E-Authentication Federation
Adopted Schemes

Version 1.0.0
Final
May 4, 2007

Document History

Status	Release	Date	Comment	Audience
Template	0.0.0	1/18/06	Outline	PMO
Draft	0.0.1	1/19/07	Initial draft	Internal
Draft	0.0.2	2/14/07	Updates per internal review	Internal
Draft	0.0.3	2/16/07	Updates per internal review	Internal
Draft	0.0.4	2/20/07	Updates per internal review	Red Team
Draft	1.0.0 RC1	3/2/07	For Approval	PMO
Draft	1.0.0 RC2	3/30/07	Updates per public comment	PMO
Draft	1.0.0 RC3	4/20/07	Updates per public comment	Internal
Final	1.0.0	5/4/07	Updates per PMO comment	Public

Editors

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

Document Introduction

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

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

By integrating with the ASC, an application owner uses a standard approach for federated authentication, rather than building or maintaining an authentication structure. The SAML schemes described in this document support assertion-based authentication. An alternative scheme, PKI, supports certificate-based authentication directly to the RP.

The primary audience for this document is non-technical personnel responsible for a Federation member system based on any of the adopted schemes described herein. This includes, but is not limited to senior managers, program managers, project managers, contracting officers, and operations staff. In addition, technical staff and implementers of Federation member systems using any of the adopted schemes described herein are encouraged to read this document as they may benefit from doing so.

This document is part of the ASC technical suite, which also includes the *Technical Approach for the Authentication Service Component* and *E-Authentication Federation Architecture 2.0 Interface Specifications*. For complete comprehension, please read this document after the Technical Approach and prior to applicable Interface Specifications.

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

Figure 1-1 E-Authentication Document Hierarchy

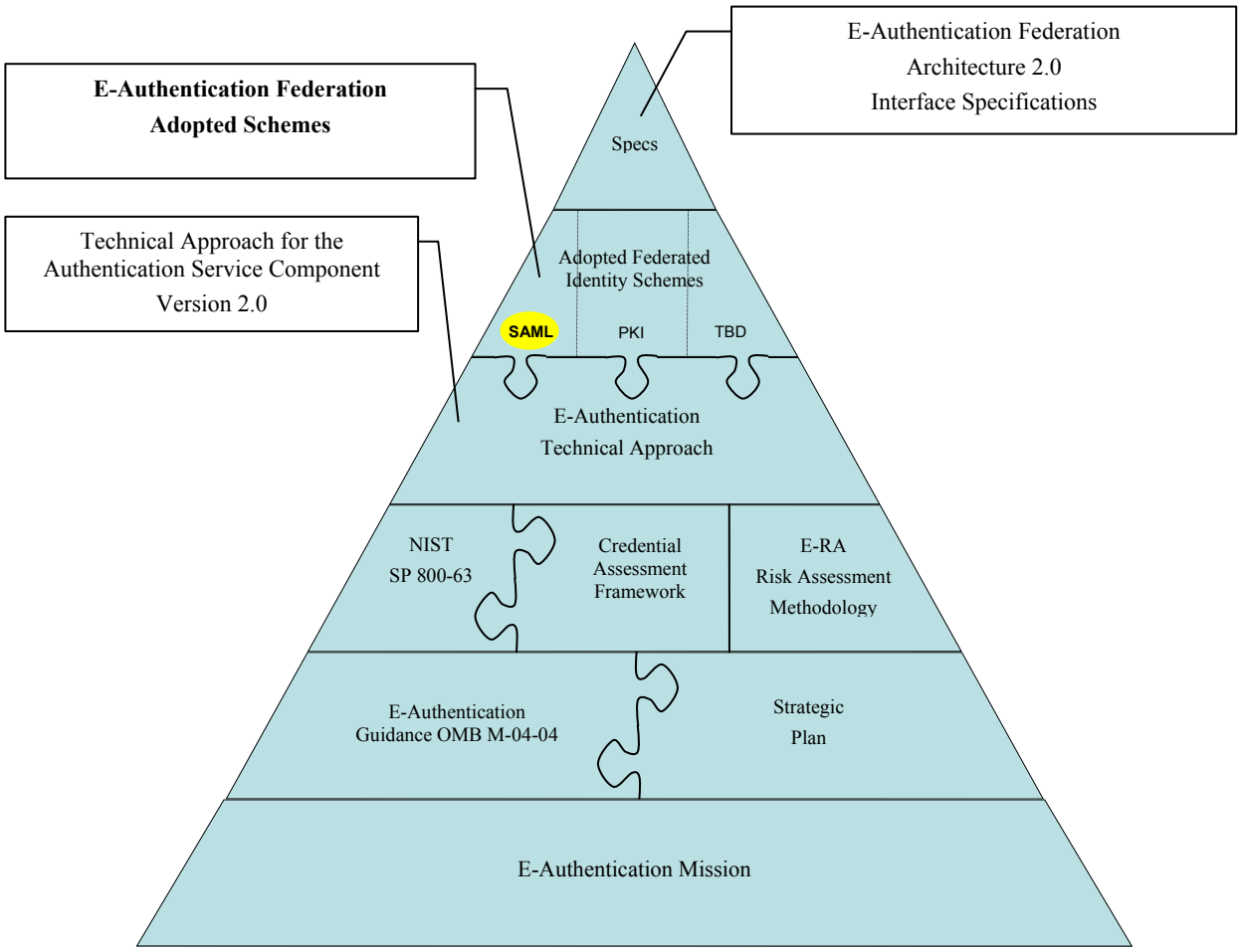


Table of Contents

Figures

1. ADOPTED SCHEME: SAML 2.0 SSO PROFILE USING HTTP POST

1.1 Introduction

Security Assertion Markup Language (SAML) 2.0 Single Sign-on (SSO) Profile Using Hypertext Transfer Protocol (HTTP) POST is one of the schemes adopted by the E-Authentication Program Management Office (PMO) and supported by the ASC. The SAML protocol facilitates exchange of end SAML messages (requests and/or responses) between endpoints. For this adopted scheme, the messages pertain to end users for reasons such as (a) delivery of an identity assertion regarding an act of authentication and attribute information[1], and (b) single logout. In the ASC, the endpoints are the RP and the credential service (CS).

This overview describes SAML 2.0 SSO Profile Using HTTP POST as an adopted scheme, and its use in the Federation. It discusses the several SAML 2.0 profiles and bindings that comprise this adopted scheme:

(1) Web SSO Profile with HTTP POST binding and HTTP Redirect binding to facilitate end user authentication;

(2) Identity Provider Discovery Profile to facilitate single sign-on; and

(3) Single Logout Profile with HTTP Redirect binding to facilitate SLO of an end user from all active Relying Party (RP) sessions

In addition, this overview discusses implementation of the following features, specifically for this adopted scheme:

(1) Governance;

(2) Use of the SAML 2.0 metadata specification, including digitally signing metadata;

(3) End user activation; and

(4) Scheme translation

This overview begins with a high-level overview of this adopted scheme. The overview continues by highlighting the adopted scheme at the transaction flow level, which includes:

(1) An end user begins at an RP;

(2) An end user begins at a CS;

(3) An end user begins at an optional external site such as USA.gov;

(4) An end user conducts transactions at other RPs using single sign-on;

(5) An end user is re-authenticated at the request of an RP (session reset),

(6) An end user initiates single logout (SLO) from all active RP sessions;

(7) An RP activates an end user; and

(8) An RP or CS deactivates an end user.

Each use case shows the flow and exchange of SAML messages. This ensures that those implementing this adopted scheme fully understand its use in E-Authentication transaction flows.

[1] See [Interface Spec] regarding required and optional attributes for this adopted scheme.

This overview concludes by discussing governance of this adopted scheme. Governance provides mechanisms for the government to assert its authority over which RPs and credential service providers (CSPs) can participate in the Federation. For this adopted scheme, the E-Governance Certification Authorities (E-GCA) issues two X.509 certificates to each Federation member – one used for digital signature and one used for encryption. Signing ensures trust, message integrity and non-repudiation. Encryption ensures confidentiality. Successfully verifying a SAML message signature indicates (a) the SAML message is from a currently approved Federation member system, and (b) there has been no tampering. Federation member systems process only successfully verified messages. The E-GCA does not participate in end user authentication. Another governance mechanism discussed is the distribution of signed metadata by the PMO. Metadata is information needed by Federation member systems to technically interoperate. This adopted scheme uses the SAML 2.0 metadata specification for industry-standard, secure exchange.

1.2 Audience and Objective

The primary objective of this overview is to provide high-level working knowledge and understanding of SAML 2.0 SSO Profile Using HTTP POST. Please refer to [Tech Approach], [Interface Spec], and the [SAML2 *] documents for additional information about SAML 2.0 SSO Profile Using HTTP POST.

1.3 Document References

[SAML2 *]	All the SAML2 document reference that immediately follow. All available at http://docs.oasis-open.org/security/saml/v2.0
[SAML2 Core]	"Assertions and Protocol for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005. Document Identifier: saml-core-2.0-os http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
[SAML2 Bindings]	"Bindings for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005. Document Identifier: saml-bindings-2.0-os http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
[SAML2 Profiles]	"Profiles for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005. Document Identifier: saml-profiles-2.0-os http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
[SAML2 Metadata]	"Metadata for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005. Document Identifier: saml-metadata-2.0-os http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf
[SAML2 Context]	"Authentication Context for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005. Document Identifier: saml-authn-context-2.0-os http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

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

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

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

[User Activation] Relying Party User Activation Within E-Authentication
http://www.cio.gov/eauthentication/TechSuite.htm

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

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

[Interface Spec] E-Authentication federation Architecture 2.0 Interface Specifications
http://www.cio.gov/eauthentication/TechSuite.htm

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

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

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

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

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

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

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

1.4 Reference Links

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

1.5 Scheme Highlights

1.5.1 SAML 2.0 Protocols, Profiles and Bindings

This adopted scheme exchanges SAML messages using the SAML Request-Response Protocol. All adopted scheme processing fully conforms to the SAML 2.0 specification [SAML2 *]. SAML messages are XML-encoded, digitally signed in whole or in part, and in some cases encrypted, as discussed later in this document. What is signed and how varies depending on the message and the binding (see [Interface Spec] for details). Figure 1-2 illustrates the Request-Response Protocol.

Figure 1-1 Request-Response Protocol

[SAML2 Core] states "In certain cases, when permitted by profiles, a SAML response MAY be generated and sent without the responder having received a corresponding request." Figure 3-2, Starting at a CS, illustrates use of that exception within this adopted scheme. Starting at a CS does not include an initial request from an RP. The end user first selects an RP while at the CS. The CS then sends the selected RP an "unsolicited" response that includes an assertion.

This adopted scheme uses several SAML profiles to achieve its purposes. SAML profiles are rules for using SAML protocol messages in a particular context of use. The profiles used are:

- **Web Browser SSO Profile** – to facilitate end user authentication
- **Identity Provider Discovery Profile** – to facilitate single sign-on
- **Single Logout Profile** – to facilitate logout of an end user from all active RP sessions; and

Each profile uses one or more SAML bindings. SAML bindings are frameworks for embedding and transporting SAML protocol messages. That is, a SAML binding is a specific means of transporting SAML protocol messages using standard transport protocols (e.g., HTTP POST). The PMO chose bindings for this adopted scheme from several available in the SAML 2.0 standard – primarily based on ease of implementation, risk management, and capabilities offered. The following sub-sections describe which SAML bindings are used for what specific purposes.

1.5.1.1 HTTP POST Binding

This adopted scheme uses the SAML HTTP POST binding as the communication mechanism for a CS 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:

- Simple to implement (e.g. no firewall reconfigurations required, no mutual TLS);
- More scalable because HTTP POST is stateless (i.e., Having no information about what occurred previously) and requires fewer hardware resources; and
- Faster and less expensive to deploy than SAML Artifact based binding

1.5.1.2 HTTP Redirect Binding

This adopted scheme uses the SAML HTTP Redirect binding as the communication mechanism for passing a SAML authentication request from an RP to a CS. This is the minimum required by [SAML2 Conform]. In addition, this adopted scheme uses the SAML HTTP Redirect binding as a communication mechanism for SAML SLO request-response message exchange.

1.6 Security and Confidentiality

Within this adopted scheme, in accordance with [SAML2 Security], ASC entities (a) digitally sign, in whole or in part, all SAML messages exchanged, and (b) encrypt the entire SAML assertion contained within a SAML response message. For purposes of this adopted scheme:

- Trust of a certificate (signing public key certificate, encryption public key certificate) is determined at metadata consumption time (i.e., when metadata is configured into the Federation member system);
- At run time, the recipient uses mechanisms such as CRL or OCSP to determine whether the applicable public key certificate is currently valid (i.e., not revoked);
- Digitally signing allows the recipient to authenticate the sender as a trusted party. The recipient does not further process the received message until such positive verification.
- Digitally signing allows the 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.
- Digitally signing ensures non-repudiation (i.e., the sender cannot later deny that they sent the message).
- 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).

1.7 Activation

Activation is the process of an RP uniquely identifying an end user. That is, the RP distinguishes the end user from all other end users – most importantly, from others with the same name. The RP activates an end user when the end user's subject name (in the SAML assertion or in the PKI certificate) is unrecognized. This is because in a federated environment, each CS and CA has a different subject name for the same end user, to guarantee Federation-wide uniqueness.

The RP determines the need for activation, and facilitates it when necessary. Every time an end user arrives at the RP with a SAML assertion, the RP checks whether it has a corresponding end user record in its local data store. The RP does this by mapping the unique subject name in the SAML assertion to equivalent information in its local data store of end user records. Subject name information in a SAML assertion consists of (a) end user name identifier, and (b) a name qualifier that guarantees uniqueness of the end user name.

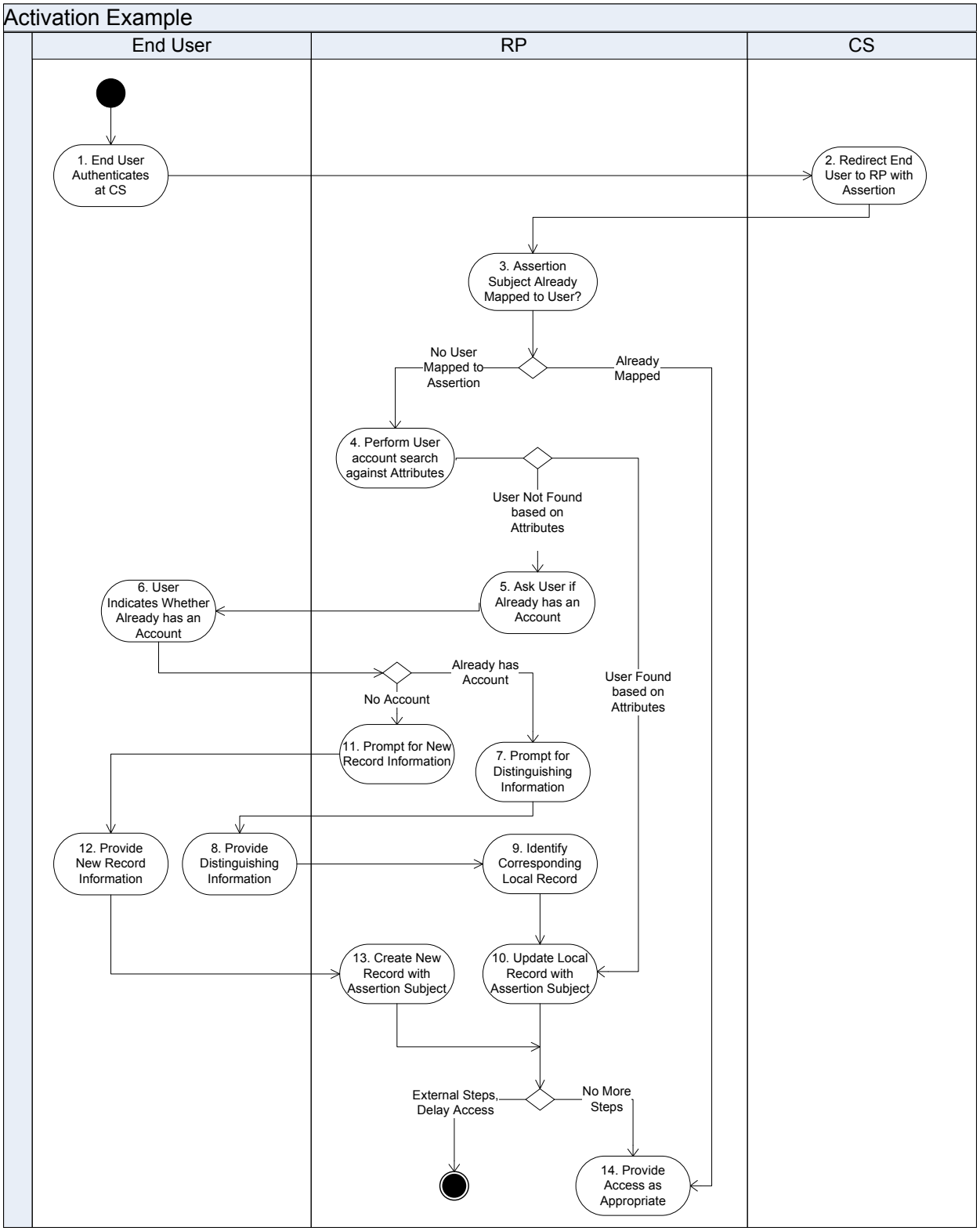
If the RP finds a match, activation is not necessary – the RP knows the end user, uniquely and with certainty. Processing continues as normal.

If the RP does not find a definitive match or any match at all using subject name, activation is required. First, the RP tries to map definitively using other SAML assertion attributes. If attribute mapping is successful, the RP updates its end user record with SAML assertion subject name information, and processing continues as necessary. If attribute mapping is not successful, the RP initiates an end user registration process.

The registration process should not require identity proofing, userid and password selection, or any other credential management – the CS does those things on behalf of the RP, in accordance with [OMB M-04-04] and [NIST SP 800-63]. Registration prompts the end user as to whether the end user already has an account at the RP. If yes, registration asks additional questions that assist with identifying the RP's end user record. The RP then updates its end user record with the subject name information from the SAML assertion. If the end user does not already have an account, registration asks the end user all questions necessary to complete a new record. The RP then creates a new record, adding the subject name information from the SAML assertion.

The RP does not have to allow access to its services immediately after activation. For example, the RP may delay end user access if additional steps are required (e.g., out-of-band review and approval of some data entered by the end user). Figure 1-3 describes the activation business process. See [User Activation] for more complete details.

Figure 1-2 Sample Activation Business Process



1.8 Single Logout

SLO is near-simultaneous logout of a collection of related sessions on request. In ASC terms, it is the logout of an end user from a specific authentication session and all active RP sessions associated with authentication session. Therefore, SLO occurs within the context of single sign-on. The end user initiates SLO by selecting a link displayed by an RP or CS.

If the end user selects SLO at an RP:

- That RP immediately logs out the end user, and redirects the end user with a SAML LogoutRequest to the CS responsible for the authentication session.
- The request causes the CS to log out all other RP sessions relying on this same authentication session. The CS does this by iterating through its list of RPs relying on this authentication session, and redirecting the end user with a SAML LogoutRequest to each.
- After logging out the end user at the request of the CS, the RP redirects the end user with a LogoutResponse back to the CS.
- Upon completion of all logouts, the CS redirects the end user with a LogoutResponse to the initiating RP. This indicates that the CS has completed its iteration processing.

If the end user selects SLO at a CS, only the CS iteration processing occurs, as described above.

Messages displayed by Federation member systems during SLO are in accordance with [FMD] to the extent defined there, otherwise implementation-specific. SLO messages may include indication that SLO processing will occur, and that SLO processing has completed. Except for status messages, SLO is transparent to the end user. Upon completion of SLO, the end user can proceed as desired (e.g., go to another web site).

1.8.1.1 Simple Logout

The alternative to SLO is simple logout, whose log out scope is limited to the current RP (i.e., the RP to which the end user's browser is currently connected). By selecting simple logout instead of SLO, the end user logs out from the current RP only. The RP does not communicate with the authenticating CS. Any other RP sessions the end user has remain active, unless any have expired in the interim. The end user proceeds as desired.

1.9 Federation Features

1.9.1 RP/CS Discovery Mechanisms

Discovery is the process of an end user finding a CS and/or RP. The following sections highlight the various discovery mechanisms in this adopted scheme.

1.9.1.1 Web Browser Bookmarks

End users can bookmark their preferred RPs and CSs within their web browser. In doing so, the end user builds a re-usable discovery mechanism customized with their preferred Federation web sites. Once redirected to the selected Federation web site, the appropriate adopted scheme use case begins. Although this discovery approach is external to the adopted scheme, this document presents it for completeness and informational purposes.

1.9.1.2 Links Presented by Federation Member System

As circumstances warrant, the CS or RP presents the end user with a list of compatible systems. The CS displays a list of compatible RPs. In addition, the CS may present the end user with a sub list of resources

(i.e., applications) per RP. The RP displays a list of compatible CSs. Upon end user selection from a list, applicable processing occurs. Figures 1-4 and 1-5 illustrate this feature.

Figure 1-3 CS Presents Links

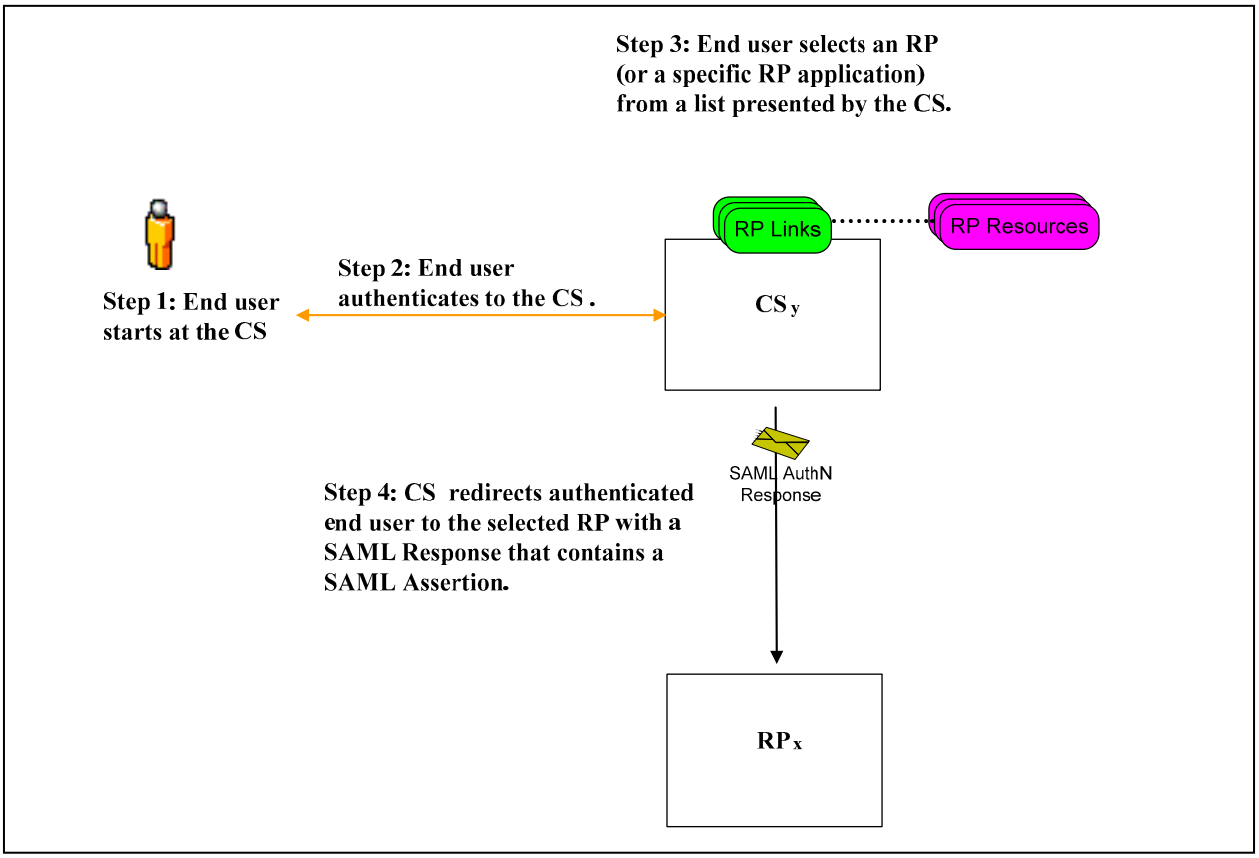
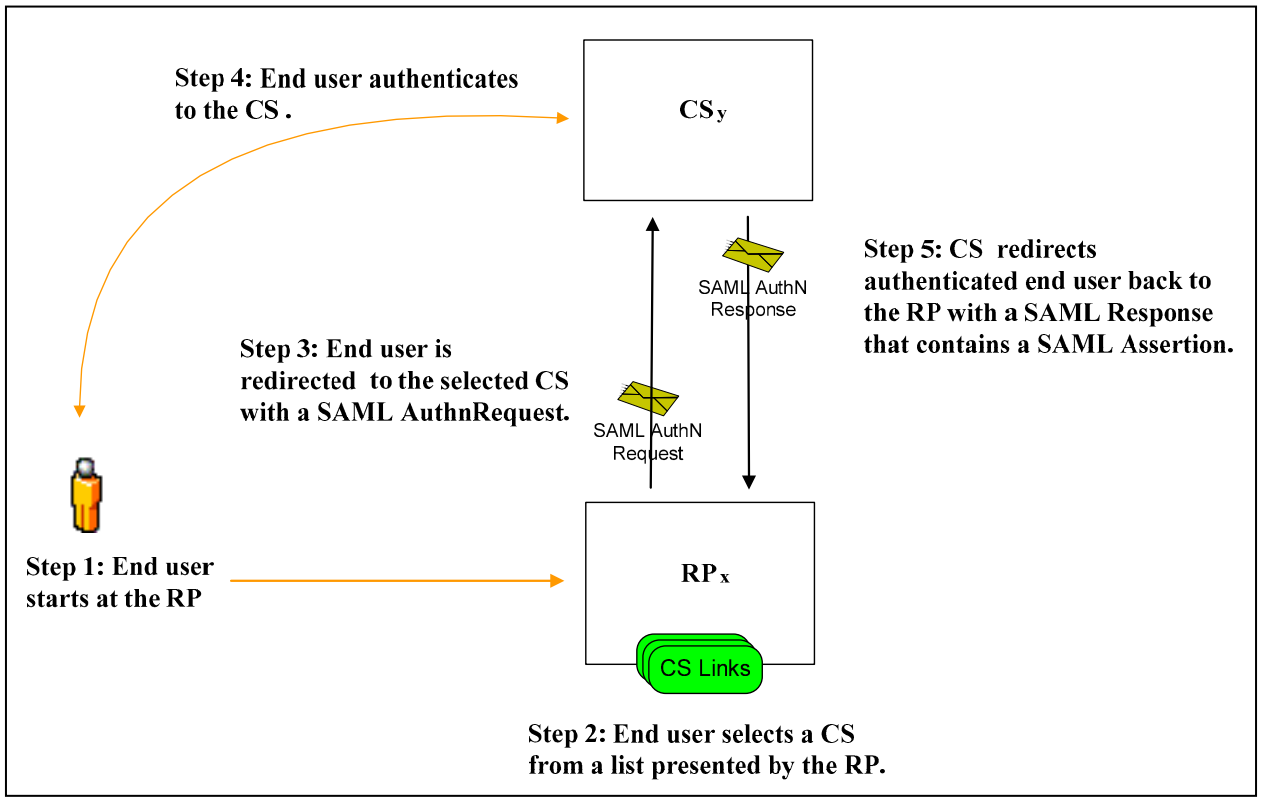


Figure 1-4 RP Presents Links



1.9.1.3 Links Presented by an External Site

This adopted scheme supports use of an external site (i.e., non-Federation member site) for CS or RP discovery by an end user. Examples of an external site include USA.gov, FORMS.gov, and an agency portal. The external site presents the end user with a list of RPs and/or CSs. However, the external site limits the end user to selecting only one or the other. That is, the end user cannot select both a CS and an RP at the external site. Once the end user selects a CS or RP, the external site redirects the end user accordingly, whereupon the selected site continues with normal scheme processing as applicable (e.g., presenting links to select a compatible system, processing per SSO).

1.9.1.4 SSO Discovery of a CS

Upon detecting an end user seeking to access its service without a SAML assertion, the RP determines whether the end user has already authenticated to a compatible CS. Per [SAML2 Profile] Identity Provider Discovery Profile, the RP uses its common domain service to read the end user's common domain cookie, if present in the browser. If the RP discovers a compatible CS listed in the common domain cookie, the RP may initiate SSO processing (i.e., immediate redirect to the discovered compatible CS), rather than presenting the end user with a list or sub list of compatible CSs from which to choose.

1.9.2 Session Reset

An RP may want to re-authenticate the end user during a currently active RP session. Reasons include, but are not limited to the following:

- The end user has been idle for a while, and the RP wants to confirm that the end user is still at the machine;

- The end-user wants to initiate a transaction deemed sensitive by the RP; and
- 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 CS responsible for the end user's current authentication session. Upon receipt, the CS re-authenticates the end user, even if the CS's own policies do not require re-authentication at that time (i.e., the end user's authentication session has not yet expired). Please see [Interface Spec] for additional details.

Similarly, a CS may want to re-authenticate an end user returning to it, even if the end user authenticated to it earlier in the same browser session and SSO is in effect. This is done by the CS setting an authentication session timeout.

1.9.3 Transaction Identification (Tracking)

Tracking transactions across ASC entities is performed by Federation member systems via an ID that originates in the SAML assertion, and uniquely identifies the SAML assertion. Propagating the assertion ID to subsequent transactions allows a set of transactions to be logically connected and traced back to the originating authentication transaction. Please see [FMD] and [Interface Spec] for additional details.

1.9.4 Error Handling and Help Desk

Federation members are responsible for error handling in accordance with [FMD] and [Interface Spec]. Responsibilities include:

- Federation member system displays error pages with messages;
- Federation member provides error reports and help desk statistics to the PMO;
- Federation member system undergoes error testing by the Federation Lab; and
- Error messages direct end users to the Federation member help desk first, rather than the FOC Helpdesk

1.9.5 Scheme Translation Determination

Before technically interoperating with a partner, the Federation member system uses configured metadata to determine whether direct communication is possible or scheme translation is required. This requires that:

- The Federation Operations Center (FOC) ensures metadata contains correct translation service URLs when applicable; and
- Federation members create links to scheme translators instead of partners when translation is required

1.9.6 Federation Information

Different sites display Federation information, which includes:

- The Federation web site located at http://cio.gov/eauthentication;
- Federation member systems; and
- External sites as may be used (e.g., USA.gov)

System owners manage the Federation information displayed on their systems in accordance with [FMD].

1.10 Use Cases

This adopted scheme encompasses numerous use cases. This section presents those use cases, highlighting the transaction flow underlying each. The use cases present the transaction flows in detail to provide a more complete picture of what actually occurs – in terms of user experience and protocol specific messages. This section and [Tech Approach] present the higher-level flows.

The primary actors (i.e., ASC entities) in each use case are the CS, RP, end user, and/or Federation Domain Name Service (DNS). Flow and interaction occurs amongst the actors.

To support single sign-on, every CS and RP using this adopted scheme utilizes the Federation common domain, which is a shared environment. However, transactions that occur between the end user and CS, and between the end user and RP remain confidential. This adopted scheme requires Federation member systems to be comprised of two underlying domains because the Federation common domain would jeopardize confidentiality if Federation member systems exist entirely in a shared environment. The two domains are:

- **Application Domain** – externally facing application that end users access and interact with to conduct transactions; this is the Federation member's existing application, which is not included in the Federation common domain in order to protect privacy and confidentiality; and
- **Common Domain** – internal service the CS or RP uses to access an end user's common domain cookie and perhaps facilitate end user discovery of a compatible CS; it has no confidential information and has no access to or knowledge of application domain processing; this internal service is included in the Federation common domain; common domains are coordinated with the Federation DNS

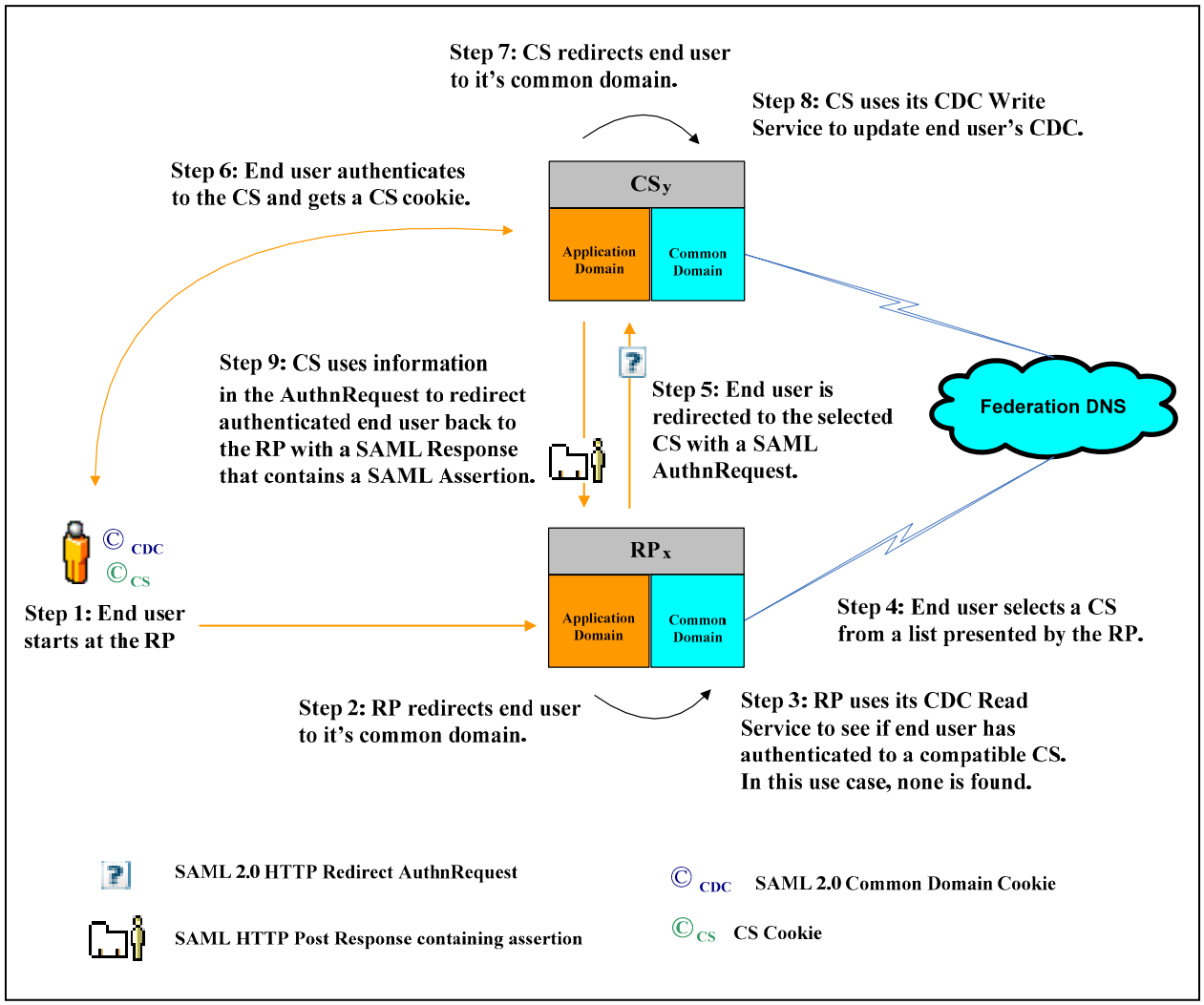
Although comprised of two underlying domains, a CS or an RP appears to be one logical entity to end users, other Federation member systems, and the FOC. For end users, there is no difference whether interacting with a Federation member system in its application domain or in its common domain That is, crossing domains is seamless and transparent. For example, an RP's common domain may interact with the end user for selection of a compatible CS. However, the end user does not notice the application domain has redirected him or her to the common domain, and that he or she is now interacting with another domain.

The use case diagrams show the underlying domains solely for transaction flow completeness. The orange arrow indicates the end user notices a redirection of their browser to a new web site. An orange application domain box indicates the end user accesses and interacts with that ASC entity at some point during the use case. All cookies reside in the end user's browser, and are session based per [OMB M-03-22] (i.e., deleted when the browser session ends).

The GSA hosts and administers the Federation DNS. Each Federation member implements the necessary common domain service necessary for its system, and uses the Federation DNS. The RP requires a common domain read service. The CS requires a common domain read/write service. All entities must implement the common domain in accordance with [SAML2 Profiles].

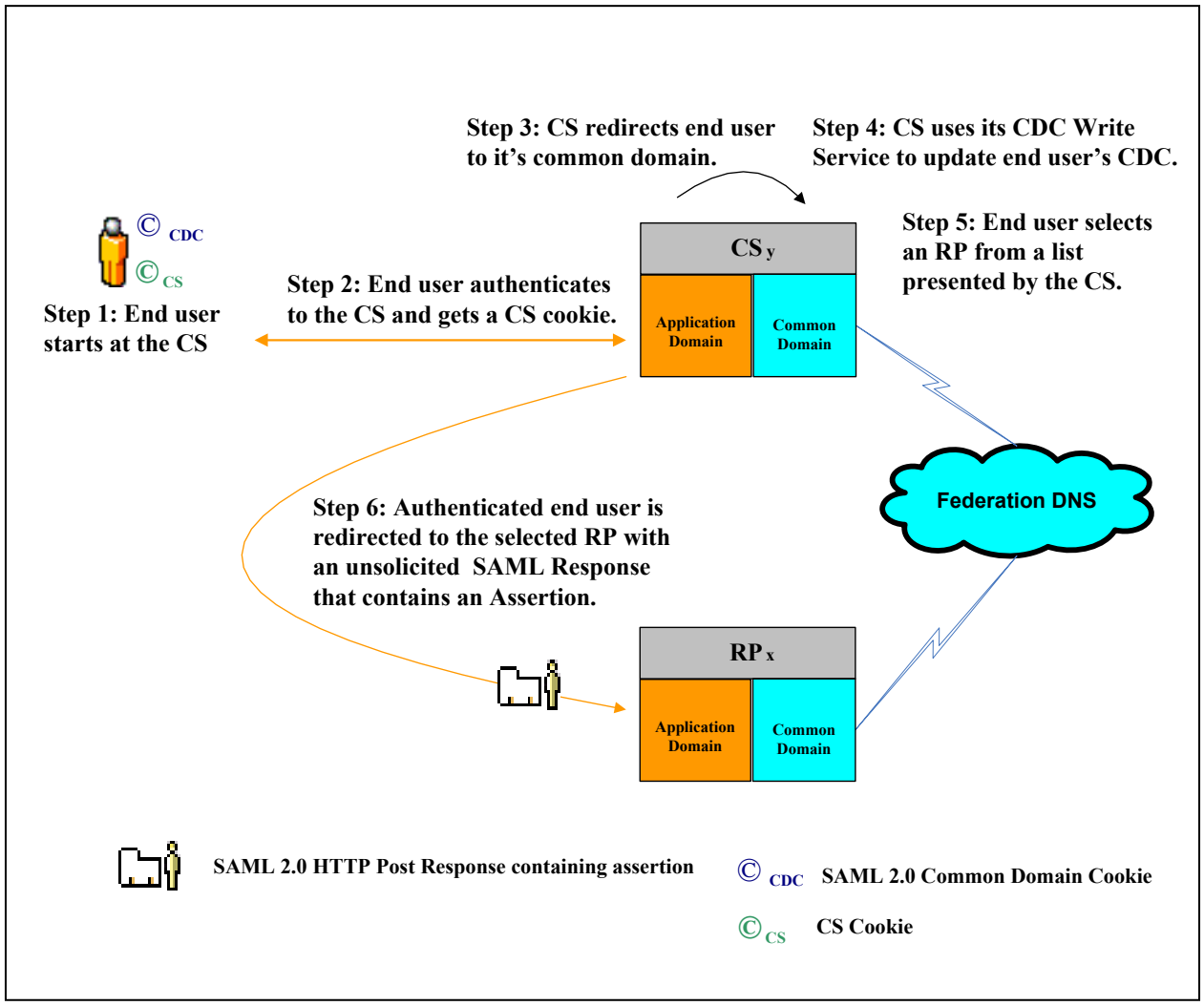
1.10.1 Starting at the RP

Figure 1-5 Use Case: Starting at the RP



1.10.2 Starting at the CS

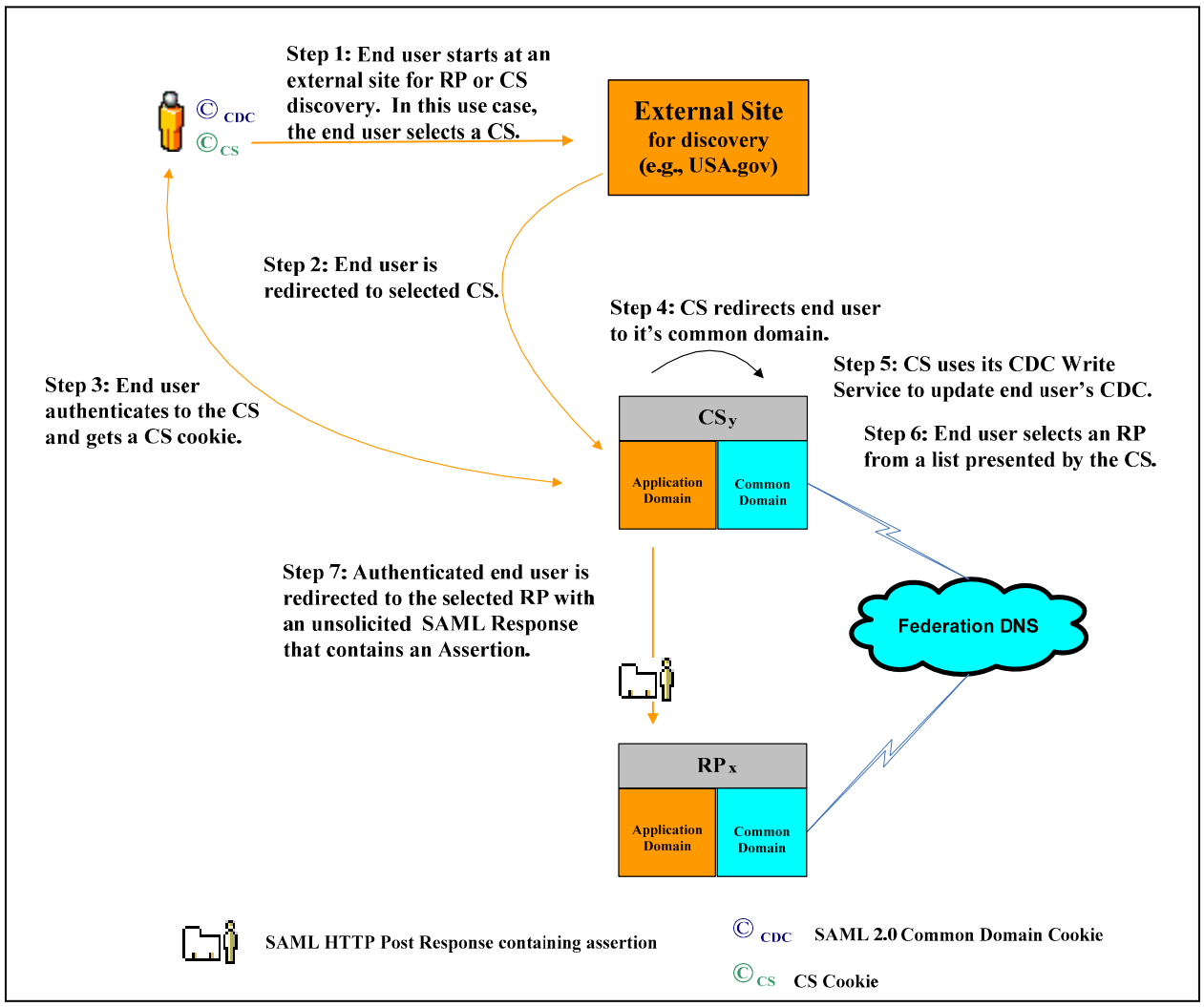
Figure 1-6 Use Case: Starting at the CS



1.10.3 Starting at an External Site

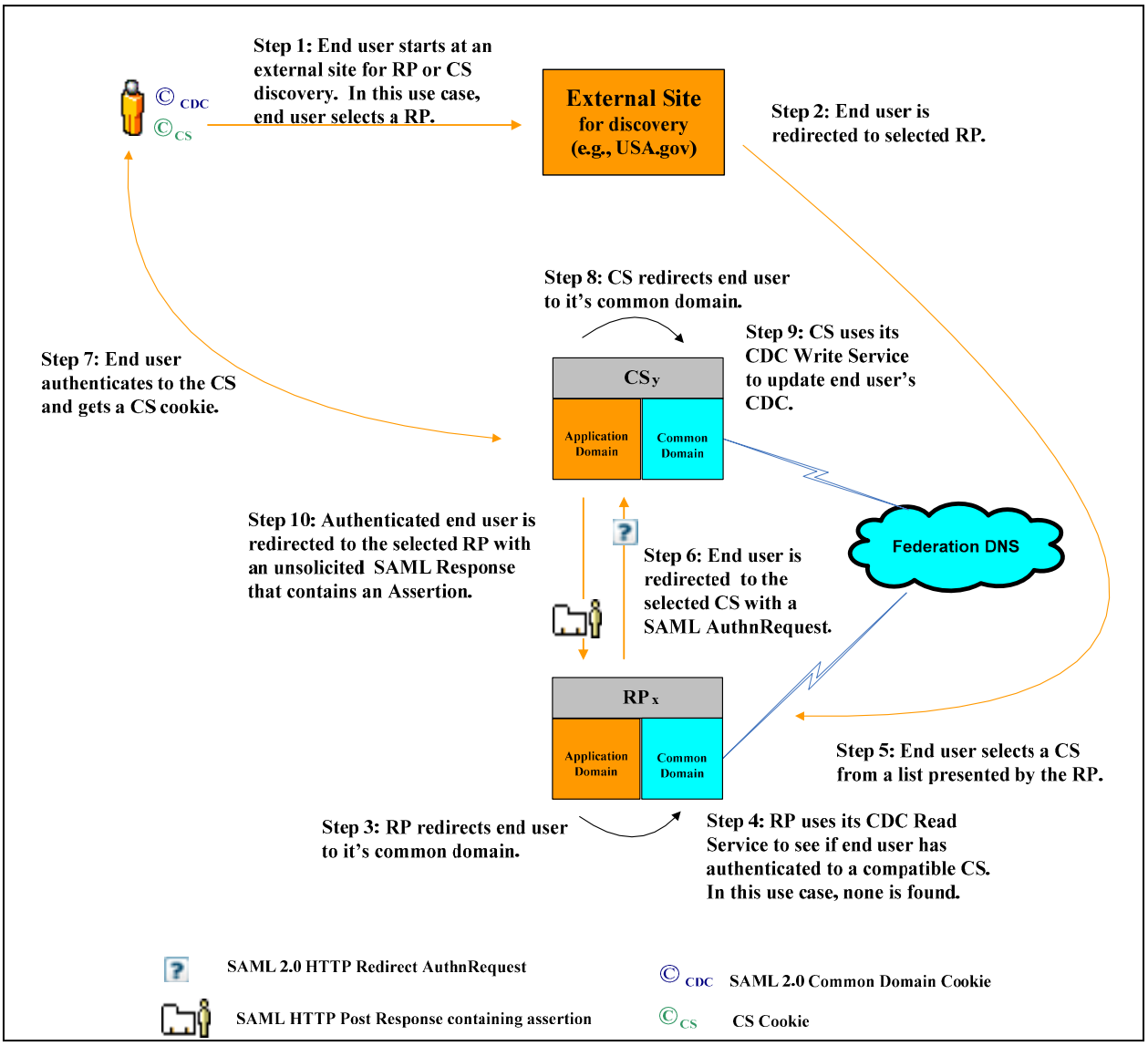
1.10.3.1 Select a CS

Figure 1-7 Use Case: Select CS at External Site



1.10.3.2 Select an RP

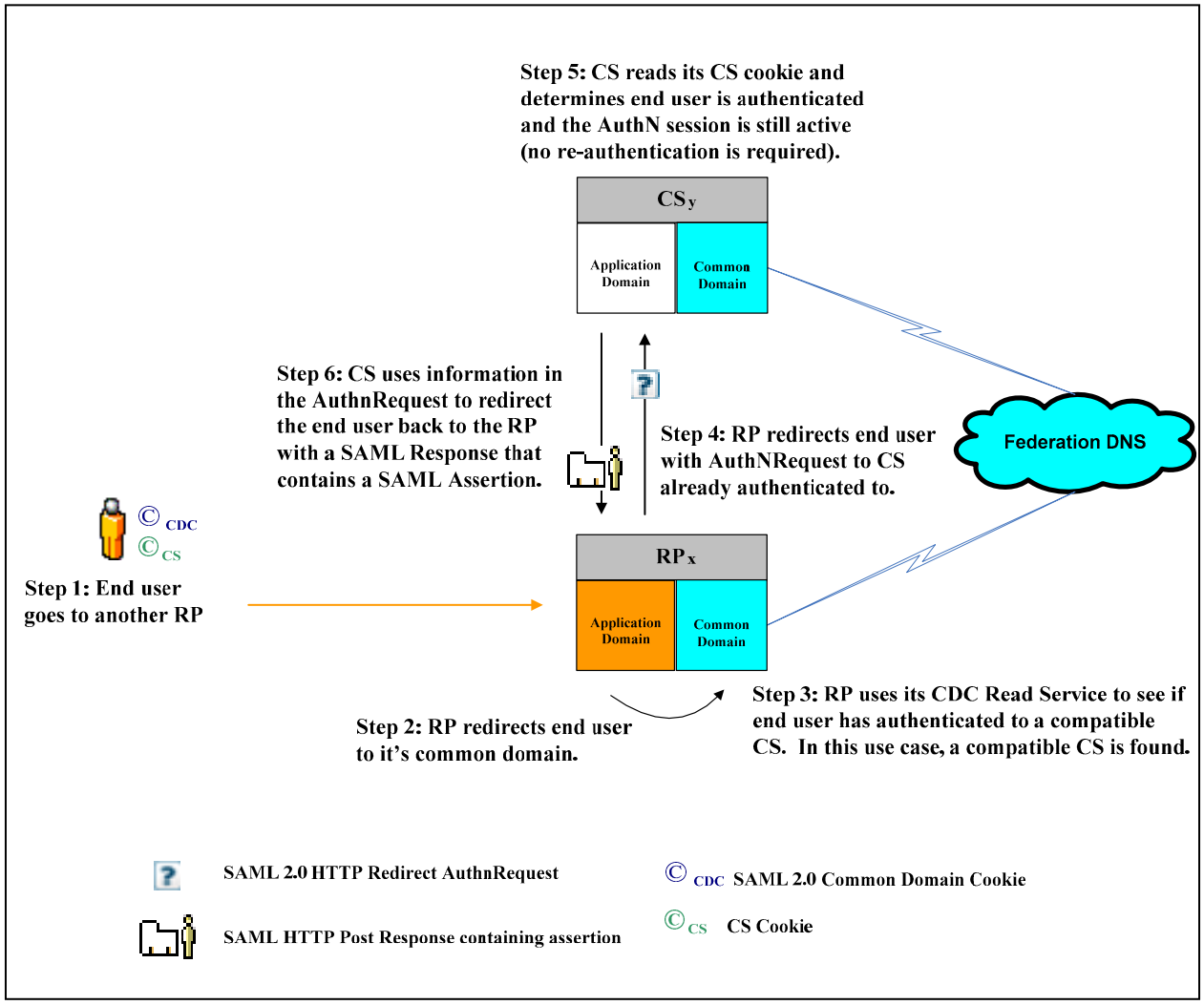
Figure 1-8 Use Case: Select RP at External Site



1.10.4 Single Sign-on

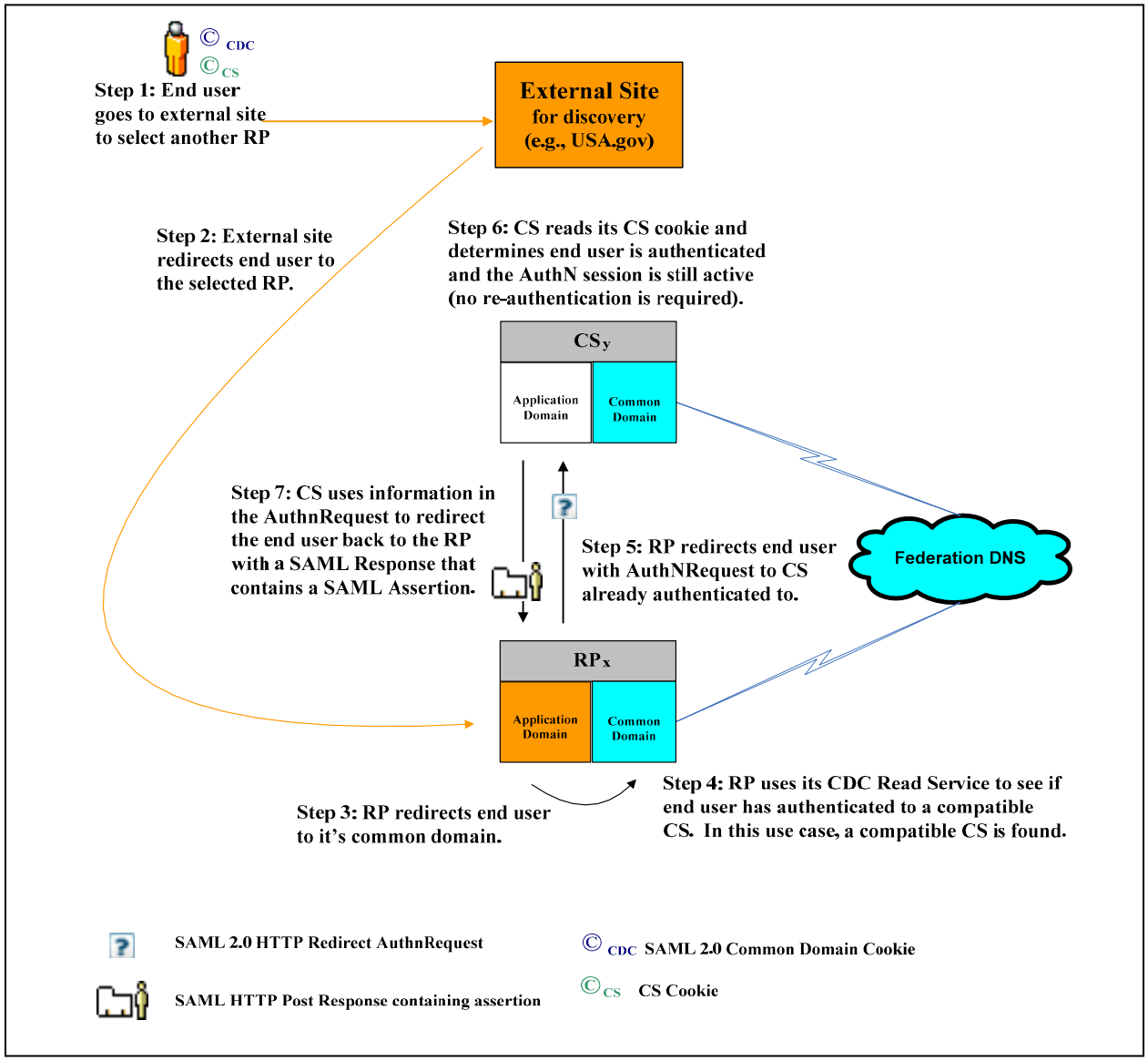
1.10.4.1 Going Directly to another RP

Figure 1-9 Use Case: SSO Direct to another RP



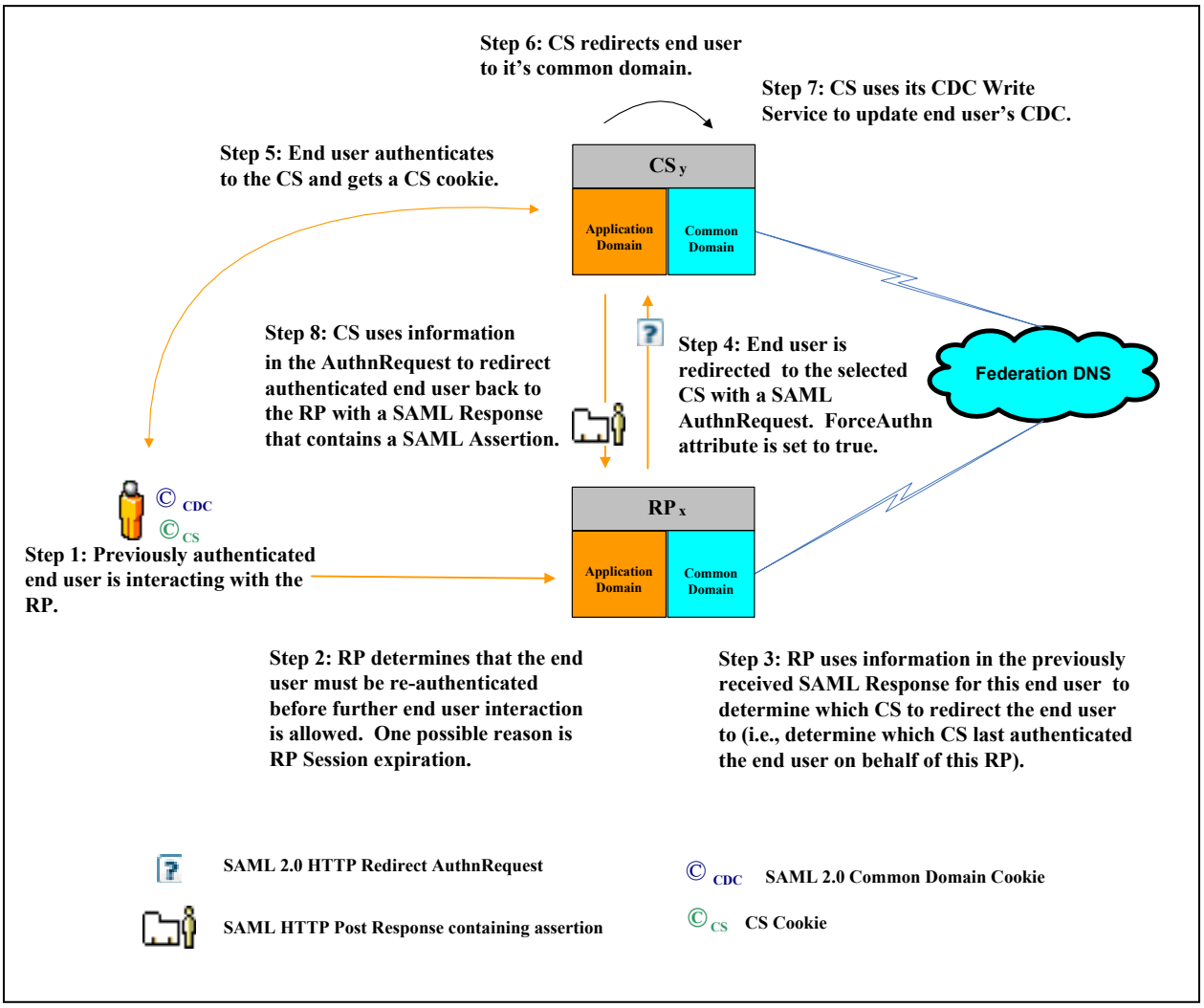
1.10.4.2 Selecting Another RP from an External Site

Figure 1-10 Use Case: SSO Select another RP from External Site



1.10.5 Session Reset

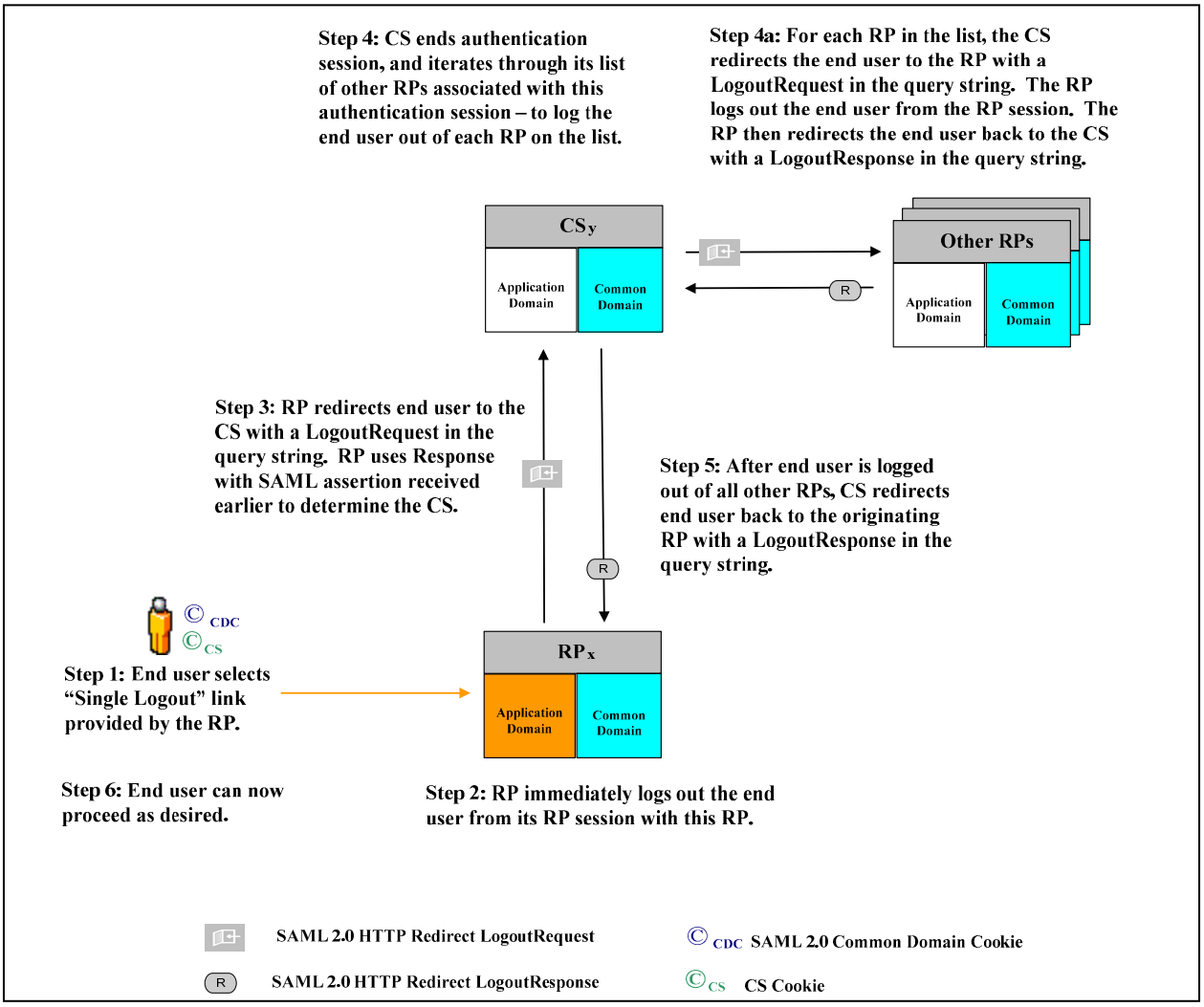
Figure 1-11 Use Case: Session Reset



1.10.6 Single Log-out

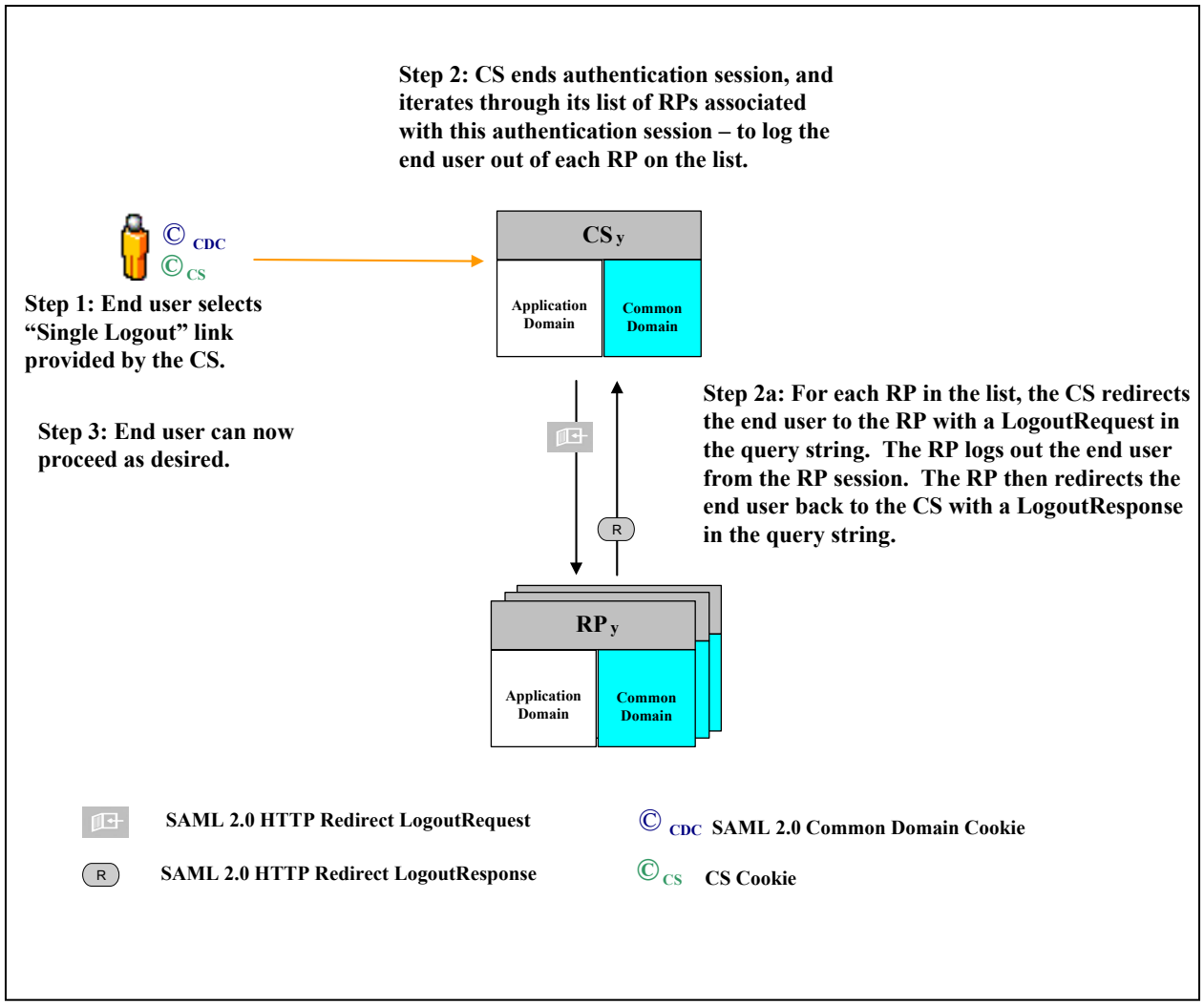
1.10.6.1 SLO from an RP

Figure 1-12 Use Case: Single Logout from an RP



1.10.6.2 SLO from a CS

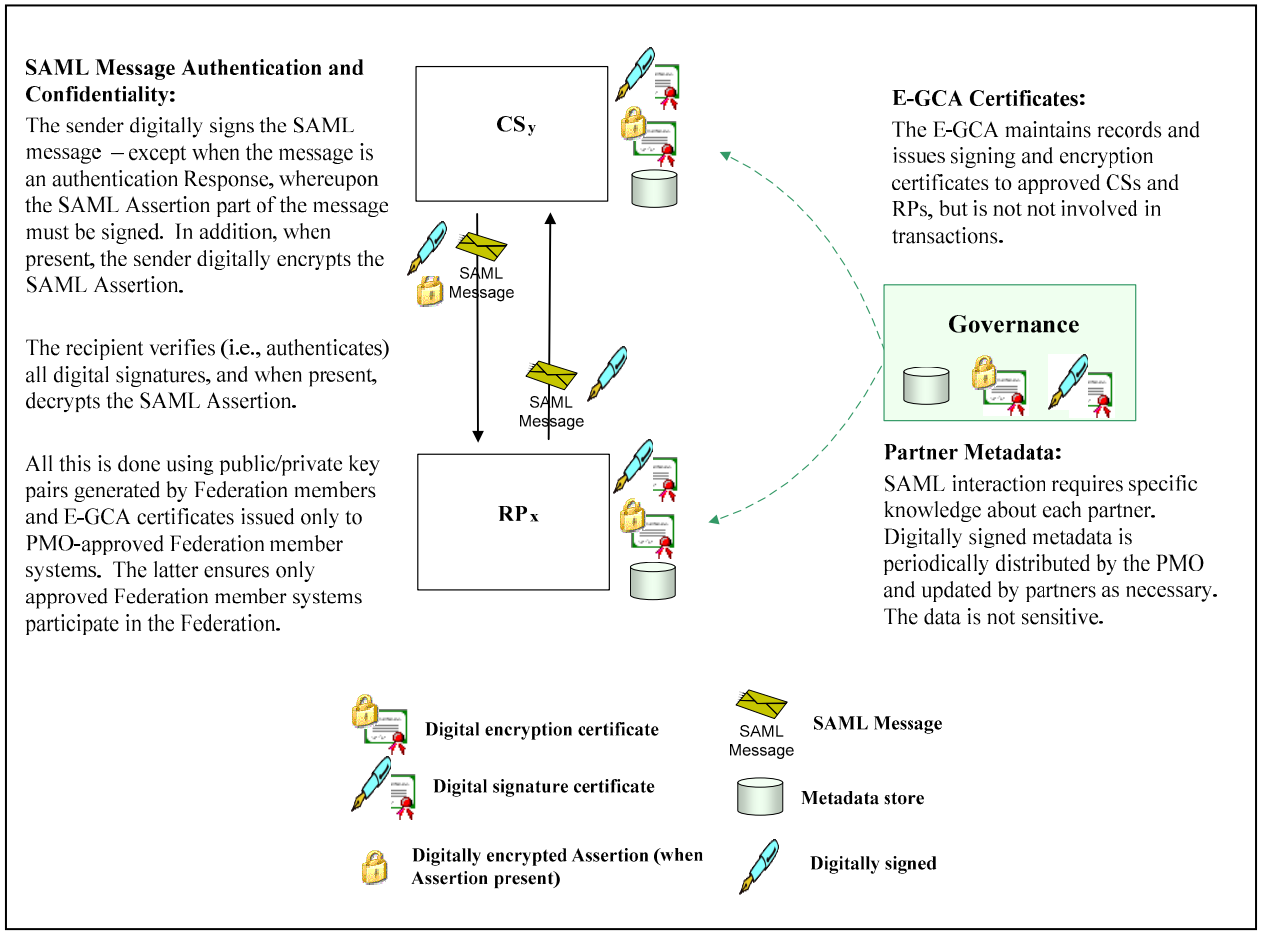
Figure 1-13 Use Case: Single Logout from a CS



1.11 Governance

Any architecture for government-wide authentication must provide some mechanism for the government to assert its authority over which entities can participate. This section describes such mechanisms specifically for this adopted scheme, such as metadata, digital signing, and digital encryption.

Figure 1-14 Governance



1.11.1 E-GCA Certificates

SAML 2.0 supports message level digital signing and digital encryption via XML Signature and XML Encryption respectively. Each requires a public /private key pair and corresponding X.509 digital certificate. See [SAML2 Security], [XML Sig], and [XML Enc] for details.

As figure 4-2 illustrates, the E-GCA issues:

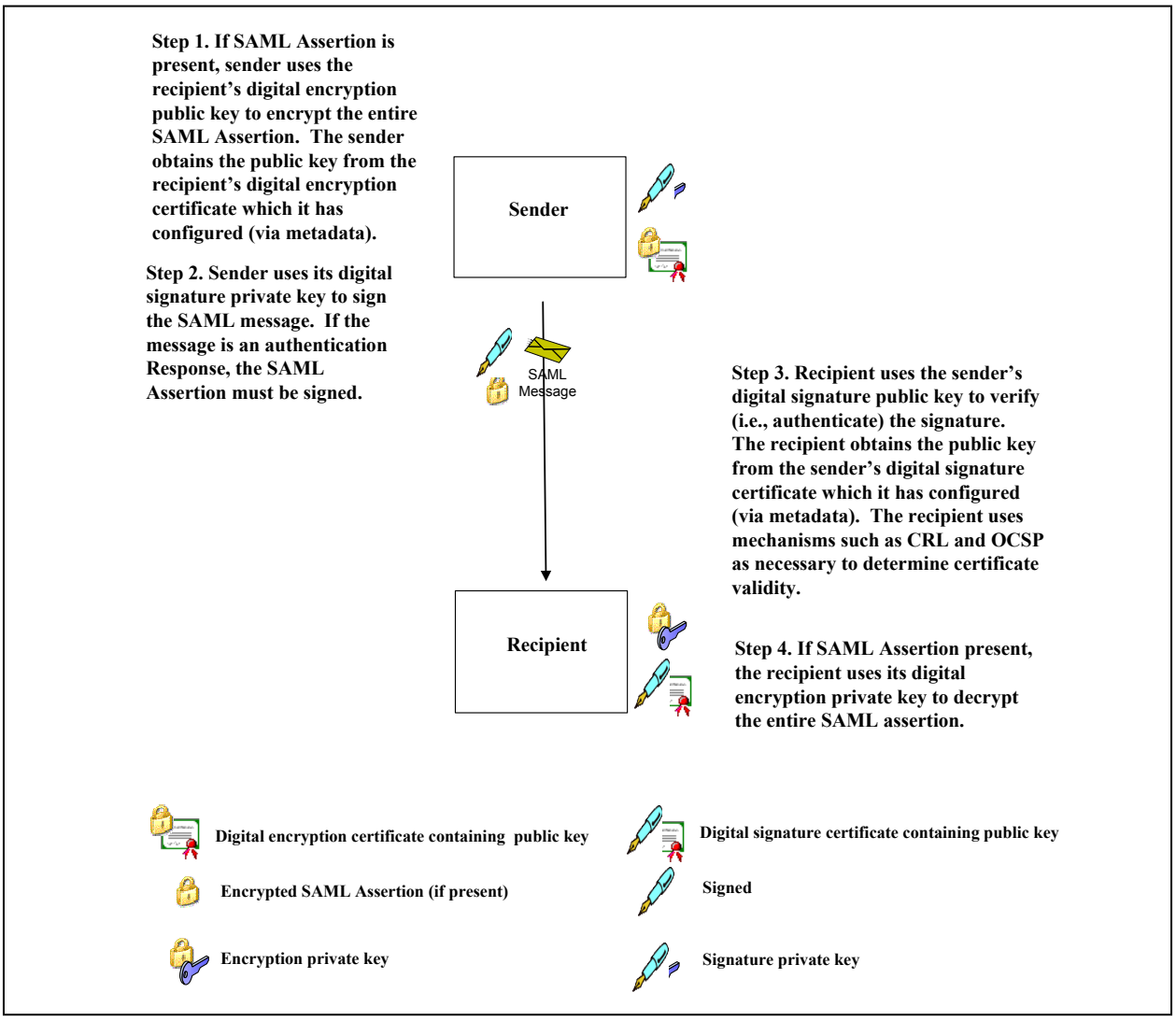
- Each RP:
  - An X.509 public key certificate exclusively for verifying the RP's digital signature; and
  - An X.509 public key certificate exclusively for encrypting a SAML assertion to be sent to the RP
- Each CS:
  - An X.509 public key certificate exclusively for verifying the CS's digital signature

Federation members pass their public key certificates to partners via metadata. A single CA issues both types of certificates. The E-GCA issues the certificates only to PMO-approved systems. This controls which systems participate in the Federation using this adopted scheme. A recipient rejects (i.e., does not process) a SAML message whose signature fails verification (i.e., the sender cannot be authenticated as a trusted system). Federation member systems are both senders and recipients of SAML messages, depending upon the SAML messages involved.

The Federation member is responsible for (a) generating the private/public key pair used for signing and encryption, and (b) providing the E-GCA with the public key.

The E-GCA issues, renews, and revokes the certificates periodically as necessary.

Figure 1-15 Use of E-GCA Certificates



1.11.2 Metadata

In this adopted scheme, SAML 2.0 message exchange between two ASC entities requires each to have specific knowledge about the other prior to technical interoperation. One example is the URL of each service with which an ASC entity technically interoperates. Without such knowledge, an ASC entity does not know where to send SAML related messages for processing. Metadata describes and conveys such information. Every Federation member creates and maintains a metadata file for each approved CS or RP it operates. There is one metadata file per approved system.

Federation members do not exchange metadata files directly. Instead, they sign and submit metadata files to the PMO. The PMO then maintains the authoritative copy of all Federation members' metadata, and distributes metadata files to Federation members as necessary.

Upon receipt, the PMO verifies the Federation member signature. The PMO then quality checks metadata content. This includes, but is not limited to verifying completeness and correctness. The PMO then distributes metadata files to applicable Federation members in a secure manner.

Upon receipt of a metadata file, the Federation member checks metadata content. If correct and complete, the Federation member system consumes the metadata as necessary (i.e., the Federation member system configures itself with the necessary metadata). Failure to configure metadata completely and correctly can preclude technical interoperation, or result in unexpected consequences or negative impacts to any number of Federation member systems.

Metadata is not sensitive and not expected to change very often. Despite its role in facilitating metadata distribution, the PMO is not involved in authentication transaction processing (the PMO focuses on policy and assessment tasks). System entities such as RPs and CSs interact directly with each other for authentication transactions using configured metadata.

This adopted scheme implements metadata in accordance with [SAML2 Metadata]. This includes:

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

1.12 SAML Message Summary

SAML Feature	SAML Request Message	SAML Response Message	Comments
Authentication	AuthnRequest	Response	▪ No AuthnRequest if end user starts at the CS ("Unsolicited HTTP POST") ▪ Encrypted assertion ▪ Signed assertion ▪ HTTP Redirect for AuthnRequest ▪ HTTP POST for Response
Single Sign-on	AuthnRequest	Response	▪ Uses Federation Common Domain ▪ Encrypted assertion ▪ Signed assertion ▪ HTTP Redirect for AuthnRequest ▪ HTTP POST for Response
Single Logout	LogoutRequest	LogoutResponse	▪ HTTP Redirect for request and response ▪ Ends authentication session and all associated RP sessions
Session Reset	AuthnRequest	Response	▪ ForceAuthn attribute set to true ▪ Encrypted assertion ▪ Signed assertion ▪ HTTP Redirect for AuthnRequest ▪ HTTP POST for Response

2. ADOPTED SCHEME: SAML 1.0 BROWSER ARTIFACT PROFILE

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

For an overview of this adopted scheme, please see:
http://www.cio.gov/eauthentication/documents/SAMLprofile.pdf.

APPENDIX A: GLOSSARY

Term	Definition
Activation	Ties an end user to a unique subject name in a SAML assertion, and updates the RP to recognize that end user with certainty. Activation solves the challenge of an RP distinguishing amongst end users – particularly amongst end users with the same name.
Adopted Scheme	Precisely scoped identity scheme accepted for use by the Federation.
Application Domain	RP or CS externally facing application that end users access and interact with to conduct transactions; this is the Federation member's existing application, which is not included in the Federation common domain in order to protect privacy and confidentiality.
Approved	Acceptance by the E-Auth PMO to participate in the E-Authentication Federation, or other inclusion or use in the E-Authentication Federation.
Assertion	A piece of data produced by a CS regarding either an act of authentication performed on a principal (e.g., end user), attribute information about the principal, or authorization data applying to the principal with respect to a specified resource.
Authentication	The process of establishing confidence in user identities. Authentication is different from authorization. However, they are usually inextricably linked. Authentication precedes authorization. Authentication simply establishes identity, or in some cases verified personal attributes (e.g., zip code), but not what that identity is authorized to do or what access privileges he or she has; this is a separate decision. The RP can use the authenticated information provided by the identity verifier to make authorization or access control decisions. The Federation directly addresses authentication, and indirectly supports authorization.
Authentication Service Component Entity (ASC Entity)	The ASC comprises various entities that actively participate in the authentication process. An ASC entity can be a system, a person, or group of persons that has a distinct role. Examples include RPS, CSs, end users, and external sites providing Federation discovery services.
Authentication Session	Period of time that an end user remains trusted after the end user authenticates. That is because a CS typically does not require an end user to re-authenticate for every page requested. Each CS defines its own authentication session duration. If an end user returns to the CS and an earlier authentication session has expired, the CS re-authenticates the end user – even if single sign-on is in effect.
Base64 Encoded	Positional notation using a base of 64. It is the largest power-of-two base that can be represented using only printable ASCII characters. This has led to its use as a transfer encoding for e-mail among other things.
Binding	Mappings of SAML request-response message exchanges onto standard messaging or communication protocols.

Term	Definition
Common Domain	RP or CS internal service to access an end user's common domain cookie and perhaps facilitate end user discovery of a compatible CS; it has no confidential information and has no access to or knowledge of application domain processing; this internal service is included in the Federation common domain; common domains are coordinated with the Federation DNS.
Common Domain Cookie (CDC)	Browser cookie that tracks the CSs to which the end user has authenticated during a particular session. CSs read and update the CDC. RPs read the CDC.
Compatible	Two Federation Member systems may technically interoperate if: ▪ The CS has an equal or higher assurance level than the RP, ▪ The CS is can provide all optional attributes required by the RP, and ▪ The CS and RP use the same interface specification version, or a scheme translator is available
Cookie (Transient Cookie)	A message given to a web browser (e.g., end user's web browser) by an ASC entity. The web browser stores the message in a file that is accessible only to the entities within the domain where the message was provided. The ASC uses cookies to facilitate single sign-on, and to manage sessions (e.g., RP session, authentication session). In addition, the ASC only uses transient cookies, which are stored in temporary memory and erased when the end user closes their web browser. Cookies do not collect information from the end user's computer. Cookies typically store information in the form of a session identification that does not personally identify the end user.
Credential Service (CS)	A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential, then each one is considered a separate CS.
CS Cookie	Once a CS authenticates an end user, the CS assigns a session cookie to the end user's browser. Upon subsequent end user visits to the CS during the same browser session, the CS uses the CS cookie to determine the end user's identity, whereupon the CS can redirect the end user without any end user interaction (i.e., no authentication required since the end user authenticated earlier), thus completing the single sign-on sequence. Content and sensitivity of the CS cookie varies among CSs.
Digital Encryption	Private key data encryption that converts data into a form that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.
Digital Signature	An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection.
Discovery	Process of an end user finding a CS and/or RP.
Domain Name Service (DNS)	Service that translates numerical IP addresses into names to identify servers on the network.

Term	Definition
E-Authentication Program Management Office (PMO)	The PMO is the organization that handles Federation program management, administration, and operations. The PMO is not involved in authentication of transactions.
E-Governance Certification Authorities (E-GCA)	Established by the government to issue certificates as applicable for the adopted scheme. Certificates that may be issued are for mutual TLS authentication, digital signing, and digital encryption. E-GCA certificates effectively control which entities can participate in the Federation.
Extensible Markup Language (XML)	XML is a specification developed by the W3C that enables the definition, transmission, validation, and interpretation of data between applications and between organizations. In a nutshell, XML describes data and focuses on what data is. XML facilitates technical interoperability, and is used in identity management standards such as SAML (e.g., to convey information in a SAML assertion).
External Site	Non-Federation member system that provides end user discovery service, and redirects the end user to the selected Federation member system. Examples include agency portals, and government sites such as USA.gov.
Federation Domain Name Service (DNS)	DNS provided and hosted by the Federation to support common domain cookie sharing/processing.
Governance	ASC mechanisms for the government to assert its authority over which ASC entities can participate in the Federation. The PMO accomplishes this by managing the interaction between ASC entities – primarily between RPs and CSs. For this adopted scheme, ASC governance mechanisms include issuance of E-GCA certificates for signing and encryption, as well a metadata management.
HTML Form Control	User interface control that serves as a point of user interaction HTML forms.
Hypertext Markup Language (HTML)	The basic language used to write web pages, which are read by browsers.
Hypertext Transfer Protocol (HTTP)	Underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. In the Federation, where appropriate, HTTP is used to redirect end users.
Metadata	SAML 2.0 message exchange between two ASC entities requires each to have specific knowledge about the other. One example is the URL of each service with which an ASC entity technically interoperates. Without such knowledge, an ASC entity does not know where to send SAML related messages for processing. Metadata describes and conveys such information.
Name Qualifier	A string that disambiguates an end user name identifier in a federated environment.
Partner	From a technical standpoint, other Federation member systems with which a Federation member system technically interoperates. From a business standpoint, other Federation members with whom a Federation member has a relationship.

Term	Definition
Private Key	The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.
Public Key	The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.
Public Key Certificate	A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key.
Public Key Infrastructure (PKI)	Using a combination of private (i.e., secret) key and public key cryptography, PKI enables a number of other security services including data confidentiality, data integrity, and non-repudiation. PKI is the combination of software, encryption technologies, and services that enables entities to protect the security of their communications and business transactions on networks. PKI integrates digital certificates, public key cryptography, and certification authorities into a complete network security architecture. A typical PKI encompasses the issuance of digital certificates to individual users and servers; end-user enrollment software; integration with certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.
Redirect	Transfer of an end user from one node (i.e., operation Federation member system) to another, as necessary. For example: • After authenticating an end user, the CS redirects the end user to the RP; • An end user that starts at an RP but has not yet been authenticated is redirected by the RP to a selected CS
Relying Party	An entity that relies upon the subscriber's credentials (i.e., requires an end user to be authenticated), typically to process a transaction or grant access to information or a system.
RP Session	The period of time an RP will trust an end user before issuing a session reset request to re-authenticate the end user (i.e., redirect the end user back to the CS). Since RPs do not have access to authentication session information, RPs must maintain their own session with an end user. The RP sets the time limit for the RP session.
Scheme Translation	Use of scheme translators to support interoperability between CSs and RPs that use different adopted schemes. Scheme translators pass identity information based on standards already adopted in the architecture. The architectural framework allows multiple scheme translators to be deployed allowing for an increase of availability and end user privacy. There is no need for RPs or CSs to engage in any special integration for scheme translators. The translators appear to be any other CS from the RP perspective, and any other RP from the CS perspective. Organizations that have invested in one of the adopted schemes will be able to use their existing systems so long as the scheme translators are available.

Term	Definition
Security Assertion Markup Language (SAML)	The set of specifications describing security assertions that are encoded in XML, profiles for attaching the assertions to various protocols and frameworks, the request/response protocol used to obtain the assertions, and bindings of this protocol to various transfer protocols (for example, SOAP and HTTP). SAML addresses web single sign-on, web services authentication, attribute exchange, authorization, non-repudiation, and secure communications. SAML defines assertion message formats that are referenced in Liberty Alliance, Shibboleth, WS-Security, and other specifications. SAML has become the standard web SSO identity management solution. Several versions have been released to date, including SAML 1.0, SAML 1.1, and SAML 2.0. The Organization for the Advancement of Structured Information Standards (OASIS) oversees SAML.
Signature Verification	The process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.
Single Logout (SLO)	Near-simultaneous logout of a collection of related sessions on request. In ASC terms, it is the logout of an end user from all active RP sessions associated with a specific authentication session.
Single Sign-on (SSO)	Once an end user has authenticated their identity at a CS, he or she may, by their choice, move among RPs compatible with the CS without re-authenticating. In other words, the end user is seamlessly logged into any other RP compatible with the CS. For privacy considerations, end users must take explicit actions to opt-in to SSO. SSO applies to assertion based Federation member systems only. In addition, SSO is in effect only for the duration of the end user's current browser session and authentication session. An end user must opt-in to SSO each time he or she opens a new web browser session. The ASC supports SSO as a core aspect of the federated architecture.
Stateless	Not having (not needing) information about what occurred previously. Stateless solutions can reduce complexity and/or increase flexibility.
Use Case	A methodology used to identify, clarify, and organize system requirements.
Web Browser	Web browsers communicate with web servers primarily using HTTP (hypertext transfer protocol) to fetch web pages. HTTP allows web browsers to submit information to web servers as well as fetch web pages from them. Web pages are located by means of a URL (uniform resource locator), which is treated as an address. Cookies can be sent by a server to a web browser and then sent back unchanged by the browser.

APPENDIX B: ACRONYMS

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