsolicited identity assertion
5
RP verifies the unsolicited assertion directly with the IdP; IdP responds with true or false
1
End user visits IdP web site
2
End user authenticates to IdP using OpenID credential
3
End user selects RP link
End User
OpenID IDP
IDMS
Userid/ Pass
Indirect Communication
Direct Communication
Browser Communication

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


End User (Browser)
RP (Web Site)
IdP (Web Site)
1. End user logs in and browses at IdP
2. Web page lists links to RPs
3. End user clicks link to RP
4. End user interaction (e.g., attribute exchange permission)
5. Unsolicited Assertion
6. Direct verification
7. Verification response (true or false)
8. Validate Assertion
9. End user Authenticated (access granted)

2.3 Features

The following sections describe the features included in this Profile.

2.3.1 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 RP policy permits, the end user is not prompted to log in (re-authenticate) when another RP accessed by the end user requests an OpenID assertion. In other words, the end user is seamlessly logged into any other RP compatible with the IdP.

2.3.2 Reduced Sign-on

In some cases, SSO may not be desired by an RP (e.g., prohibited by RP policy). As a result, the end user may be asked to re-authenticate by some RPs even when SSO is in effect. This scenario is called Reduced Sign-on as SSO occurs for some, but not all RPs.

2.3.3 Session Reset

Session reset allows an RP to force end user re-authentication in order to obtain a fresh identity assertion. An example of session reset is when the end user has been idle on a screen for too long, whereupon the RP would like to time out the end user's session and have the end user re-authenticate.

Session reset is achieved by following the "Starting at the RP" use case and indicating max_auth_age=0 in the OpenID request (see Section 3.3.1). This setting tells the IdP to force the end user to re-authenticate, even if SSO is in effect.

2.3.4 Attribute Exchange

OpenID 2.0 provides an extension that allows for the exchange of end user attributes. Currently, the RP and IdP discuss in advance which attributes the IdP has available, by what names, and in what formats[2]. In addition, OpenID 2.0 has identified attributes in the AX [OpenID AX] and Simple Registration (SREG) [OpenID SREG] specifications. Table 1 lists the predefined attributes that may be exchanged via AX or SREG. Additional attributes may be exchanged as appropriate. Attribute exchange must be handled in accordance with privacy requirements (see Section 2.4).

Table 1 Attributes Predefined by OpenID 2.0

Type URI	Label	SREG Property
http://axschema.org/namePerson/friendly	Alias/Username	openid.sreg.nickname
http://axschema.org/contact/email	Email	openid.sreg.email
http://axschema.org/namePerson	Full name	openid.sreg.fullname
http://axschema.org/birthDate	Birth date	openid.sreg.dob
http://axschema.org/person/gender	Gender	openid.sreg.gender

[2] The ICAM Architecture Working Group (AWG) is currently working on an identity data dictionary that may facilitate this process.

Type URI	Label	SREG Property
http://axschema.org/contact/postalCode/home	Postal code	openid.sreg.postcode
http://axschema.org/contact/country/home	Country	openid.sreg.country
http://axschema.org/pref/language	Language	openid.sreg.language
http://axschema.org/pref/timezone	Time zone	openid.sreg.timezone

Because this Profile is for LOA 1 only, there is often no need to verify end user personal data. However, there may be situations where data provided by the end user could present harm to someone else. For example, the end user could provide someone else's email or name on a public comment. In those cases, the RP should take steps to verify or limit use of the data provided by the end user.

2.3.5 Authentication Policy

OpenID 2.0 provides an extension that allows an RP to request that IdP policies conform to OpenID 2.0 *authentication policies*. This facilitates an RP’s trust of IdPs from whom it will receive end user identity assertions. Authentication policies address identity management topics including, but not limited to identity proofing, credential token strength, privacy, and security management.

Authentication policies can be defined by standards bodies, working groups, or agreement directly between RPs and IdPs. This Profile and its governing documents are represented by one such authentication policy, which is identified by the following URL (see Section 3.3.1 for more information):

http://www.idmanagement.gov/schema/2009/05/icam/openid-trust-level1.pdf.

In addition, the RP can request that the elapsed time between the end user authenticating and the creation of the assertion not be longer than the number of seconds indicated by the RP in its request (see Section 3.3.1, *Provider Authentication Policy Extension (PAPE) Request*, for more information).

2.3.6 Pseudonymous Identifiers

Unique identifiers, especially those shared with multiple RPs, are considered personally identifiable information (PII). There are a number of considerations that Federal agencies must take into account whenever PII is collected. It is often desirable for Federal agencies to avoid receiving PII unless it is required to do business. OpenID 2.0 usually relies on a unique handle to identify an end user to all RPs. That unique handle can be considered PII. To avoid the unnecessary exchange of PII, this Profile provides a feature that requires the IdP to create a different identifier for each end user at each RP.

There are two primary components that enable pseudonymous identifiers. The first is the Private Personal Identifier (PPID), which is a pair-wise pseudonym used to uniquely identify an end user at each RP they visit. Section 3.4.2 explains this component in more detail. The other component is the requirement that RPs not request an end user’s OpenID handle. Instead, an RP presents the end user with a list from which the end user selects an IdP. Section 3.1 explains this component in more detail.

2.4 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 attributes that it does not need, or has not included in a Privacy Impact Assessment or System of Records notification;
2. As previously mentioned, this Profile uses pseudonymous identifiers to enhance end user privacy; and
3. Prior to any attribute exchange:
   a. The end user must be notified of the attributes to be exchanged; and
   b. The end user must consent to the exchange. An RP cannot require the end user to consent to attribute exchange as a condition of accessing the RP. An alternative method for obtaining and verifying attributes or of obtaining another credential must be provided.

2.5 Security

This Profile includes the following high-level security measures for OpenID 2.0 message transactions (see Section 3 for additional details):

1. The IdP and RP use SSL/TLS to positively identify one another during all direct communication.
   a. SSL/TLS processing includes encryption of OpenID 2.0 messages[3].
2. During discovery and Direct Communication, the RP verifies that the IdP is an ICAM-authorized LOA 1 IdP.
3. An RP and IdP establish a Hash Message Authentication Code (HMAC) secret and a reference to the HMAC called an Association Handle.
   a. The OpenID 2.0 assertion from the IdP contains the Association Handle. The RP uses the Association Handle to look up the HMAC secret that was established with the IdP. This removes the need for subsequent direct requests to verify the signature after each authentication request/response.
   b. Digital signature of response messages is performed by hashing the fields and values of the OpenID 2.0 response and encrypting with the HMAC secret.
   c. The IdP uses the HMAC secret to digitally sign subsequent messages, and the RP uses the HMAC secret to verify those messages[4].

Note that at LOA 1, all end user information contained in an assertion is considered self-asserted (i.e., provided by the end user without verification). RPs should not assume that information is true. RPs should make a risk-based decision whether to use the information in any capacity.

2.6 End User Activation

The first time an end user authenticates to an RP via assertion, 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[5]) with the end user's identifier from the IdP.

While the OpenID 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

[3] OpenID 2.0 messages aren't encrypted at the application level. They are only encrypted within TLS/SSL.

[4] In OpenID 2.0, only responses are signed. Requests are not signed.

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

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 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 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. By correlating the information it receives from the assertion, for example 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 A provides an example activation process.

2.6.1 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 gain them immediate access to the RP application.

Note that LOA 1 authentication provided by OpenID 2.0 should never be used to give an end user access to another RP application with a higher LOA requirement, even if the accounts are linked.

2.6.2 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 AX. 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 gain them immediate access to the RP application.

2.7 Programmed Trust

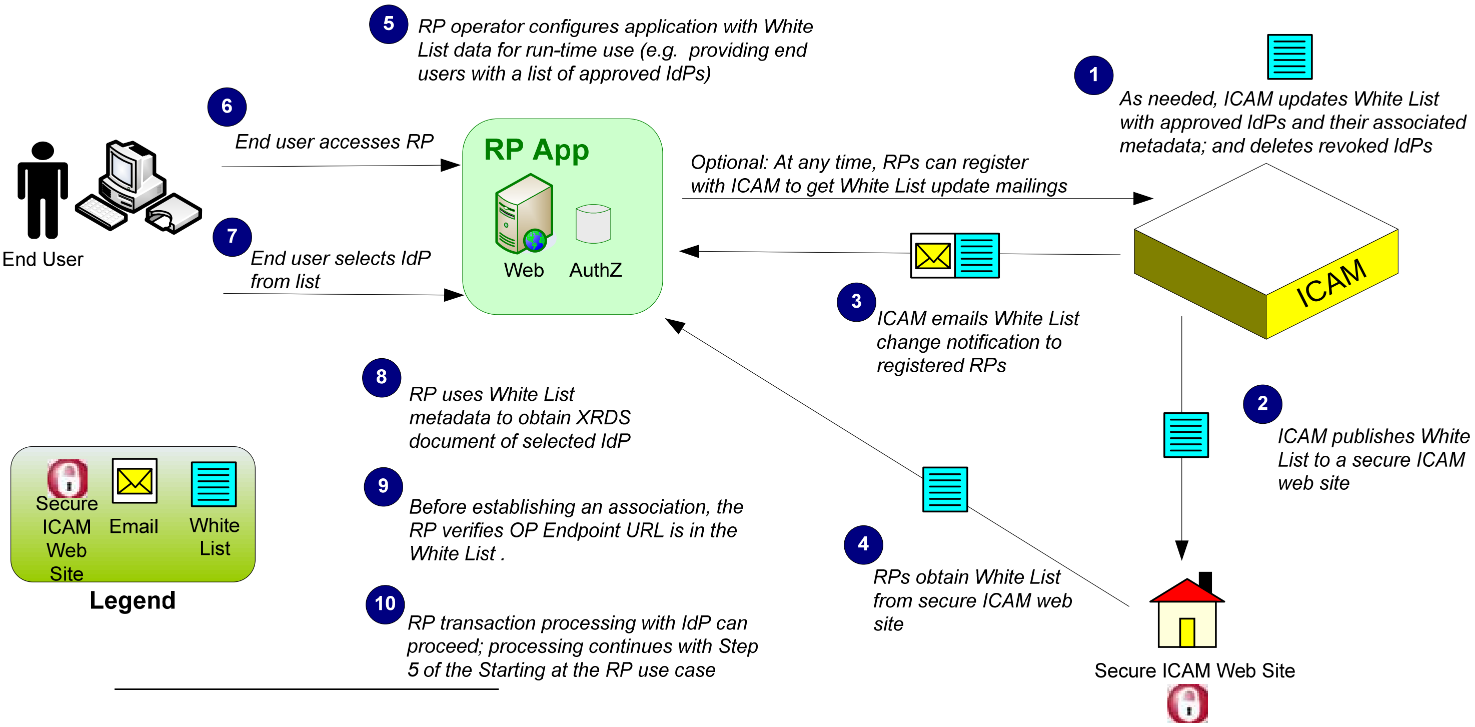
In addition to the governance outlined in [TFPAP], each ICAM adopted scheme must provide some mechanism to indicate to RPs which IdPs are approved for use within ICAM[6]. For the OpenID 2.0 adopted scheme, ICAM maintains and distributes a White List containing metadata for each approved IdP. The metadata consists of (a) display name, (b) icon URL, (c) endpoint URL, and (d) discovery URL.

The RP uses the display names and/or icons to provide the end user with a list (choice) of IdPs. The RP determines the manner in which it displays the list (e.g., display a list of links, display a page with icons, display a pull-down menu). Upon end user selection of an IdP, the RP uses the discovery URL to obtain an eXtensible Resource Descriptor Sequence (XRDS) document containing current IdP information needed to perform an OpenID 2.0 transaction (e.g., the URL to contact in order to establish an association handle with the IdP). Before establishing an association or performing direct verification with the IdP, the RP MUST also verify that the OP Endpoint URL is trusted. See [OpenID 2.0] for more information regarding the OP Endpoint URL.

The OpenID 2.0 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 5 illustrates the high-level programmed trust process flow for the end user starts at the RP use case. For the end user starts at the IdP use case, the RP must verify that the IdP's Endpoint URL is in the White List before requesting direct verification (see Section 2.2 above)

Figure 5 High-level Programmed Trust Process Flow



1 As needed, ICAM updates White List with approved IdPs and their associated metadata; and deletes revoked IdPs

2 ICAM publishes White List to a secure ICAM web site

3 ICAM emails White List change notification to registered RPs

4 RPs obtain White List from secure ICAM web site

5 RP operator configures application with White List data for run-time use (e.g. providing end users with a list of approved IdPs)

6 End user accesses RP

7 End user selects IdP from list

8 RP uses White List metadata to obtain XRDS document of selected IdP

9 Before establishing an association, the RP verifies OP Endpoint URL is in the White List .

10 RP transaction processing with IdP can proceed; processing continues with Step 5 of the Starting at the RP use case

Optional: At any time, RPs can register with ICAM to get White List update mailings

[6] 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.

3. TECHNICAL PROFILE

Like most specifications, OpenID 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 OpenID 2.0 specification.

3.1 Directed Identity

1. End users MUST select an ICAM-approved Identity Provider (IdP) from a list provided by the Relying Party (RP) (e.g., set of clickable icons, dropdown menu selection). This use case is commonly referred to as "directed identity".
    a. The RP MUST NOT allow an end user to enter an openid, as it may be considered Personally Identifiable Information (PII). Federal Agencies are required to follow strict regulations regarding collection of PII.
2. The RP MUST only discover the OpenID Provider (OP) Identifier Element for initial discovery (See [OpenID 2.0] Section 7.3.2.1.1). Subsequent discovery to verify the Positive Assertion MUST use the Claimed Identifier Element (See [OpenID 2.0] Section 7.3.2.1.2).

3.2 Association Handles

1. The RP MUST form an association with the IdP and include the association handle in the authentication request.
2. The RP SHOULD request an association type of HMAC-SHA256 (See [OpenID 2.0] Sections 6.2 and 8.3).
3. The IdP SHALL set the `expires_in` value for an association to no greater than 86400 seconds.
4. The IdP SHALL NOT reuse the HMAC secret across association handles.

a. The IdP SHOULD use some pseudo random function to generate HMAC keys.

5. To avoid association poisoning, the RP MUST separate association handles by IdP.
    a. Because the association handle can be easily learned by an attacker, the RP SHOULD use the association handle and the OP Endpoint Uniform Resource Locator (URL) (See [OpenID 2.0] Section 2) as a key to lookup HMAC secrets.

3.3 Requesting Authentication

1. The RP MUST supply a unique and consistent `realm` in the authentication request.
    a. The `realm` in the OpenID request MUST begin with https://
    b. Because the IdP uses `realm` to track pseudonyms, if an RP changes its `realm`, then all pseudonymous identifiers will be changed (See Section 3.4.2 of this document).
2. If the length of the corresponding HTTP GET URL is longer than 2,048 characters, the RP MUST use the OpenID POST binding to send the request.[7]
3. The RP SHOULD send `openid.mode.checkid_setup` to indicate that the IdP MAY interact with the end user.

[7] Some Internet browsers truncate URLs that are greater than 2,048 characters in length.

3.3.1 Provider Authentication Policy Extension (PAPE) Request

1. The RP MUST use OpenID PAPE 1.0 to ensure that the following authentication policies be met by the IdP:
    a. `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier`
        i) When this URL is present in the PAPE request, the IdP MUST generate a pseudonymous identifier for the end user that is persistent and unique across the requesting `realm`.
        ii) The pseudonym SHALL be used as the `openid.claimed_id` and `openid.identity` (see Section 3.4.2 of this document) for the end user at the `realm` for all OpenID transactions.
        iii) The IdP MUST NOT specify an `openid.identity` different from the `openid.claimed_id`, with the exception of a fragment[8] that may be appended to the `openid.claimed_id`.
    b. `http://www.idmanagement.gov/schema/2009/05/icam/openid-trust-level1.pdf`
        i) When this URL is present in the PAPE request, the IdP MUST only respond with a positive assertion if the IdP is an ICAM-authorized LOA 1 IdP.
        ii) An IdP response indicates that the end user meets LOA 1 requirements and that the IdP is following this Profile.
2. The RP MAY use the OpenID PAPE 1.0 extension to indicate that the IdP MUST NOT include any PII in the response:
    a. `http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf`
        i) When this URL is present in the authentication request, the IdP MUST NOT include end user PII (e.g., OpenID, AX information [OpenID AX], or Simple Registration (SREG) information [OpenID SREG]) in the assertion.
3. The RP MAY indicate in the `openid.pape.max_auth_age` field of the request the maximum number of seconds that can elapse between the end user performing interactive login at the IdP, and the IdP receiving the `checkid_setup`.
    a. If the elapsed time is greater than the value of `max_auth_age`, then the IdP MUST force the end user to re-authenticate before an assertion can be sent.
    b. If the RP wants the IdP to unconditionally re-authenticate the end user, the RP SHOULD send a `max_auth_age` value of 0 in the request. There may be a delay before the end user returns to the RP. Therefore, the RP SHOULD make a risk-based determination of the appropriate `auth_time` that it will accept in the response.
    c. If the IdP requires end user authentication to the IdP prior to accepting any RP requests to avoid phishing, the IdP MAY treat a requested `max_auth_age` of 0 as if it were 1,800 seconds.
        i) The IdP MUST still return the actual value of `auth_time` based on the last interactive login.

[8] A URI fragment follows the "#" at the end of a URI (e.g., http://host.gov/path#fragment). It is an optional part of a URI.

The following is a sample PAPE 1.0 request:

```
openid.pape.max_auth_age=0
openid.pape.preferred_auth_policies=
      http://www.idmanagement.gov/schema/2009/05/icam/no-pii.pdf
      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privat
      epersonalidentifier
      http://www.idmanagement.gov/schema/2009/05/icam/openid-
      trust-level1.pdf
```

3.4 Positive Assertion Formulation

1. If the length of the corresponding HTTP GET URL is longer than 2,048 characters, the IdP SHOULD use the OpenID POST binding to send the request.

3.4.1 PAPE Response

1. A positive assertion MUST contain a PAPE 1.0 response that addresses the requested PAPE 1.0 authentication policies (see Section 3.3.1 of this document).

The following is a sample PAPE 1.0 response:

```
openid.pape.auth_policies=
      http://www.idmanagement.gov/documents/TrustFrameworkProvider
      AdoptionProcess.pdf
      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privat
      epersonalidentifier
      http://www.idmanagement.gov/schema/2009/05/icam/openid-
      trust-level1.pdf
```

3.4.2 Private Personal Identifiers

1. The IdP MUST establish a unique and persistent pseudonymous end user identifier for each user-RP pair. This Private Personal Identifier (PPID) SHALL be expressed in both the `openid.identity` and `openid.claimed_identity` fields within positive assertions about the end user.
   a. The pseudonym is used to identify the end user to the RP in a way that protects the end user's privacy by preventing propagation of the end user's common identifier throughout the Federal Government.
   b. All pseudonyms MUST be globally unique.
      i) The IdP MUST NOT use the same pseudonym for an end user at multiple RP `realms`.
      ii) To ensure global uniqueness the IdP SHOULD include an IdP specific base within the PPID.
2. The IdP MUST protect pseudonyms from disclosure outside of the user-RP pair.
3. The IdP MUST construct a pseudonym in a way that ensures that it cannot be reverse engineered to help identify an end user across multiple `realms`.
4. For purposes of computing the PPID, the IdP MAY normalize the `realm` by using the fully qualified domain name excluding the pre-pended www domain segment, if included.

3.4.3 Simple Registration and Attribute Exchange

1. The assertion MUST NOT include any end user PII (i.e., AX and SREG) unless the RP specifically requests the attribute(s) and the request does not include an authentication policy precluding the exchange of PII.
2. The IdP MUST display a list of attributes to be sent to the RP, and receive positive confirmation from the end user that it is permissible to send the listed attributes.
    a. The IdP MAY implement a mechanism for the end user to opt in to always sending the listed attributes to the specific RP for subsequent transactions.

3.5 Positive Assertion Verification

1. The RP MUST verify that all of the following fields (without the "openid." prefix prepended) are included in the IdP signature: `op_endpoint, return_to, response_nonce, assoc_handle, claimed_id, and identity`.
2. The IdP MUST sign all OpenID extension fields.
3. The RP MUST verify the signature of all OpenID PAPE and AX extension fields.
4. The RP MUST check the `openid.response_nonce` to make sure that an assertion from the IdP with this nonce has not already been used.
5. It is RECOMMENDED that the RP set a restriction on the amount of elapsed time from the timestamp in the nonce until receipt.
6. The RP MUST check the `return_to` value in the assertion to verify that the assertion was produced for the RP.
7. The RP MAY use "Direct Verification" to validate the assertion (See [OpenID 2.0] Sections 10 and 11.4.2) when:
    a. The IdP includes an `openid.invalidate_handle` indicating that the association has expired.
    b. The IdP sends an unsolicited assertion (see Section 3.6 of this document).

3.6 Unsolicited Positive Assertions

1. The RP MAY accept an unsolicited positive assertion provided the following:
    a. The assertion is formulated in accordance with Section 2.4 of this document.
    b. In addition to validating the assertion properly, the RP can confirm that the IdP sending the unsolicited response is an ICAM-authorized LOA 1 IdP.
2. The RP MUST reject an unsolicited assertion that does not contain the following PAPE 1.0 authentication policies (see Section 3.3.1 of this document for a description of these policies):
    a. `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier`
    b. `http://www.idmanagement.gov/schema/2009/05/icam/openid-trust-level1.pdf`
3. The RP MUST reject an unsolicited assertion if it contains PII that it would not otherwise request or is not authorized to accept.

3.7 Relying Party Discovery

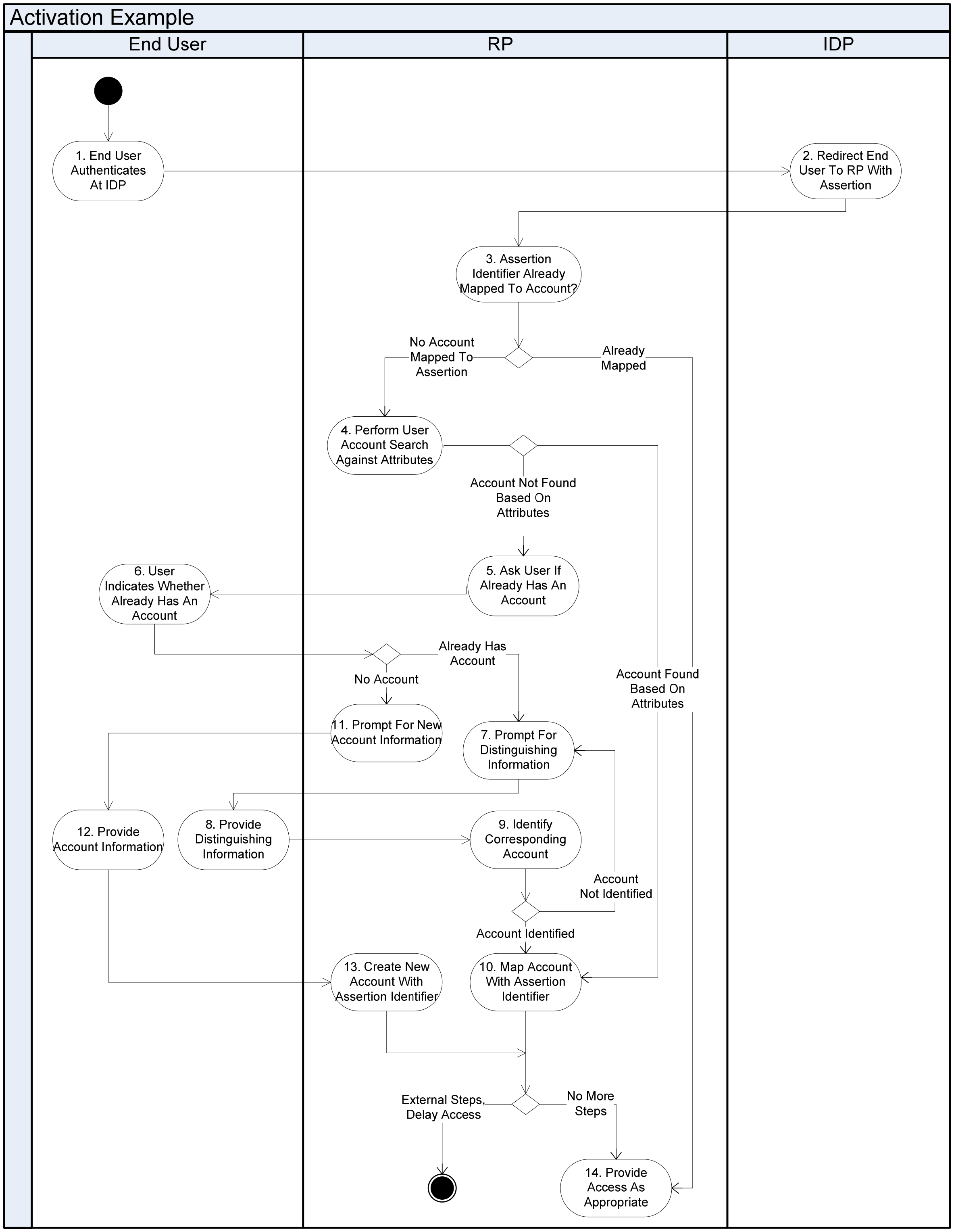
1. The RP MUST publish an eXtensible Resource Descriptor Sequence (XRDS) discovery document for its `realm` per [OpenID 2.0] Section 13.
    a. The XRDS MUST be published at the URL matching the `realm`.
2. The Uniform Resource Identifier (URI) for the XRDS document discovered via Yadis MUST have an https: scheme.
3. The IdP MUST perform RP discovery and `return_to` validation per [OpenID 2.0] Section 9.2.1.
    a. If `return_to` validation fails, the IdP MUST present a stern warning to the end user stating there is a potential attempt to compromise their session and personal information.
    b. In addition, the IdP MAY present an error message and discontinue the OpenID authentication process.

3.8 Security Considerations

1. TLS/SSLv3 MUST be used at all endpoints, discovery redirects, and the URI of the XRDS document.
2. During the SSL/TSL handshake, the RP SHOULD negotiate a cipher suite that includes either Triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES).
    a. NIST encourages use of the faster and stronger AES algorithm[9].
3. During discovery and Direct Communication, the RP MUST verify that the IdP is an ICAM-authorized LOA 1 IdP through verification of URL endpoints and server certificates (see Section 2.7).
4. During Direct Communication, the RP MUST check the revocation status of the IdP server certificate.
5. The RP and IdP SHOULD employ frame busting techniques throughout to avoid possible eavesdropping by a third-party web site.
6. The RP MUST reject any assertion where `openid.ns` is other than http://specs.openid.net/auth/2.0.

[9] Federal Register / Vol. 69, No. 142 / Monday, July 26, 2004 / Notice

APPENDIX A – 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 Identifier Already Mapped To Account?
No Account Mapped To Assertion
Already Mapped
4. Perform User Account Search Against Attributes
Account Not 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
Account Found Based On Attributes
11. Prompt For New Account Information
7. Prompt For Distinguishing Information
12. Provide Account Information
8. Provide Distinguishing Information
9. Identify Corresponding Account
Account Not Identified
Account 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 B – 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.
Assert	To make a statement about the properties of a user or user's act of authentication.
Association	As part of the OpenID protocol, a relying party establishes shared secrets (called ‘associations’) with identity providers that are used to verify identity assertions.
Association Poisoning	Each Association is assigned a handle, which is a name by which the RP and the IdP will refer to the shared secret in later transactions. If the RP does not account for the fact that the two identical handles can come from different IdPs, then an attacker may masquerade as an IdP, use an identical handle, and hijack the shared secret, thereby gaining the ability to assert the identity of any end user from the other IdP.
Cipher Suite	A set of algorithms for performing encryption and decryption. There are many different algorithms. Some provide the highest levels of security, but require a large amount of computation for encryption and decryption; others are less secure, but provide rapid encryption and decryption. The length of the key used for encryption affects the level of security - the longer the key, the more secure the data. Accordingly, security protocols such as SSL and TLS allow end users to select from cipher suite the algorithm that suits their needs, and to enable communication with others who may have different needs.
Direct Communication	Direct communication is initiated by a Relying Party to an IdP's OP endpoint URL. It is used for establishing associations and verifying authentication assertions.
Directed Identity	Information provided to the RP by the end user that does not expose the end user’s OpenID.
Fragment	A URI fragment follows the “#” at the end of a URI (e.g., http://host.gov/path#fragment). It is an optional part of a URI.
Frame Busting Techniques	A piece of code, usually JavaScript, that doesn't allow a web page to be displayed within a frame. Frame Busting Techniques are used to prevent an external web site from loading pages within a disguised frameset without permission.
Identifier	For the OpenID purposes, an Identifier is either a "http" or "https" URI, (also referred to as a "URL"), or an XRI. Identifiers are used when something needs to be uniquely distinguishable. Examples of identifiers are used include endpoints, authentication policies, and AX attribute types.

Term	Definition
Metadata	Information shared between endpoints (e.g., Relying Party, Identity Provider) necessary for technical interoperation. Metadata may be conveyed via a White List.
OpenID Provider	An IdP that provides an OpenID authentication service on which a Relying Party relies for an assertion.
Persistent	Ability to maintain data.
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.
Positive Assertion	In general, an Positive Assertion is a successful authentication assertion regarding an end user. See [OpenID 2.0] Section 10.1 for an exact technical definition.
Provider Authentication Policy Extension (PAPE)	Extension to the OpenID Authentication protocol that provides a means for a Relying Party to request previously agreed upon authentication policies be applied by the OpenID Provider and for an OpenID Provider to inform a Relying Party what authentication policies were used. Thus a Relying Party can request the End User authenticate, for example, by means which are resistant to common phishing attacks or that provide for multi-factor authentication. Likewise, the OpenID Provider is able to convey to the Relying Party that the End User either met or did not meet the requirements of the requested policy, or policies, in the OpenID Authentication response message as well as the general strength of the credential(s) being used.
Pseudonym	Private OpenID pseudonym that will only be used with one site. With an OpenID pseudonym, 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."
White List	A White List specifies Identity Providers (IdPs) that Relying Parties (RPs) can trust during the authentication process. The White List may include metadata necessary for technical interoperation.
Yadis	Communications protocol for discovery of services such as OpenID, OAuth, and XDI connected to a Yadis ID.

APPENDIX C - ACRONYMS

Acronym	Definition
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AX	Attribute Exchange
EGCA	E-Governance Certification Authorities
GSA	General Services Administration
HMAC	Hash Message Authentication Code
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICAM	Identity, Credential, and Access Management
IdP	OpenID Provider
IETF	Internet Engineering Task Force
LOA	Level of Assurance
NIST	National Institute of Standards and Technology
OGP	Office of Governmentwide Policy
OMB	Office of Management and Budget
PAPE	Provider Authentication Policy Extension
PII	Personally Identifiable Information
PPID	Private Personal Identifier
RFC	Request for Comment
RP	Relying Party
SHA	Secure Hash Algorithm
SREG	Simple Registration
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XRDS	eXtensible Resource Descriptor Sequence
XRI	Extensible Resource Identifier

APPENDIX D - DOCUMENT REFERENCES

[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

[OpenID 2.0] OpenID Authentication 2.0
http://openid.net/specs/openid-authentication-2_0.html#discovery

[OpenID AX] OpenID Attribute Exchange 1.0
http://openid.net/specs/openid-attribute-exchange-1_0.html

[OpenID SREG] OpenID Simple Registration
http://openid.net/specs/openid-simple-registration-extension-1_0.html

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

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

[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