Technical Approach for the Authentication Service Component

Version 2.0.0
Final
May 4, 2007

Document History

Status	Release	Date	Comment	Audience
Draft	0.0.1	11/03/03	Initial Draft, limited release, do not distribute	Limited
Release Draft	1.0.0 RC1	05/17/04	Updated per comments	Limited
Release Draft	1.0.0 RC2	05/28/04	Updated per comments	Limited
Final	1.0.0 RC3	06/28/04	Public release	Public
Release Draft	1.1.0 RC1	9/11/05	Initial draft of version 1.1.0	Limited
Release Draft	1.1.0 RC2	10/5/05	Updated per comments	Limited
Release Draft	1.1.0 RC3	10/20/05	Updated per comments	User Group
Final	1.1.0 RC4	11/15/05	Public release	Public
Draft	1.1.1	2/20/07	Initial revisions to address additional adopted scheme (SAML 2.0 SSO Profile Using HTTP POST). Make presentation more generic, rather than SAML 1.0 Browser Artifact Profile specific.	Internal
Draft	1.1.2	2/21/07	Updates per internal review	Internal
Draft	1.1.3	2/23/07	Updates per internal review	Red Team
Draft	2.0.0 RC1	3/2/07	Updates per Red Team	PMO
Draft	2.0.0 RC2	3/30/07	Updates per public comment	PMO
Draft	2.0.0 RC3	4/20/07	Updates per public comment	Internal
Final	2.0.0	5/4/07	Updates per PMO comment	Public

Editors

Dave Silver
Andrew Chiu
Steve Lazerowich

Terry McBride
Chris Broberg
Matt tebo

Chris Louden
Treb Farrales

Executive Summary

As a key component 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.

After careful analysis and proofs-of-concept, the E-Authentication Program Management Office (PMO) decided to implement E-Authentication infrastructure as a federated architecture called the Authentication Service Component (ASC). The ASC leverages credentials from multiple credential providers through certifications, guidelines, standards, and policies. The ASC accommodates assertion-based authentication and certificate-based authentication. Assertion-based authentication uses passwords and PINs. Certificate-based authentication uses Public Key Infrastructure (PKI) certificates.

The ASC is not reliant on a single identity assurance scheme or a single identity assurance commercial product. Rather, the ASC is an architectural framework that (a) supports multiple identity assurance schemes concurrently, and (b) allows any commercial identity product conformant with Federation implementation requirements. Over time, the ASC may support additional schemes as they emerge from identity management standards bodies such as OASIS (e.g., SAML), Liberty Alliance (e.g., Identity Federation Framework), and Internet2 (e.g., Shibboleth).

The Federal Enterprise Architecture (FEA) uses the ASC as its government-wide authentication component.

The technical approach presented herein aligns with Office of Management and Budget (OMB) M-04-04, which provides policy guidance for identity authentication. It also aligns with National Institute for Standards and Technology (NIST) Special Publication 800-63, which is the technical companion document to OMB M-04-04. While the ASC architecture addresses authenticating end users to applications, authorization privileges at the application are beyond the scope of the ASC architecture and this document.

This document discusses core architectural requirements derived from the Federation Strategic Plan (Strategic Plan), including:

- High-level requirements (e.g., leveraging credentials, single sign-on, privacy, governance); and
- Design goals (e.g., standards based approach, use of commercial off the shelf products, federation, durability, flexibility)

In addition, this document discusses:

- Support of multiple authentication models (e.g., assertion based, PKI);
- Support of multiple identity assurance schemes;
- ASC entities (e.g., relying parties (RPs), credential services (CSs), end users, Portals) and their roles in various use cases;
- Various session types within the framework (browser session, authentication session, and RP session);
- Activation;
- Governance; and
- Technical approaches to assertion-based authentication and certificate-based authentication in separate sections because of the significant difference between them

The assertion-based authentication technical approach highlights various transaction flows (use cases) per adopted scheme. This is because these use cases differ from one adopted scheme to another. They include single sign-on, which allows end users to move between RPs of equal or lesser assurance level without re-authenticating. The document shows ASC support of multiple schemes via an abstract transaction flow that seamlessly includes a scheme translator interposed between different adopted scheme protocols. A methodology for scheme adoption is also detailed.

The certificate-based authentication technical approach highlights various PKI transaction flows (use cases) including: (1) RP uses a certificate validation service, and (2) RP integrates validation software to perform local certificate validation. The ASC supports various validation mechanisms including, but not limited to Online Certificate Status Protocol (OCSP), Simple Certificate Validation Protocol (SCVP), and XML Key Management Specifications (XKMS). In addition, the ASC supports use of PKI credentials at assertion-based RPs. A transaction flow for this use case highlights a special scheme translator provided by the Managed Validation and Translation Service. (MVTS).

PKI credentials offer considerable advantages for authentication. They can be validated using only public information (i.e., non-confidential information). Standards for PKI are also more mature and more widely used than the emerging standards for assertion-based authentication of PIN and password credentials. The Federal PKI (FPKI) works to ensure Certification Authorities (CAs) implement similar policies and procedures that allow relying parties to trust credentials at certain levels of assurance. The Federation defers assessment and governance of PKI based CSs to the FPKI Policy Authority (PA), the governing body for the Federal Bridge CA (FBCA).

The technical approach addresses exception scenarios. Similar to use cases, this discussion is specific to each adopted scheme. Standard error codes are used where and when possible to ensure completeness and consistency throughout the ASC.

The technical approach supports secure email by leveraging the PKI certificate validation techniques available in certificate-based authentication. Any Secure/Multipurpose Internet Mail Extensions (S/MIME) capable email software product can be used to process signed and encrypted email. Four use case transaction flows are discussed: (1) email application requests certificate verification from validation service, (2) email application validates the certificate directly by running certificate validation software on the end user's desktop, (3) email application uses a dedicated validation service for organizations who trust certification authorities that are not trusted government-wide, and (4) a combination of the previous options.

In addition, the technical approach supports secure submission of electronic forms. Some Federation members use electronic form applications rather than web forms. These applications do not have the same characteristics as browser-based applications. The section discusses three use case transaction flows, dependent upon the adopted scheme: (1) certificate-based authentication of electronic forms, (2) pop up an E-Authentication browser window in the electronic form to leverage all Federation CSs and to minimize the need to customize electronic forms applications, and (3) use an electronic form with a Security Assertion Markup Language (SAML) assertion embedded within the form.

Table of Contents

Figures

1 INTRODUCTION

1.1 Purpose of this Document

This document sets the technical direction and approach for the ASC. It describes the architectural framework under which the PMO implements technologies, products and technical standards to meet its program objectives. In addition, it provides a methodology for graceful adoption of new identity schemes as they emerge. This is a technical document for a technical audience presumed to be familiar with the Federation.

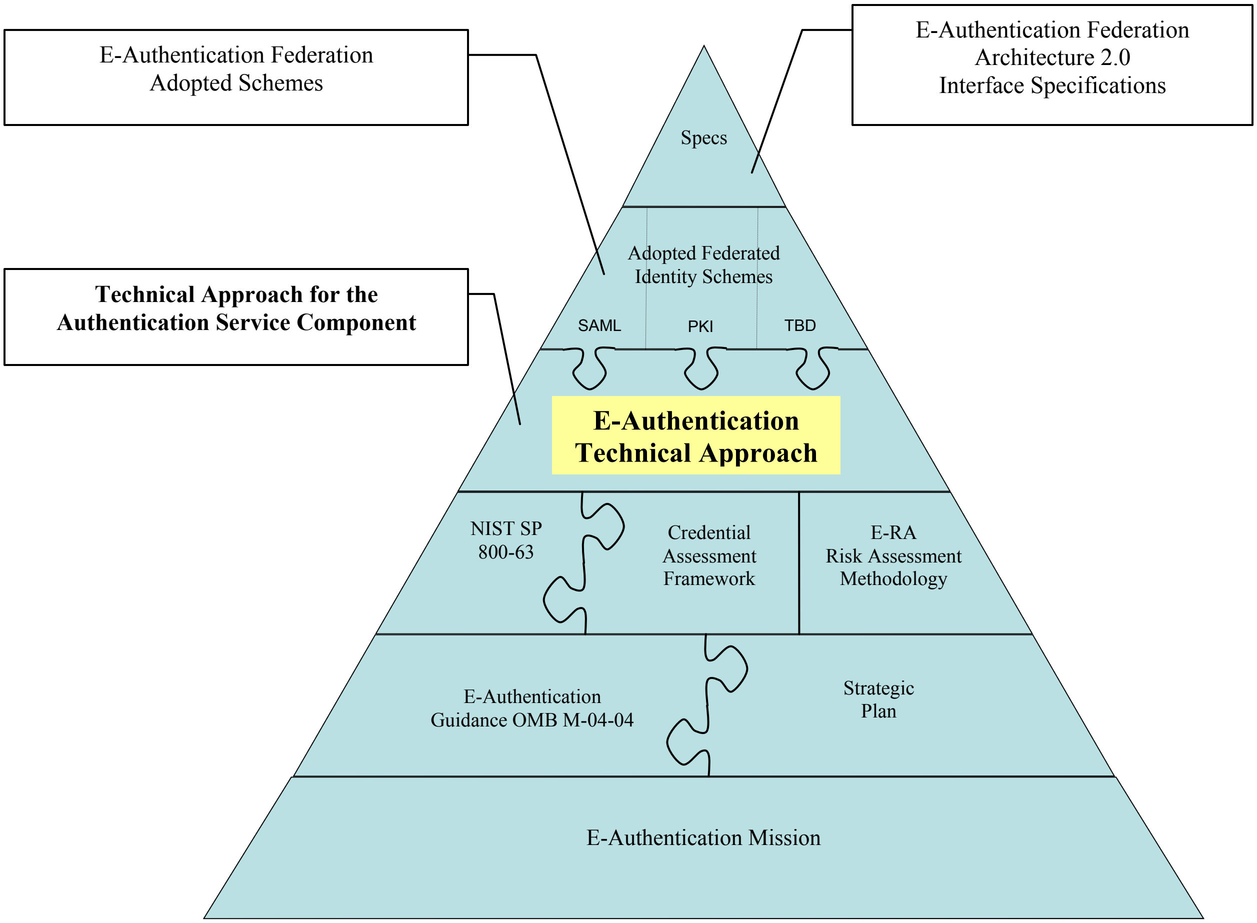
This document is not autonomous. It builds on the following core documents:

- *E-Authentication Guidance for Federal Agencies* [OMB M-04-04]; and
- *Electronic Authentication Guideline* [NIST SP 800-63]

Further, this document is part of the ASC technical suite, which includes (a) an overview for each adopted scheme, and (b) interface specifications for each adopted scheme. Those other documents in the ASC technical suite build on this technical approach document. Therefore, for optimal comprehension, please read this document prior to any adopted scheme or interface specification. Figure 1-1 shows the documentation relationships for E-Authentication.

For additional information about the Federation, and the latest version of each technical suite document, please visit the Federation web site at http://www.cio.gov/eauthentication.

Figure 1-1 E-Authentication Document Hierarchy



1.2 Document References

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

[Burton Group Report] Burton Group Report on the Federal E-Authentication Initiative;
August 30, 2004
http://www.cio.gov/eauthentication/documents/BurtonGroupEAreport.pdf

[FEA] Federal Enterprise Architecture
http://www.whitehouse.gov/omb/egov/a-1-fea.html

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

[HSPD-12] Homeland Security Presidential Directive/HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors;* August 27, 2004
http://csrc.ncsl.nist.gov/policies/Presidential-Directive-Hspd-12.html

[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

1.3 Scope

The E-Authentication technical approach aligns with [OMB M-04-04], which provides policy guidance for identity authentication, not authorization or access control. Specifically, the ASC implements applicable identity authentication recommendations documented in [NIST SP 800-63], which is the technical companion document to [OMB M-04-04].

[NIST SP 800-63] provides recommendations for humans authenticating to applications. While [NIST SP 800-63] does not specify the mechanism by which a human end user authenticates to an application, the ASC specifically addresses authentication using a web browser. Authorization privileges at the application are beyond the scope of this document, [NIST SP 800-63], and the ASC. Application owners are solely responsible for authorization and related functionality such as access control, entitlements, and provisioning.

The Federation Technical Working Group (TWG) considered many features and scenarios not addressed in these guidance documents because of the need to balance utility, complexity, and patience with industry standards. Appendices address approaches for secure email and electronic forms applications. Other features, including Personally Identifiable Information (PII) and attribute sharing, non-browser thin clients (e.g., personal digital assistant, cell phone), cell phone proxies, billing and charge-back protocols, group/role identification, trust agent and power of attorney scenarios have been deferred to a later revision to allow industry standards and government requirements to mature.

For purposes of this document, Transport Layer Security (TLS) includes Secure Sockets Layer V3.0[1].

1.4 ASC Vision and Direction

The Strategic Plan defines the vision and direction for the E-Authentication Federation – including the ASC. The Strategic Plan includes specific actionable tasks to achieve the ASC mission. The tasks encompass design goals and high-level requirements.

1.4.1 Design Goals

1. **Standards-based**: The architectural framework should rely on existing industry standards while remaining cognizant of emerging standards;
2. **Commercial off the Shelf (COTS)**: The architecture should employ COTS products wherever possible;
3. **Federation**: Authentication should be federated amongst multiple credential service providers (CSPs);
4. **Durable**: The architectural framework should be designed to allow for the evolution of technology, providing for easy migration as the industry evolves;
5. **Flexible**: The architectural framework should not rely on any single standard, vendor, product, or integrator;
6. **Scalable**: The solution must be scalable both technologically and administratively;
7. **Reliable:** The architecture must be very dependable, applying best practices and establishing a high level of credibility and confidence;
8. **Ease of use:** Make the end user experience as simple as possible by improving usability, availability and ease of use of credentials;
9. **Ease of adoption:** mitigate technical barriers to entry; and
10. **Cost-effective**: financially viable to implement and maintain

1.4.2 High Level Requirements:

1. **Credential Reuse**: A credential from any approved CS should be usable at any application of equal or lower assurance level. RPs must be able to leverage existing credentials rather than establish new credentialing systems.
2. **Single Sign-on**: Once an end user has authenticated, he or she must be able to move between applications with equivalent (or lower) assurance levels without re-authenticating. For privacy considerations, end users must take explicit action to opt-in to single sign-on.
3. **Privacy Protection**: There must be no central audit log indicating which end users accessed which applications. There must be no centralized electronic authentication system. Credentialing must be federated amongst multiple providers.
4. **Governance**: The architectural framework must provide explicit control over which CSs and RPs can join the Federation.

[1] Use of SSLv3.0/TLS must be compliant with Federal guidelines (e.g., FIPS 140-2, FIPS 180-2, NIST SP 800-52) and agency policies.

5. **Manageable**: The architecture must comply with the policy framework requirements (e.g., [NIST SP 800-63], [OMB M-04-04], [HSPD-12]).

1.5 The Federation Concept

As a key component of the President's Management Agenda, the Federation enables trust and confidence in E-Government transactions via integration of policy and technical infrastructure for electronic authentication. As a result, citizens, businesses and government have simpler and more secure access to multiple online applications through the re-use of credentials and established identities.

Federation members include RPs and CSPs that adopt Federation agreements, standards, and technologies to make identity portable across multiple domains. For more details, please refer to [FMD].

The ASC is the government-wide authentication component of the FEA. The ASC leverages credentials from multiple domains through certifications, guidelines, standards adoption, and policies. The Federation has implemented the ASC as an open, standards-based solution that addresses the need for Federation members to exchange information about their users in a secure and privacy-preserving manner.

Managing transitive trust among RPs (e.g., Federal agencies), CSPs, and the end user community (e.g., individuals, businesses) is the essence of the Federation. In addition to the ASC, the Federation manages the transitive trust by providing:

- Policies and guidelines for federal authentication;
- Credential service assessments;
- Interoperability testing of candidate products, schemes or protocols; and
- Management and control of adopted Federation schemes operating within the environment

By supporting various identity schemes simultaneously, the ASC supports all four levels of assurance, as described in [OMB M-0404] and [NIST SP 800-63]. In addition, the ASC allows Federation members to rely on credentials issued by Federation partners even if partners deploy different authentication technologies (e.g., CSP implements PKI, RP implements SAML). All technical interoperation is precisely defined by Federation-scoped interface specifications.

The ASC does not rely on a national identifier card, unique national identifier number, or any single centralized registry of personal information, attributes, or authorization privileges.

The ASC focuses on authentication. It does not directly address authorization. In general, authentication precedes authorization.

The ASC resides in the FEA Service Component Model, providing security management services within the Support Services domain. The Federation aligns with the FEA Performance Reference Model through its mission of increasing the public trust, with the FEA Business Reference Model by supporting the delivery of services, and with the FEA Technical Reference Model by identifying technologies and standards relevant to E-Authentication.

2 TECHNICAL APPROACH

2.1 Architectural Framework

The ASC is a federated identity framework that allows the coexistence of multiple federated identity schemes within a single architecture. This provides a lasting architectural model not bound to a single industry standard, vendor, or product. This is in accordance with ASC design goals and the [NIST SP 800-63] directive that the technical approach be technology neutral, if possible.

The architectural framework includes a methodology and process for evaluating and adopting schemes over time. In general, the PMO adds or deletes identity schemes from the framework as necessary. Accordingly, the framework accommodates both forward and backward compatibility with multiple adopted schemes, yielding true interoperability. When necessary, the Federation adds intermediate components (scheme translators) to facilitate technical interoperation between disparate adopted schemes.

Per [Burton Group Report], this framework strategy is sound, since federated identity standards will change and converge over time.

The following sections describe the architectural framework in more detail. Figure 2-1 summarizes the framework in terms of current capabilities.

Figure 2-1 Current Identity Management Capabilities

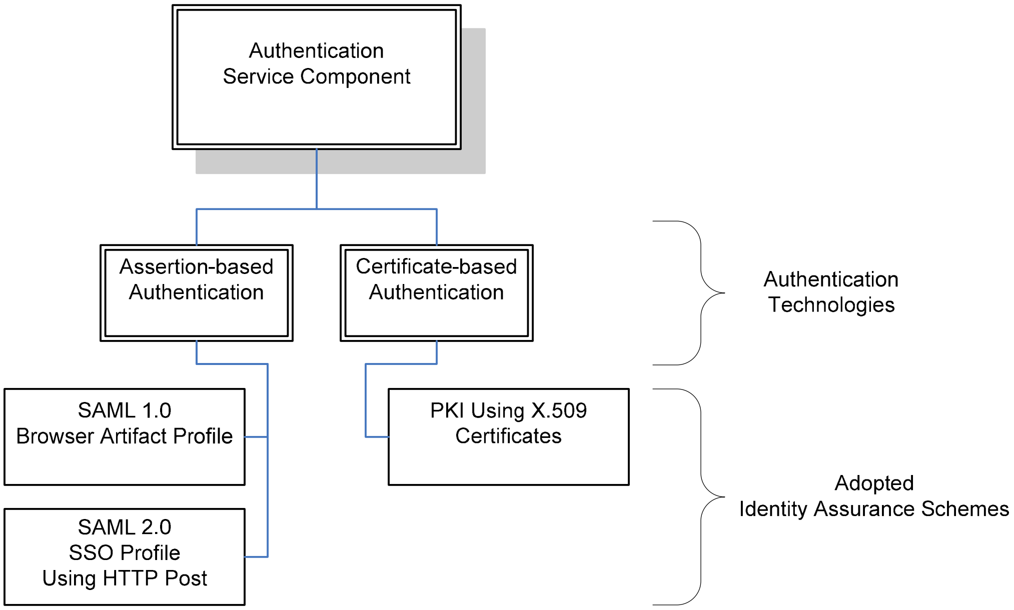

Authentication Service Component
Assertion-based Authentication
Certificate-based Authentication
Authentication Technologies
SAML 1.0 Browser Artifact Profile
SAML 2.0 SSO Profile Using HTTP Post
PKI Using X.509 Certificates
Adopted Identity Assurance Schemes

Figure 2-2 is a representative configuration showing co-existence of systems and adopted schemes within the ASC. The cloud represents the Federation wide area network linking the various systems. It includes two assertion-based adopted schemes (AS #1 and AS #2) and one certificate-based adopted scheme (AS #3). Note that some Federation member systems may be capable of supporting more than one adopted scheme concurrently – if the identity management COTS product used supports it. Federation-provided components are included as needed for each adopted scheme. For this representative configuration, that includes:

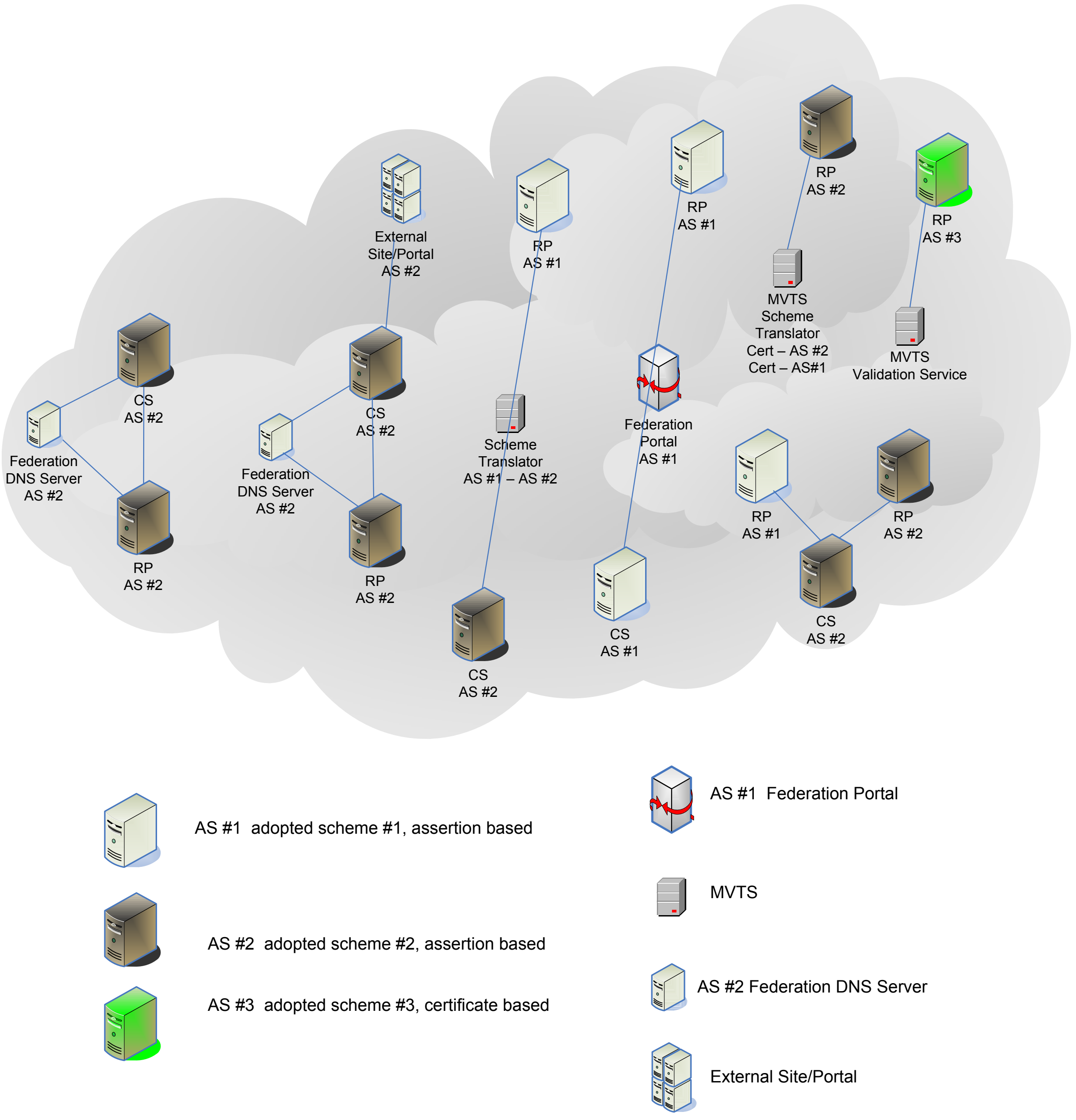
- The Federation Portal for adopted scheme #1;
- The Federation Domain Name Service (DNS) server for adopted scheme #2;
- A scheme translator for translation between the two assertion-based adopted schemes;
- The MVTS validation service for the certificate based adopted scheme; and
- The MVTS translation service to allow certificates to be used at the assertion-based adopted schemes

The ASC allows each adopted scheme to leverage external sites/portals (e.g., USA.gov or FORMS.gov) to provide end users with RP/CS discovery capability – redirecting the end user accordingly. This example shows that capability for adopted scheme #2.

Many other variations and relationships can exist within the ASC. To enhance basic understanding, and make relationships stand out, this example isolates (highlights) specific relationships and connections. A similar diagram for an operation environment would be more extensive, showing more systems and many arrows connecting those systems – especially true as the ASC scales up with more Federation member systems and adopted schemes.

The remainder of this document explains the ASC in general, and each system and adopted scheme specifically.

Figure 2-2 Sample ASC Configuration



2.2 Support for Multiple Authentication Technologies

Currently, the architectural framework accommodates assertion-based authentication, and certificate-based authentication within the same environment.

Assertion based authentication typically addresses lower levels of assurance (i.e., levels 1 and 2) where PINs and Passwords are used by end users. The end user authenticates to a selected CS, which in turn asserts the end user identity to the appropriate RP

Certificate based authentication typically addresses higher levels of assurance (i.e., levels 3 and 4) where X.509 digital certificates in a PKI infrastructure are used by end users. Certification Authorities issue X.509 certificates to end users. The end user presents their certificate to the RP (possibly to a scheme translator) for authentication. In general, the Federation leverages FPKI work, such that FPKI-compliant credentials can be used at the higher identity assurance levels.

The ASC allows for the introduction of other authentication technologies over time, such as knowledge-based authentication. Support for one-time passwords, certificate validation of digitally signed forms, and machine-to- machine communications such as web services may also be added. One of the Federation's strategic objectives is to support a variety of state-of-the-art technologies and methodologies.

In addition, the ASC allows RPs to rely on any authentication whose assurance level is greater than or equal to the assurance level required by the RP. In other words, higher-level credentials can be used at lower assurance level RPs – significantly enhancing credential re-use. For example, an assurance level 1 RP can rely on an assurance level 2 authentication. Another example is an assurance level 2 RP can rely on a level 4 authentication.

2.3 Support for Multiple Identity Assurance Schemes

An identity assurance scheme is a specific subset of an identity standard used (adopted) by the Federation. Any Federation member using the scheme must conform to the corresponding interface specification documented and published by the Federation. One or more adopted schemes can be defined from a single authentication technology. Currently, the Federation has approved integration of the following identity schemes into the ASC:

- PKI;
- SAML 1.0 Browser Artifact Profile (SAML 1.0 BAP); and
- SAML 2.0 SSO Profile using HTTP POST (SAML 2.0 SSO)

Within the ASC, SAML-based identity schemes are associated with authentication using PINs and passwords. PKI is associated with authentication using X.509 certificates. However, to support use of higher assurance level credentials by lower assurance level RPs, the ASC allows use of assertion-based mechanisms when X.509 certificates are used for authentication (see Section 2.4.2.1, Scheme Translators).

PKI is based on public key certificates and a verifiable association between a public key and the holder of the corresponding private key. SAML is an assertion-based identity standard for web single sign-on (SSO), web services authentication, and attribute exchange across domain boundaries (i.e., Federation member systems). The Federation may adopt other federated identity schemes, such as Shibboleth, over time.

2.4 ASC Entities

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.

2.4.1 Federation Member Systems

Approved Federation Member systems integrate into the ASC in accordance with applicable interface specifications, certification testing, and procedures. Once integrated into the ASC, Federation Member systems technically interoperate with compatible Federation Member systems and/or PMO-provided components as necessary to authenticate end users.

2.4.1.1 Relying Party[2]

A RP is an Internet based Federation member system that take an action based on identity information from a trusted Federation Member system. The Federation requires RPs to manage all business transactions and all end user authorization decisions, as those responsibilities are outside the scope of the ASC.

The Federation member (i.e., organization) that provides the Internet based service is also called a Relying Party. In this context, the RP Federation member can be a Federal department, agency, government sponsored corporation, or other instrumentality, or any state or local government.

2.4.1.2 Credential Service[3]

A CS is a Federation member system that creates, maintains, and manages identity information for end users, and may provide end user authentication services to RPs. In other words, a CS provides the Federation with identity management services.

The Federation member that provides the CS is a CSP. A CSP can be a commercial or government entity.

2.4.2 PMO-Provided Components

PMO-provided components are subsystems that support the design goals, high-level requirements, and operation of the Federation. They are deployed and withdrawn as necessary. They may be deployed for wide-spread use, or on a per adopted scheme basis (e.g., only relevant to one adopted scheme).

2.4.2.1 Scheme Translators

A scheme translator facilitates technical interoperability between CSs and RPs that use different adopted schemes (e.g., between a PKI CS and a SAML 1.0 Browser Artifact Profile RP). Scheme translators pass identity information based on standards already adopted in the architecture. The ASC allows deployment of schemes translators as necessary. This includes deploying multiple scheme translators concurrently. There is no need for any special integration of translators into CSs or RPs. A scheme translator appears to be any other CS from the RP perspective, and any other RP from the CS perspective. As long as the ASC has the applicable scheme translator(s), organizations that have invested in one of the adopted schemes will be able to use their existing systems with Federation member systems using other adopted schemes.

[2] The identity management industry also calls this a ‘Service Provider’
[3] The identity management industry calls this an ‘Identity Provider’

Some COTS products may directly support more than one adopted scheme. For example, some SAML COTS products support SAML 1.0 and SAML 2.0. In this situation, a scheme translator may not be required between different adopted schemes because the Federation member system can technically interoperate with more than one adopted scheme. In other words, some Federation member systems de facto support multiple adopted schemes by virtue of the COTS product.

2.4.2.2 Validation Service

The MVTS validation service provides TCP/IP interfaces that accept remote validation requests for X.509v3 PKI certificates, and processes a status response indicating whether the certificate is valid or not. A validation service is an end-to-end solution spanning server-side (i.e., the validation service provider's hosted service) and client-side (i.e., software integrated into the RP).

In general, the ASC can support various validation mechanisms (interfaces) as may be needed in the future. This includes, but is not limited to OCSP, SCVP, and XKMS.

2.4.2.3 Federation Portal

The Federation Portal is a website that helps end users locate the CSs and/or RPs they need to complete their transactions. If the end user explicitly makes one of those selections before accessing the Federation Portal (e.g., starting at the RP, starting at the CS), the architectural framework allows the Federation Portal to avoid redundant end user interaction. This capability reduces the required click count and generally simplifies the end user experience. The Federation Portal also facilitates SSO by optionally tracking all CSs selected by the end user during the browser session. In addition, the Federation Portal maintains information about CSs and RPs, referred to as metadata. The Federation Portal also generates Transaction Identifiers (TIDs) used to track transactions across various components in the architecture. When the end user opts into SSO, the Federation Portal assigns a Portal cookie.

The PMO has deployed the Federation Portal specifically for one adopted scheme – SAML 1.0 Browser Artifact Profile – mainly to address limitations of that SAML standard. Other currently adopted schemes do not require the Federation Portal (or any Portal at all) because of their use of SAML 2.0, which provides equivalent functionality.

2.4.2.4 Federation DNS Server

The Federation DNS server supports adopted schemes that use a common domain to share information. The DNS server maps human-readable domain names to IP addresses needed by Federation member systems.

2.4.3 External Sites/Portals

External sites are non-Federation sites. They provide limited Federation capability (e.g., RP/CS discovery) and do not undergo Federation conformance testing. Examples of external sites include, but are not limited to government portals (e.g., USA.gov, FORMS.gov). In addition, a Federal agency, whether a Federation member or not, can provide an agency portal highlighting all of its online applications available through the Federation.

The ASC allows adopted schemes to integrate external sites into the end user flow, if for no other reason, to provide additional web sites for the end user to discover CSs and/or RPs. The external site, having necessary non-sensitive metadata from the Federation, redirects the end user per their selection, as appropriate for the adopted scheme. Each adopted scheme defines the scope and extent of external site functionality and processing. External sites can be used in conjunction with the Federation Portal.

2.4.4 Principals

A principal is any ASC entity that authenticates its identity via the ASC. The following sections discuss the principles currently supported by the ASC.

2.4.4.1 End Users

An end user is any citizen, government employee, contractor, or business that authenticates to a Federation RP using a credential issued by a Federation CS.

2.5 Session Types

The ASC supports three session types, as defined in the following sections.

2.5.1 Browser Session

The browser session is the period of time the end user's web browser (e.g., Internet Explorer) is open. The browser session begins when the end user opens the browser and ends when it is closed. When the browser session ends, all session cookies are terminated for privacy purposes. Any browser with TLS and session cookie support can be used with the ASC, although individual RPs and CSs may have additional requirements.

2.5.2 Authentication Session

The authentication session is the 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 SSO is in effect.

2.5.3 RP Session

The RP session is the period of time an RP will trust an end user before handing the end user off to the CS for re-authentication. RPs do not have access to authentication session information, so they must maintain their own session with an end user and decide how long an end user remains trusted once starting transaction processing at the RP. If an RP returns an end user to the CS for re-authentication, the CS re-authenticates the end user – even if the authentication session has not yet expired.

2.6 Use of Cookies

An integral part of the ASC is cookies. The ASC uses cookies to facilitate SSO and to manage sessions (e.g., RP session, authentication session). In addition, the ASC only uses transient cookies per [OMB M-03-22]. Transient cookies 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.

The following sections describe the various cookies used in the ASC. Each adopted scheme uses a different set of cookies.

2.6.1.1 CS Cookie

Once a CS authenticates an end user, the CS assigns a CS cookie to the end user. The CS cookie facilitates SSO. The contents and sensitivity of the CS cookie may vary among CSs. SAML 1.0 BAP and SAML 2.0 SSO use the CS cookie.

2.6.1.2 RP Cookie

An RP may assign an end user an RP cookie to help track the RP session, or other application session information. SAML 1.0 BAP and SAML 2.0 SSO use the RP cookie.

2.6.1.3 Portal Cookie

The Federation Portal uses the Portal cookie to track the CS selected by the end user in the current browser session. The combination of the Portal cookie and the CS cookie is used only in one adopted scheme (SAML 1.0 Browser Artifact profile) as the mechanism for SSO. This approach addressed limitations in the early version of the SAML standard. SAML 1.0 BAP uses the Portal cookie.

2.6.1.4 Common Domain Cookie

The common domain cookie (CDC) tracks the CSs to which the end user has authenticated during a particular session. CSs read and update the CDC. RPs read the CDC. In addition, the CDC is used only in adopted schemes using SAML 2.0 (SAML 2.0 Web SSO Profile Using HTTP POST).

2.6.1.5 Implementation-specific Cookies

Within each adopted scheme, ASC entities may implement additional cookies as necessary to facilitate processing. For example, a CS may implement an additional cookie to track RPs associated with a particular authentication session. This would be useful for single logout processing, which is a feature of SAML 2.0 Web SSO Profile Using HTTP POST. SAML 1.0 BAP and SAML 2.0 SSO may use implementation-specific cookies.

2.7 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 ASC supports activation, but is not responsible for activation. An adopted scheme may offer activation approaches not available in other adopted schemes. The RP determines the need for activation, and facilitates it when necessary. See [User Activation] for more complete details.

2.8 Governance

The ASC currently provides two 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. ASC governance mechanisms include (a) issuance of certificates by the E-Governance Certification Authorities (E-GCA), and (b) metadata management by the PMO. Governance is dependent upon the adopted scheme. Therefore, the specific details of governance may differ from one adopted scheme to another.

2.8.1 E-GCA Certificates

The government issues E-GCA certificates to approved Federation members. In addition, the E-GCA issues only those certificate types applicable to the adopted scheme. The government issues E-GCA certificates as follows:

- For SAML 1.0 Browser Artifact Profile as an Adopted Scheme:
  - Mutual TLS authentication between the RP and the CS;
- For SAML 2.0 SSO Profile Using HTTP POST as an Adopted Scheme:
  - Digitally signing/verifying SAML messages; and

- Digitally encrypting/decrypting any SAML message containing PII (e.g., SAML Assertion)

2.8.2 Metadata

The government validates and distributes metadata information only to PMO-approved ASC entities. Metadata is information necessary for ASC entities (e.g., RPs, CSs) to technically interoperate. Metadata is dependent upon the adopted scheme. Therefore, metadata information and the method for sharing metadata information may differ from one adopted scheme to another. In general, metadata information typically encompasses (a) Federation specific information, and (b) scheme specific information. Failure to configure metadata completely and correctly can preclude technical interoperation, or result in unexpected consequences or negative impacts to any number of operational nodes. Metadata does not contain confidential information.

2.9 Implementation

The architectural framework presented herein does not prescribe the specific standards currently employed by each adopted scheme. Rather, each adopted scheme addresses specific standards relevant to it. Towards this, an interface specification accompanies each adopted scheme. The interface specification provides detailed technical specifications for use of the adopted scheme within the architectural framework. In addition, each adopted scheme includes an overview document that provides high-level descriptions and context.

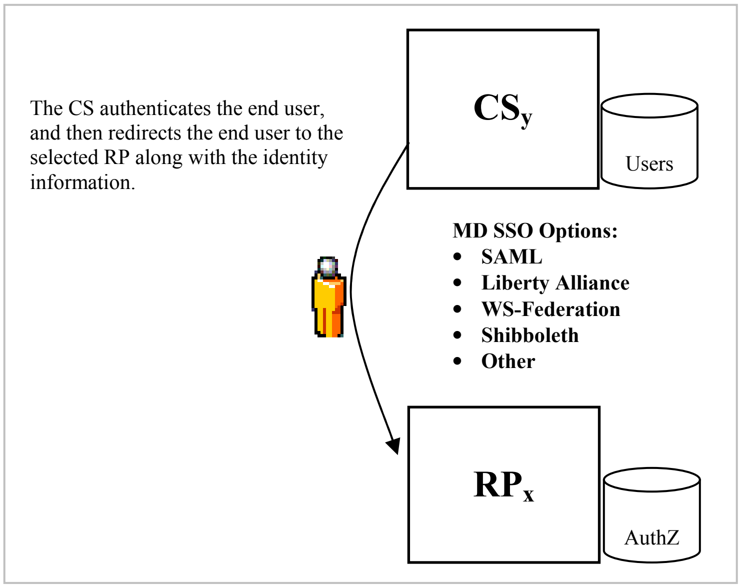
Federation members must select one (or more) of the adopted schemes to technically interoperate with partners within the ASC. For each adopted scheme, the PMO provides a list of approved COTS products. Approval indicates that the COTS product has proven technical interoperability as required by the applicable interface specification. There are additional agreements with which Federation members must comply. Those agreements are out of scope for this document, but interested parties should contact the PMO for more information.

3 ASSERTION-BASED AUTHENTICATION USE CASES

Within the architectural framework, the end user interacts directly with RPs, CSs, and, depending upon the adopted scheme, possibly a Portal or external site. The end user may interact with a CS, Portal, or external site to locate a desired CS and/or RP. The end user interacts with the CS to obtain, manage, and validate credentials. The CS passes an identity assertion and associated identity information about the end user to the RP. Once the RP has the assertion and identity information, the RP can decide to allow the end user to conduct business transactions. The RP initiates end user activation as necessary, and may initiate SSO with a CS. The RP is solely responsible for end user authorization.

The redirect from the CS to the RP is a classic case of Multi-Domain Single Sign-On (MD SSO) – an end user authenticated in one domain (the CS) becomes known to another domain (the RP) without re-authenticating. This redirect from CS to RP is a primary point in the architecture where assertion-based adopted schemes are used. Figure 3-1 highlights the industry standard options for MD SSO.

Figure 3-1 MD SSO Industry Standard Options


The CS authenticates the end user, and then redirects the end user to the selected RP along with the identity information.
CS_y
Users
MD SSO Options:
• SAML
• Liberty Alliance
• WS-Federation
• Shibboleth
• Other
RP_x
AuthZ

Once a CS authenticates an end user on behalf of an RP, subsequent visits to other compatible RPs during the same browser session do not require re-authentication, unless the authentication session has expired. The CS simply redirects the end user to each subsequent compatible RP without end user interaction at the CS.

Currently SAML, Liberty Alliance, Shibboleth, and WS-Federation all provide mechanisms for MD SSO. The Federation can use any of these schemes to meet its assertion-based requirements. It is unclear which of these schemes will become dominant in the market, and it is quite possible that more than one will be in common use. In addition, other standards based mechanisms are likely to become available and existing schemes are likely to evolve.

Since the CS is directly involved in SSO, it can intervene if the end user has opted out of SSO, or if CS privacy policy prevents it – by always presenting the end user with a list of compatible RPs and requiring the end user to make a selection from the list. SSO is one of several end user preferences. The CS manages end user preferences and other identity management. There is no need for a government-wide repository of these preferences.

Each adopted scheme manages SSO via the use of cookies. The specifics are dependent upon the adopted scheme.

The ASC allows end users to be redirected from one ASC entity to another, as necessary, and as applicable for the adopted scheme. Some redirects may be transparent to the end user (e.g., to support seamless SSO). In this case, the end user neither sees nor interacts with the ASC entity to which it is redirected – the end user simply "passes through". Other redirects are noticeable to the end user, as a new web site/page appears, and interaction is required (e.g., redirect to a CS, and then authenticate to the CS).

The ASC allows end users to start at various points in the architecture – for ease of use and convenience. For example, but dependent upon the adopted scheme, an end user can start at a CS, at an RP, at the Federation Portal, or at an external site/portal.

The ASC allows external sites to have Federation metadata and to provide end users with a CS/RP discovery service. Upon end user selection, the external site redirects the end user as appropriate for the adopted scheme.

The following sub-sections describe how each assertion-based scheme currently adopted by the Federation addresses MD SSO.

3.1 SAML 1.0 Browser Artifact Profile Adopted Scheme

This was the first scheme adopted by the Federation. At adoption, the Federation used “Agency Application (AA)” instead of the current term “Relying Party (RP)”. This section continues uses AA because it is fundamental to the adopted scheme (e.g., AAid).

In this adopted scheme, the Federation Portal is integral to authentication processing flow and facilitating essential functionality (e.g., SSO, transaction tracking). Federation member systems must redirect unauthenticated end users to the Federation Portal when attempting to access a protected resource. Not all end users start at the Federation Portal. Therefore, this adopted scheme allows end users to start at a number of places (e.g., AA, CS, Federation Portal), depending upon which is most convenient to the end user.

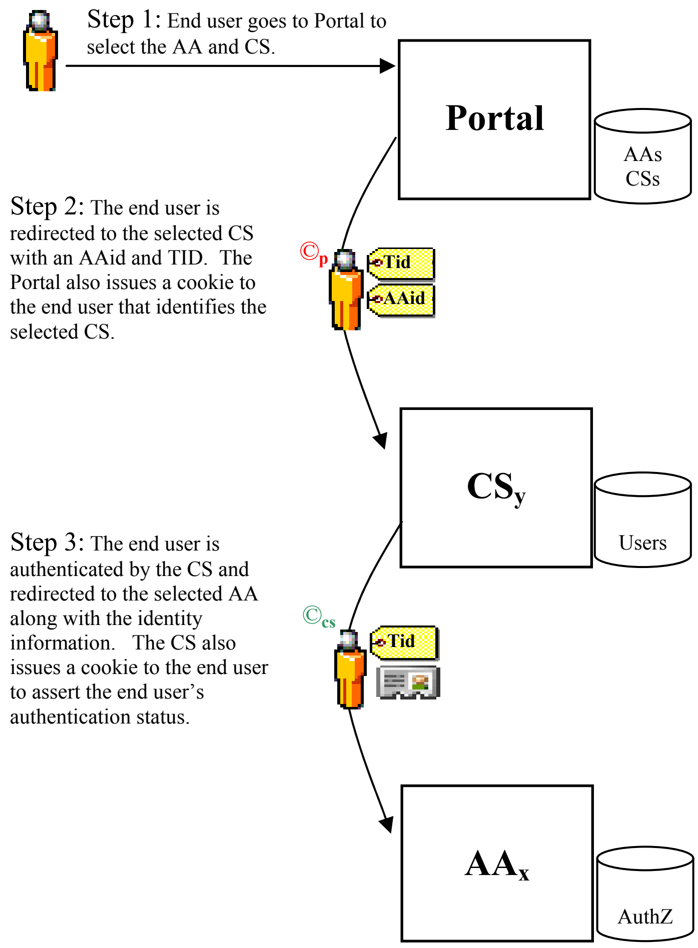
The PMO is planning to phase out this adopted scheme some time in 2007 in favor of a SAML 2.0 based adopted scheme (see Section 3.2). A migration plan will guide Federation members and COTS vendors through the transition.

3.1.1 Starting at the Federation Portal

Figure 3-2 depicts the sequence of events for starting at the Federation Portal. In Step 1, the end user goes to the Federation Portal and selects an AA. The Federation Portal then presents the end user with a list of CSs with appropriate assurance levels (equal to or higher). The end user selects a CS. In step 2, the Federation Portal redirects the end user to the CS with the identifier for the selected AA (AAid) and a Federation Portal generated TID. As part of this redirect, the Federation Portal gives the end user a session cookie (Portal cookie) that contains the CS the end user selected. The Portal cookie remains operational for the duration of the browser session. This cookie enables SSO in later transactions[4]. The end user then authenticates to the CS directly, and the CS assigns a session cookie (CS cookie) to manage the authentication session. In Step 3, the CS redirects the authenticated end user to the AA along with TID and the identity information, allowing the AA to manage transactions and authorization. Typically, the AA assigns a cookie to manage the agency session.

Since the redirect to the AA includes end user identity, some PII is included. The CS may adjust the PII made available to a given AA based on the end user's preferences, their privacy policies, or by prompting the end user before the redirect. The interface specification for this adopted scheme specifies the minimum set of identity attributes required for all redirects.

Figure 3-2: Starting at the Federation Portal



Step 1: End user goes to Portal to select the AA and CS.

Step 2: The end user is redirected to the selected CS with an AAid and TID. The Portal also issues a cookie to the end user that identifies the selected CS.

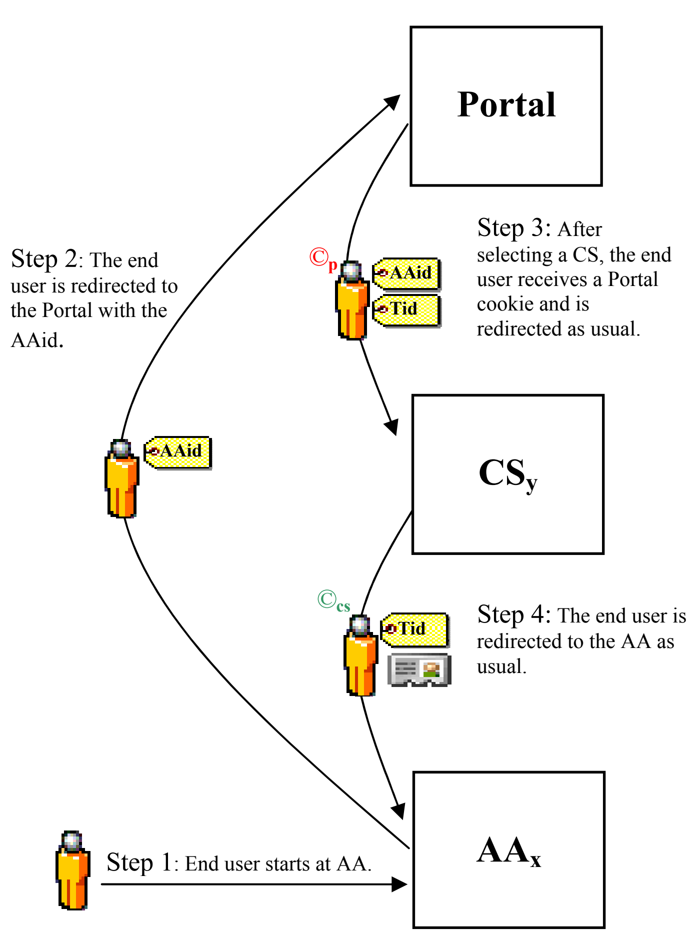
Step 3: The end user is authenticated by the CS and redirected to the selected AA along with the identity information. The CS also issues a cookie to the end user to assert the end user's authentication status.

[4] This, and subsequent use case references to single sign-on, presumes the end user has opted in to single sign-on. See section 1.4.2 for details.

3.1.2 Starting at the Agency Application

Figure 3-3 depicts the sequence of events for end users that start at the AA. Step 1 shows the end user starting at the AA. Since the AA has no indication that the end user is authenticated, the AA redirects the end user to the Federation Portal. The redirect includes the AA's unique AAid, as shown in Step 2. The Federation Portal does not have to ask the end user to select an AA – The Federation Portal knows it from the AAid. The Federation Portal checks for a Portal cookie. If present, the Portal cookie specifies CS selected during the same browser session. If any CS is compatible to the AA, the Federation Portal immediately redirects the end user to that compatible CS without any end user interaction at the Federation Portal. If none of the CSs in the Portal cookie is compatible, or no Portal cookie is present, the Federation Portal displays a list of compatible CSs from which the end user selects. The Federation Portal redirects the end user to the selected CS, as shown in Step 3.

Figure 3-3: End user Starts at AA


Portal
Step 3: After selecting a CS, the end user receives a Portal cookie and is redirected as usual.
©p
AAid
Tid
Step 2: The end user is redirected to the Portal with the AAid.
AAid
CSy
©cs
Tid
Step 4: The end user is redirected to the AA as usual.
AAx
Step 1: End user starts at AA.

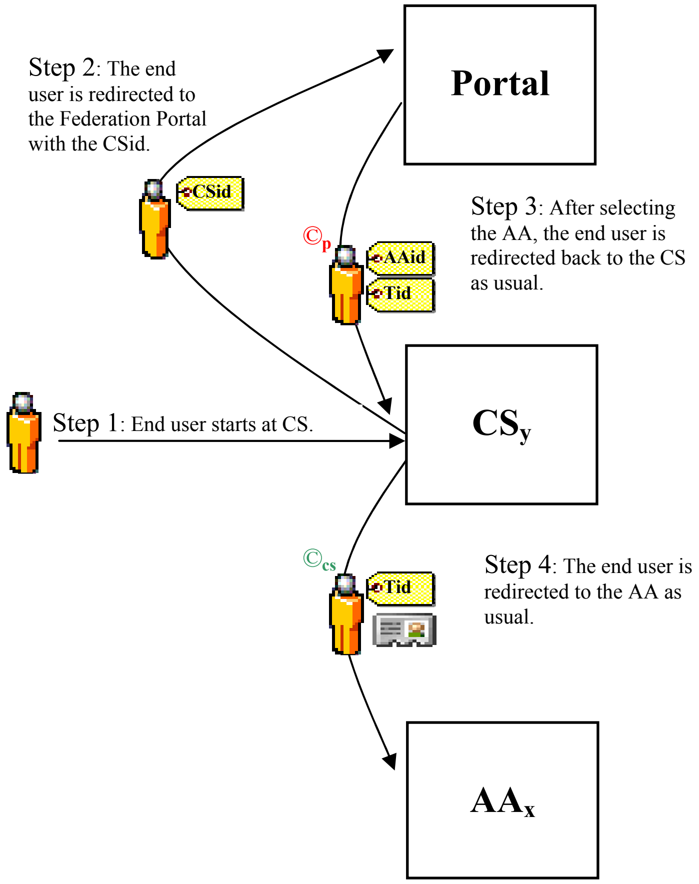
The CS checks for a CS cookie to determine if the end user has already authenticated to it. If not yet authenticated (no CS cookie), or an established authentication session has expired, the end user authenticates to the CS. Otherwise, no authentication is required (i.e., no end user interaction with the CS is required, thus facilitating SSO). The CS redirects the end user to the originating AA. The combination of Portal cookie and CS cookie is the mechanism for seamless, transparent SSO in this adopted scheme. The Portal cookie allows the Federation Portal to redirect the end user to the CS without end user interaction at the Federation Portal. The CS cookie allows the CS to redirect the end user to the AA without interaction at the CS.

3.1.3 Starting at the Credential Service

In some cases, the end user may begin a session at the CS. For example, a bank Federation member may provide a link to the Federation Portal and inform the end user that the credential may be used to conduct government business. The end user, already authenticated to the bank and conducting business, may select the link and begin a session. Figure 3-4 depicts the sequence of events for this case.

The end user starts at the CS and selects a link to the Federation Portal that includes a CS identifier (CSid), as shown in Step 1. In Step 2, the CS redirects the end user to the Federation Portal. The Federation Portal presents the end a list a list of AAs compatible with the CS, as well as some indication that other applications may be available for higher-level credentials. The end user selects an AA, whereupon the Federation Portal redirects the end user to the originating CS with the AAid and TID, as shown in Step 3. In step 4, the CS redirects the end user to the AA as usual. If the end user has already authenticated to the CS, the CS immediately redirects the end user to the AA (i.e., without interaction at the CS).

Figure 3-4: User Starts at CS


Step 2: The end user is redirected to the Federation Portal with the CSid.
CSid
Portal
©p
AAid
Tid
Step 3: After selecting the AA, the end user is redirected back to the CS as usual.
Step 1: End user starts at CS.
CS$_y$
©cs
Tid
Step 4: The end user is redirected to the AA as usual.
AA$_x$

This use case demonstrates how CSs can advertise the utility of their credential, increasing the value proposition for CSPs. It also opens up every CS as a channel to advertise the availability of various AAs. The use case further illustrates the flexibility of the Federation Portal. In addition to supporting SSO, the principal function of the Federation Portal is to help the end user select the CS and/or AA. If the end user explicitly makes one of those selections before accessing the Federation Portal, the architectural framework allows the Portal to avoid redundant end user interaction. This capability reduces the required click count and generally simplifies the end user experience.

3.1.4 Distributed Federation Portal Functionality

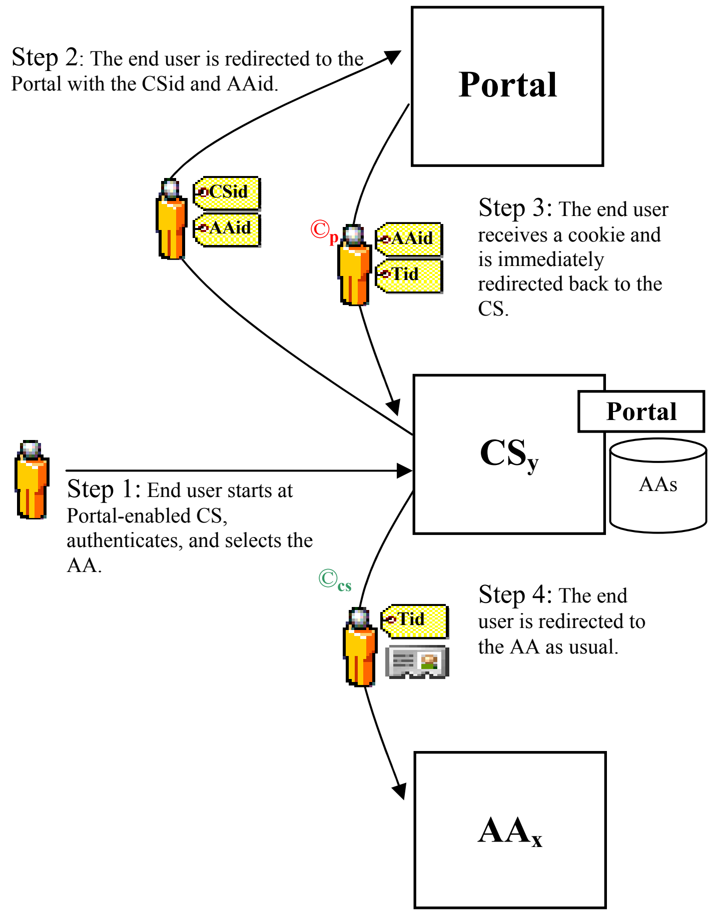
The PMO can share AA and CS metadata stored at the Federation Portal with other applicable ASC entities. There is nothing sensitive about the information and no reason to keep it isolated at the Federation Portal. Other sites equipped with the information could assist end users during the selection of an AA or CS. The Federation Portal's ability to process passed AAids and CSids enables other sites to add value without requiring redundant interaction with end users.

One example is for a CS to present the end user with compatible AAs that will accept their credentials. CSs, such as banks, may be able to add value by suggesting AAs that are relevant to a particular end user or related to the business the end user is engaged in during a particular browser session. A CS configured with metadata about AAs is Portal-enabled if it has the ability to present the end user with compatible AAs, and can redirect the end user through the Federation Portal to the AA. The following sections describe use cases where other sites have been Portal-enabled.

3.1.4.1 Federation Portal Functions at the Credential Service

It is possible for a CS to provide some Federation Portal functions in this architectural framework. Figure 3-5 shows the sequence of events for this case. In Step 1, the end user starts at the CS, perhaps conducting routine business. The CS has integrated AA metadata and presents the end user with a list of compatible AAs that can be accessed with their credential. When the end user selects an AA, the CS redirects the end user to the Federation Portal with the AAid and the CSid, as shown in Step 2. Since the end user arrives at the Federation Portal with both AAid and CSid, there is no need for the Federation Portal to interact with the end user. The end user simply receives a Portal cookie and the Federation Portal redirects the end user back to the CS, as shown in Step 3. In Step 4, the CS has already authenticated the end user, so it immediately redirects the end user to the AA as described in “starting at the Federation Portal”.

Figure 3-5: User Starts at Portal-enabled CS


Step 2: The end user is redirected to the Portal with the CSid and AAid.
Portal
CSid
AAid
©P
AAid
Tid
Step 3: The end user receives a cookie and is immediately redirected back to the CS.
CS_y
Portal
AAs
Step 1: End user starts at Portal-enabled CS, authenticates, and selects the AA.
©cs
Tid
Step 4: The end user is redirected to the AA as usual.
AA_x

While it would be possible for the CS to initiate the redirect to the AA directly, the CS must redirect the end user to the Federation Portal for SSO to work properly because SSO requires both the Portal cookie and the CS cookie. If the CS redirected the end user directly to the AA, the end user would not be automatically authenticated on subsequent visits to other AAs. Therefore, the CS must redirect the end user through the Federation Portal even when the end user will not interact with the Federation Portal.

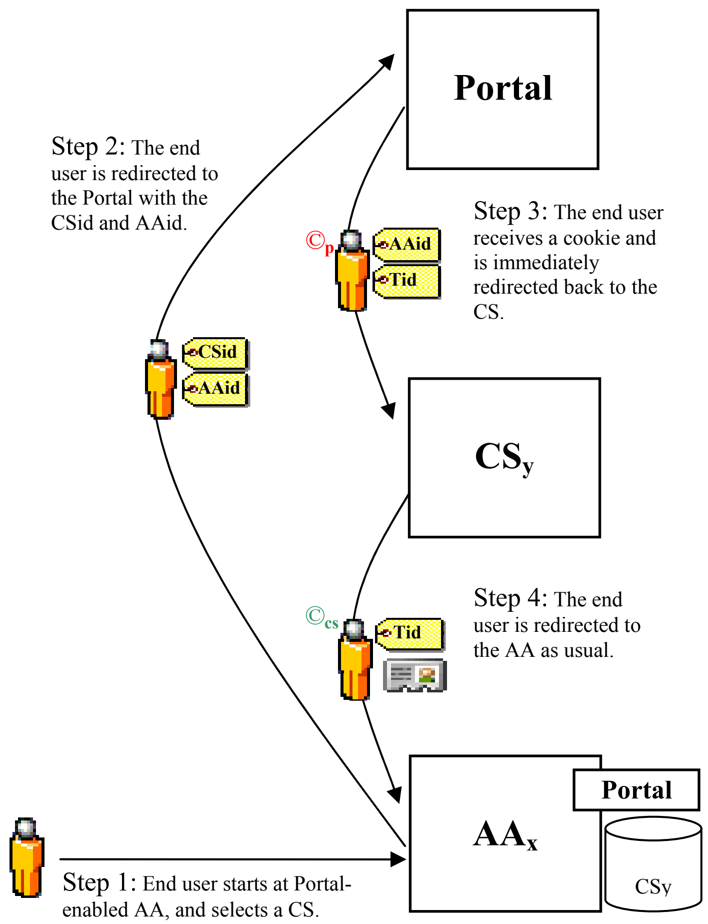
Explicit support for this scenario in the architecture encourages CSPs to advertise the availability of government applications. It also provides an easy mechanism for CSs to show the value of their credential to their end user base. The end user benefits from easier availability and access to government applications.

3.1.4.2 Federation Portal Functions at the AA

It is also possible for an AA to provide some Federation Portal functionality. If an AA loads the metadata for CSs, it could provide end users with a list of compatible CSs.

Figure 3-6 shows the sequence of events for the Portal-enabled AA case. In Step 1, the end user starts at the AA, which has integrated the metadata for CSs. The AA presents the end user with a list of compatible CSs. After the end user selects a CS, the AA redirects the end user to the Federation Portal with the AAid and CSid, as shown in Step 2. Once again, because there is no interaction with the Federation Portal, the end user simply receives a Portal cookie and is redirected to the CS, as shown in Step 3. Finally, the CS authenticates the end user and redirects the end user back to the AA, as described in Step 4.

Figure 3-6: User Starts at Portal-enabled AA


Portal
Step 2: The end user is redirected to the Portal with the CSid and AAid.
©p
AAid
Tid
Step 3: The end user receives a cookie and is immediately redirected back to the CS.
CSid
AAid
CS_y
©cs
Tid
Step 4: The end user is redirected to the AA as usual.
Portal
AA_x
CSy
Step 1: End user starts at Portal-enabled AA, and selects a CS.

Not Recommended

The PMO does not recommend this scenario because it can interfere with SSO. If the end user had already authenticated to a different AA earlier in the browser session and then accessed the Portal-enabled application, the end user would have to select the CS a second time at the Portal-enabled AA. If the AA simply redirected the end user to the Federation Portal as described in figure 3-2, the end user would not be required to make the selection a second time. This scenario is presented because it may provide utility to some agencies in certain circumstances, and requires no additional functionality in other architectural components.

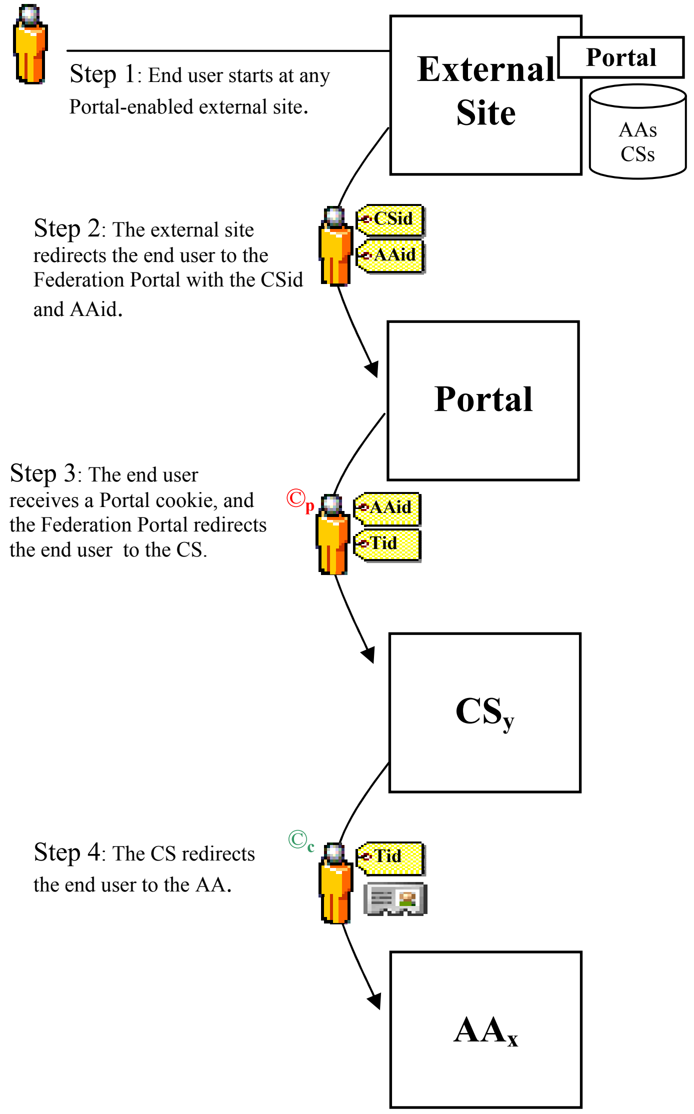
If this were the end user's first authentication, then subsequent access to other AAs would provide SSO.

3.1.4.3 Starting at an External Site

The ability of the Federation Portal to accept incoming AAids and CSids supports various scenarios that allow for flexibility in the end user experience. For example, it would also be possible for a government portal (e.g., USA.gov, FORMS.gov) to load Federation metadata and provide Federation Portal functionality, simply redirecting the end user to the Federation Portal once the end user selected a CS and AA. Agency websites could offer similar functionality, highlighting the applications provided by the agency. These scenarios, and others, are possible and ultimately benefit the end user and the government by increasing the exposure of E-Government applications.

Figure 3-7 depicts the sequence of events for these scenarios. In Step 1, the end user starts at any external site that has integrated Federation metadata. The end user selects a CS and AA. In Step 2, the external site redirects the end user to the Federation Portal with the CSid and AAid as described in the previous use cases. The Federation Portal gives the end user a Portal cookie, and then immediately redirects the end user to the CS without any end user interaction at the Federation Portal, as shown in Step 3. The sequence continues as described in "starting at the Federation Portal", where the end user authenticates to the CS, and then the CS redirects the end user to the AA, as shown in Step 4.

Figure 3-7: User Starts at External Site


Step 1: End user starts at any Portal-enabled external site.
External Site
Portal
AAs
CSs
Step 2: The external site redirects the end user to the Federation Portal with the CSid and AAid.
CSid
AAid
Portal
Step 3: The end user receives a Portal cookie, and the Federation Portal redirects the end user to the CS.
©p
AAid
Tid
CS$_y$
Step 4: The CS redirects the end user to the AA.
©c
Tid
AA$_x$

3.2 SAML 2.0 SSO Profile Using HTTP POST Adopted Scheme

This adopted scheme does not make use of the Federation Portal. RPs and CSPs now provide this functionality due to new features in SAML 2.0. Affected functionality includes key features such as SSO, RP/CS discovery, and transaction tracking. Eliminating the Federation Portal streamlines processing flow, and reduces process complexity and operational burden.

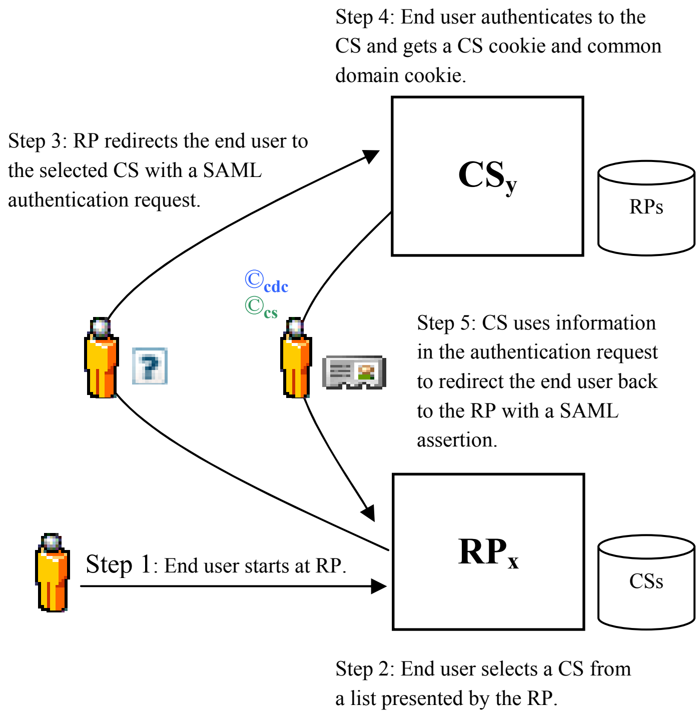
SAML 2.0 facilitates SSO via a common domain and a common domain cookie, which replaces the Portal cookie. RPs and CSs use the Federation common domain to share access to an end user's common domain cookie, which lists CSs the end user has authenticated to during the current browser session. The combination of common domain cookie and CS cookie is the mechanism for SSO in this adopted scheme.

This adopted scheme allows end users to start at a number of places (e.g., RP, CS, external site), depending upon which is most convenient to the end user.

3.2.1 *Starting at the Relying Party*

Figure 3-8 depicts the sequence of events for end users that start at the RP. Step 1 shows the end user starting at the RP. In Step 2, the RP checks the end user's common domain cookie and determines that the end user has not authenticated to a compatible CS. Accordingly, the RP presents the end user with a list of compatible CSs. The end user makes a selection. In Step 3, the RP redirects the end user to the selected CS with an authentication request. In Step 4, the end user authenticates to the CS. The CS gives the end user a CS cookie, and updates the end user's common domain cookie to add itself to the list of CSs that have authenticated the end user during this browser session. Finally, in Step 5, the CS uses information in the authentication request to identify the originating RP, and redirects the end user back with a digitally encrypted and digitally signed assertion.

Figure 3-8: End user Starts at RP

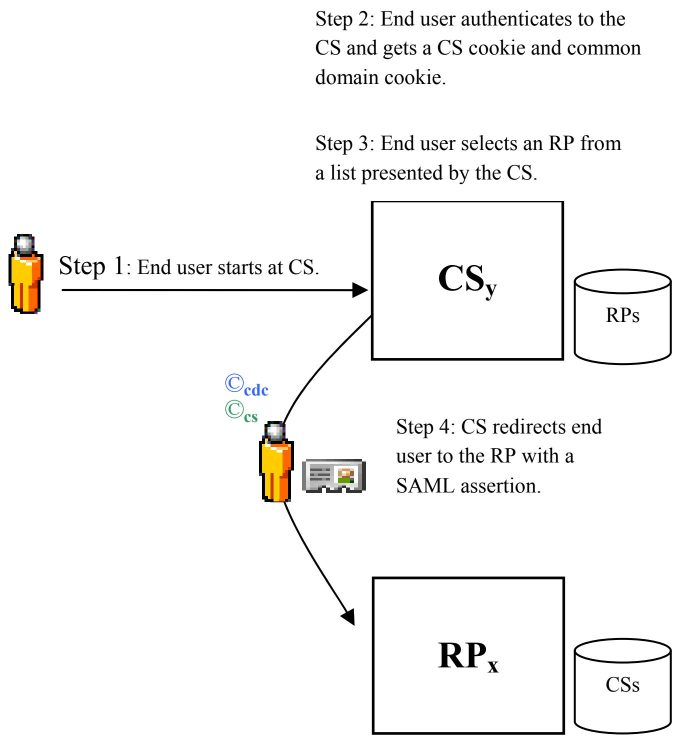

Step 4: End user authenticates to the CS and gets a CS cookie and common domain cookie.
CSy
RPs
Step 3: RP redirects the end user to the selected CS with a SAML authentication request.
©cdc
©cs
Step 5: CS uses information in the authentication request to redirect the end user back to the RP with a SAML assertion.
RPx
CSs
Step 1: End user starts at RP.
Step 2: End user selects a CS from a list presented by the RP.

If in Step 2 the RP determines that the end user has authenticated to a compatible CS, the RP may not present a CS list. Instead, the RP could immediately redirect the end user to the compatible CS for SSO processing.

3.2.2 *Starting at the Credential Service*

Figure 3-9 depicts the sequence of events for end users that start at the CS. Step 1 shows the end user starting at the CS. In Step 2, the end user authenticates to the CS. The CS gives the end user a CS cookie, and updates the end user's common domain cookie to add itself to the list of CSs that have authenticated the end user during this browser session. Since the end user arrived without an authentication request, the CS knows that the end user has not yet selected an RP. Accordingly, the CS presents the end user with a list of compatible RPs, as shown in Step 3. The end user makes a selection. Finally, in Step 4, the CS redirects the end user to the selected RP with a digitally encrypted and signed assertion.

Figure 3-9: End user Starts at CS


Step 2: End user authenticates to the CS and gets a CS cookie and common domain cookie.
Step 3: End user selects an RP from a list presented by the CS.
Step 1: End user starts at CS.
CSy
RPs
©cdc
©cs
Step 4: CS redirects end user to the RP with a SAML assertion.
RPx
CSs

If in Step 2 the CS determines the end user is already authenticated to it, and the authentication session has not expired, no authentication is required (i.e., SSO is in effect).

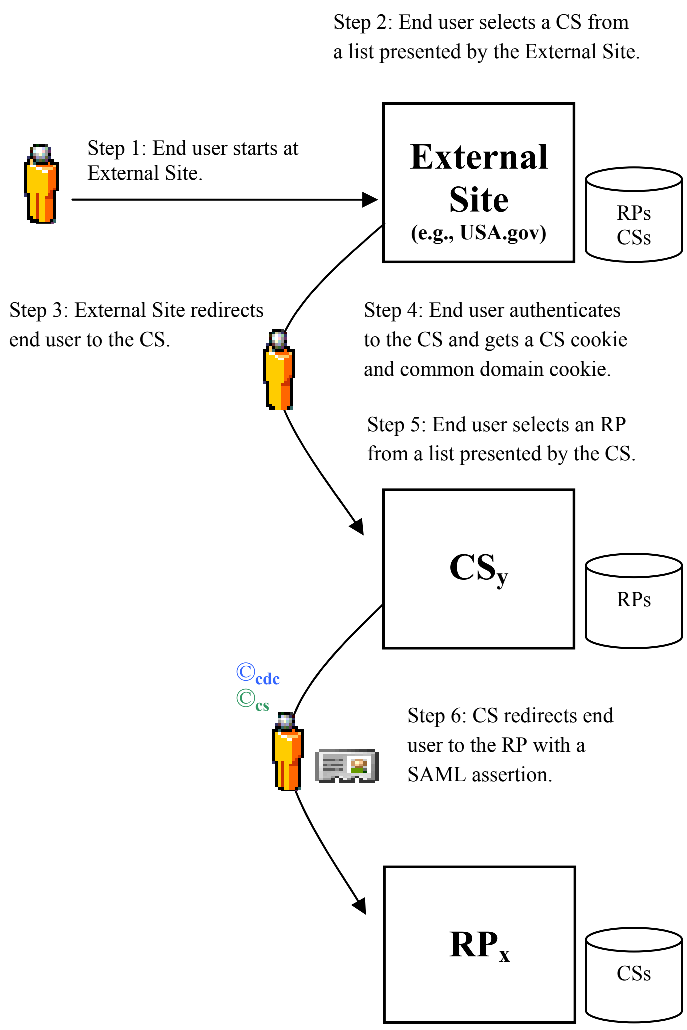
If in Step 3 the CS determines the end user has selected an RP (i.e., an authentication request accompanies the end user), then processing occurs per the "starting at the RP" use case.

3.2.3 *Starting at an External Site*

Figure 3-10 depicts the sequence of events for end users that start at an external site such as an agency portal or government-wide portal (e.g. USA.gov, FORMS.gov). Step 1 shows the end user starting at the external site. In this adopted scheme, external sites allow end users to discover and select an RP or a CS – but not both. This limitation precludes the need for external sites to implement SAML. In this use case, the end user selects a CS, as shown is Step 2. In Step 3, the external site redirects the end user to the selected CS. From this point forward, processing continues per the "starting at the CS" use case. The external site simply provided an additional, convenient discovery service to the end user.

If in Step 2 the end user discovers and selects an RP, the external site redirects the end user to the selected RP, and processing continues per the "starting at the RP" use case.

Figure 3-10: End user Starts at External Site


Step 2: End user selects a CS from a list presented by the External Site.
Step 1: End user starts at External Site.
External Site (e.g., USA.gov)
RPs CSs
Step 3: External Site redirects end user to the CS.
Step 4: End user authenticates to the CS and gets a CS cookie and common domain cookie.
Step 5: End user selects an RP from a list presented by the CS.
CS$_y$
RPs
©cdc
©cs
Step 6: CS redirects end user to the RP with a SAML assertion.
RP$_x$
CSs

4 Certificate-Based Authentication Use Cases

PKI based credentials offer considerable advantages for authentication. They are capable of certificate-based authentication transactions and can be validated using only public information. The standards for PKI are also more mature and more widely used than the emerging standards for federated PIN/Password based electronic authentication.

The FPKI works to ensure CAs implement similar policies and procedures that allow relying parties to trust credentials at certain levels of assurance. The Federation has deferred assessment and governance of PKI based CSs to the FPKI PA, the governing body for the FBCA. Additional information on the FPKI is available at http://www.cio.gov/fpkipa.

The ASC approach for accepting PKI based credentials is providing mechanisms for RPs to validate certificates. That is, a certificate-based RP authenticates the end user, rather than having a CS authenticate the end user on behalf of the RP. In this context, the RP acts as both a CS and an RP.

End users can start directly at the desired RP, or another ASC entity that provides RP discovery service can redirect the end user to the RP.

The following sections describe the various use cases for certificate validation services.

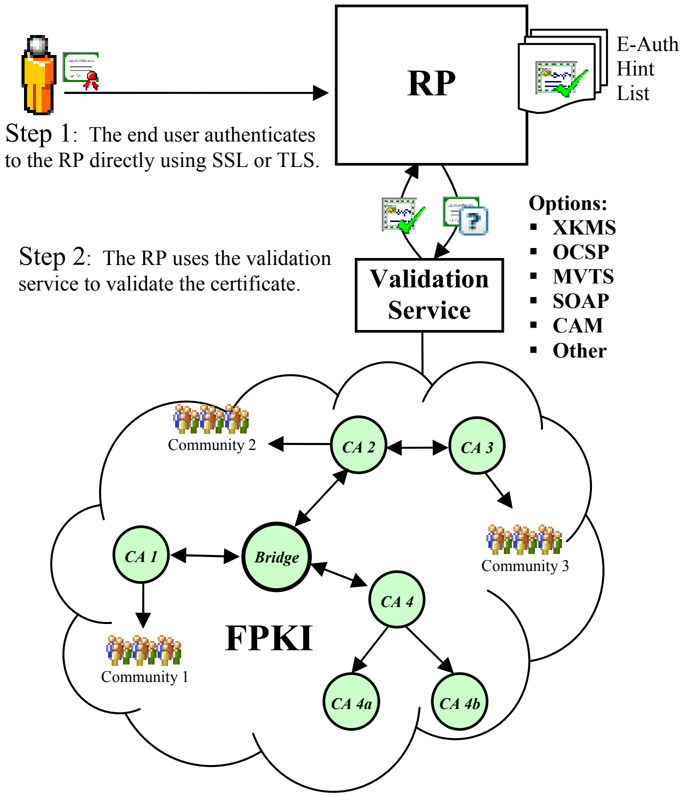
4.1 Certificate Validation Service

The Federation offers the MVTS certificate validation service to RPs (see Section 2.4.2.2). Figure 4-1 depicts the use of the certificate validation service for authentication. In Step 1, the end user arrives at the RP either directly or via redirect from an ASC entity providing RP/CS discovery service.

There is no need for the RP to redirect the end user to a CS. That is because TLS and Secure Socket Layer (SSL) allow the end user to authenticate directly to the RP using a certificate without revealing any secret information. The RP authenticates the end user, then delegates validation of the certificate to the validation service in Step 2.

To the greatest extent possible, the validation service is comprised of COTS products using standard protocols. NIST has established requirements for certificate path validation, initially using the Federation Interoperability Lab to determine appropriate products and interface specifications.

Figure 4-1: Certificate Validation Service



Over time, the validation service may support multiple products and standards, but the functionality will remain the same. The ASC architectural framework leaves room for appropriate standards to be adopted as they mature.

The TLS/SSL protocol requires the web server to present a list of acceptable CAs to the browser during the TLS/SSL handshake in Step 1. The PMO publishes a hint list of CAs available for use by RPs. The Federation hint list helps end users select an appropriate certificate. The hint list is not used for any other purpose, including certificate validation[5].

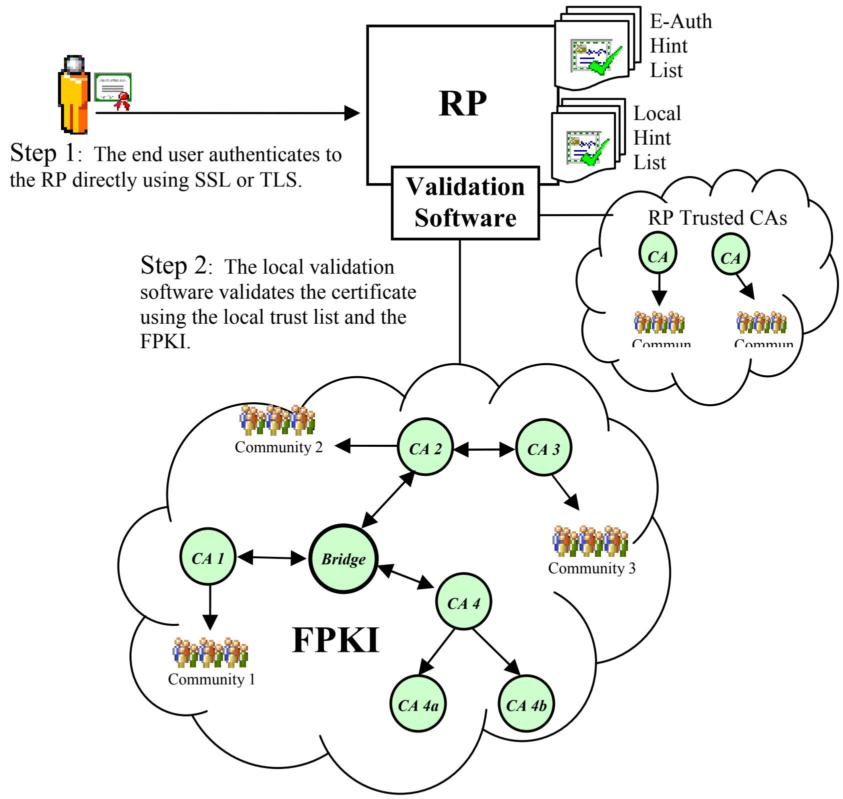
[5] Additional information on the use of hint lists is available at http://www.cio.gov/eauthentication.

4.2 Local Validation

In some cases, agencies may wish to perform certificate validation locally. For example, if an agency has elected to trust CAs not cross-certified with the FBCA, the agency has to add those CAs to its local trust list. The PMO supports these agencies by performing software evaluation on products that can be run locally. The PMO performs software evaluation based on the FPKI requirements established by NIST, and provides an approved product list for agencies.

Figure 4-2 depicts this use case. In Step 1, the end user arrives at the RP either directly or via redirect from an ASC entity providing RP/CS discovery service. There is no need for the RP to redirect the end user to a CS. That is because TLS and SSL allow the end user to authenticate directly to the RP using a certificate without revealing any secret information. The RP authenticates the end user, and then uses locally installed validation software that validates credentials using the agency's trust list. Communication with a validation service is not required.

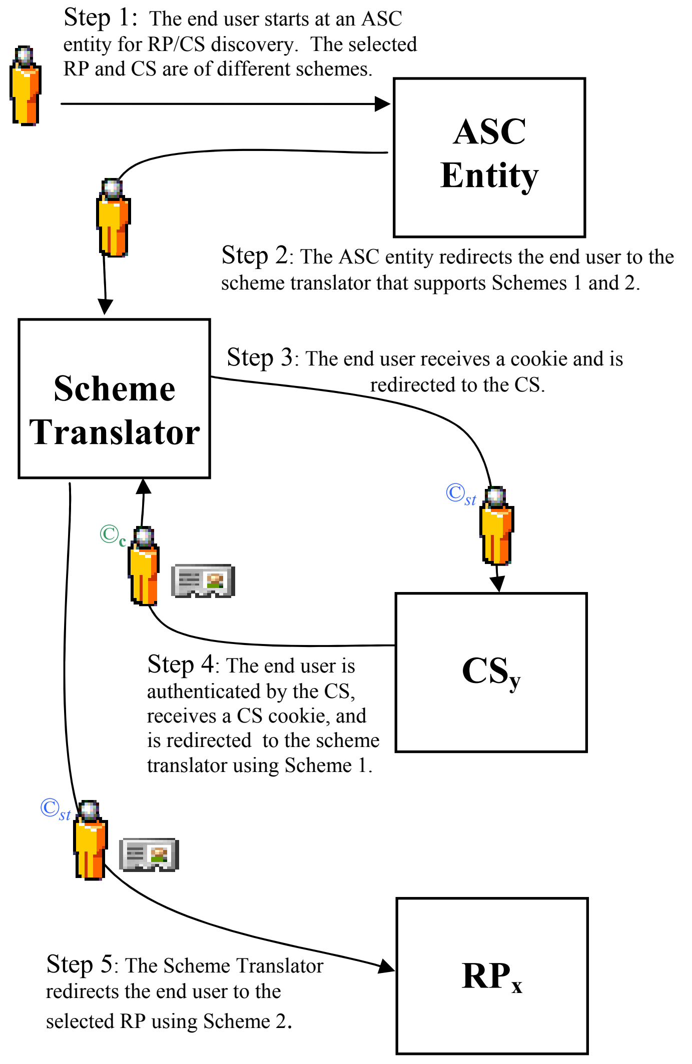
Figure 4-2: Local Validation


E-Auth
Hint
List
RP
Local
Hint
List
Step 1: The end user authenticates to the RP directly using SSL or TLS.
Validation Software
RP Trusted CAs
CA
CA
Commun
Commun
Step 2: The local validation software validates the certificate using the local trust list and the FPKI.
Community 2
CA 2
CA 3
Community 3
CA 1
Bridge
CA 4
FPKI
Community 1
CA 4a
CA 4b

5 Scheme Translation Use Cases

Figure 5-1 is a possible sequence of events for scheme translation within the architectural framework[6]. The exact flow depends upon the adopted scheme. In this example, the end user starts at an ASC entity to select a CS and RP, as shown in Step 1. Upon detecting that the RP and CS are of different adopted schemes, the ASC entity redirects the end user to the appropriate scheme translator (i.e., supports the adopted schemes of both the RP and the CS), as shown in Step 2. The scheme translator provides the end user with a cookie that contains the selected RP (to know where to redirect the end user once returned from the CS), then redirects the end user to the CS, as shown in Step 3. The CS performs the same functions as any other use case, authenticating and redirecting the end user, as shown in Step 4. The scheme translator now has the identity assertion for the end user and redirects the end user and the identity assertion to the RP using adopted scheme 2.

Figure 5-1: Scheme Translator


Step 1: The end user starts at an ASC entity for RP/CS discovery. The selected RP and CS are of different schemes.
ASC Entity
Step 2: The ASC entity redirects the end user to the scheme translator that supports Schemes 1 and 2.
Scheme Translator
Step 3: The end user receives a cookie and is redirected to the CS.
©st
©c
CSy
Step 4: The end user is authenticated by the CS, receives a CS cookie, and is redirected to the scheme translator using Scheme 1.
©st
Step 5: The Scheme Translator redirects the end user to the selected RP using Scheme 2.
RPx

Since the scheme translator does not interact with the end user, its role is completely transparent.

The CS interacts with the scheme translator as if it were any other RP. Therefore, CSs do not require additional functionality to interface with scheme translators.

The RP interacts with the translator as if it were any other CS. Therefore, RPs do not require additional functionality to interface with scheme translators.

Only the ASC entity configuration and the scheme translator are required to bridge the gap among multiple adopted schemes.

Starting elsewhere (e.g., at the CS, at the RP) generally works the same.

[6] Additional specifications will be developed for scheme translators as required by the Federation.

5.1 Certificate-Based Credentials at Assertion-Based Applications

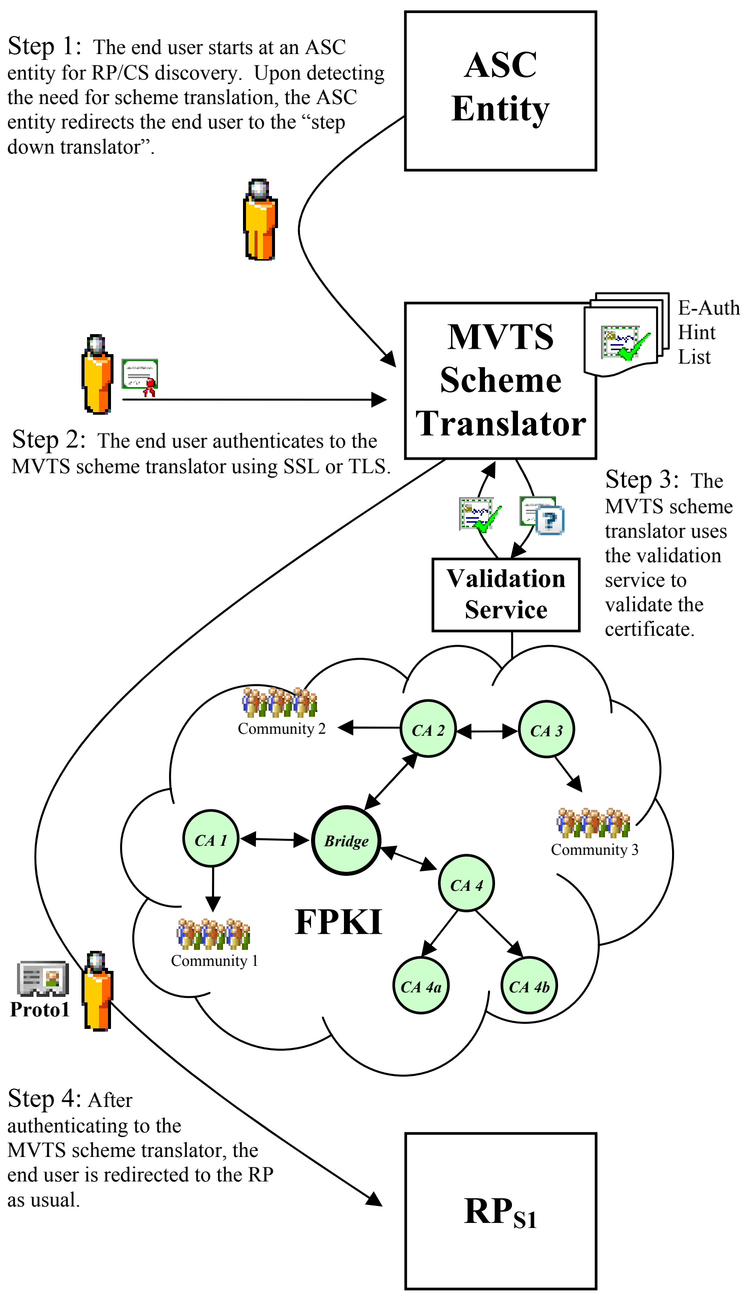
One Federation requirement is that credentials should be usable with any RP that has an equal or lower assurance level. That implies that PKI credentials should be usable at assertion-based RPs. To avoid the need for assertion-based RPs to validate certificates, the PMO deploys a special scheme translator via the MVTS. It translates certificates trusted by the FBCA into the Federation's SAML based adopted schemes.

Figure 5-2 is a possible sequence of events for an end user with a PKI credential accessing an assertion-based RP. The exact flow depends upon the adopted scheme.

In Step 1, the end user starts at an ASC entity providing RP/CS discovery service. Upon end user selection, the ASC entity determines the need for scheme translation and redirects the end user to the MVTS scheme translator. In Step 2, the end user authenticates to the MVTS scheme translator using a certificate. In Step 3, the MVTS scheme translator uses the validation service to validate the certificate before redirecting the end user to the RP in Step 4.

The RP does not need any special capabilities to leverage the MVTS scheme translator. The MVTS scheme translator interacts with the RP as if any other CS. The intelligence that determines whether scheme translation is necessary is in the ASC entity providing CS/RP discovery service.

Figure 5-2: Certificates at Assertion-Based RPs



Step 1: The end user starts at an ASC entity for RP/CS discovery. Upon detecting the need for scheme translation, the ASC entity redirects the end user to the "step down translator".

Step 2: The end user authenticates to the MVTS scheme translator using SSL or TLS.

Step 3: The MVTS scheme translator uses the validation service to validate the certificate.

Step 4: After authenticating to the MVTS scheme translator, the end user is redirected to the RP as usual.

APPENDIX A: SCHEME ADOPTION

Considering the architectural framework allows multiple scheme translators to co-exist, the PMO must carefully govern the introduction of new schemes. Scheme translators add complexity to the architecture and establish an additional point of failure in transactions. Therefore, the PMO should minimize their use. Ideally, only very few schemes exist in the architectural framework at any given time, and the PMO phases out scheme translators over time as Federation members adopt dominant schemes.

Figure A-1 depicts the lifecycle for adopting new schemes. As new schemes emerge that meet Federation requirements, they are assessed for the availability of interoperable COTS, then piloted on a small scale. If the pilots are successful, Federation members migrate to support the new scheme and/or the PMO deploys scheme translators. The scheme translators eliminate the need for every Federation member to migrate at the same pace. Federation members slower to implement new adopted schemes can rely on scheme translators (if available) until they are ready to implement or the Federation sunsets the older adopted scheme. Federation members that have adopted new schemes can begin to use them immediately, enjoying other features they may offer without losing authentication interoperability with the rest of the Federation.

Figure A-1: Scheme Adoption Lifecycle

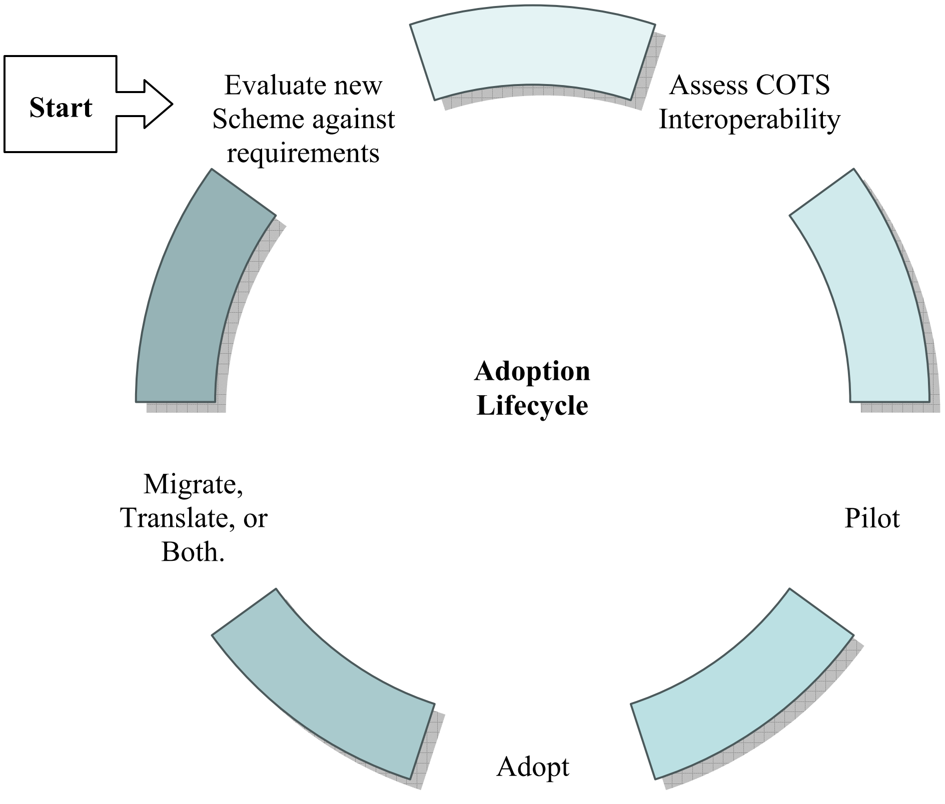
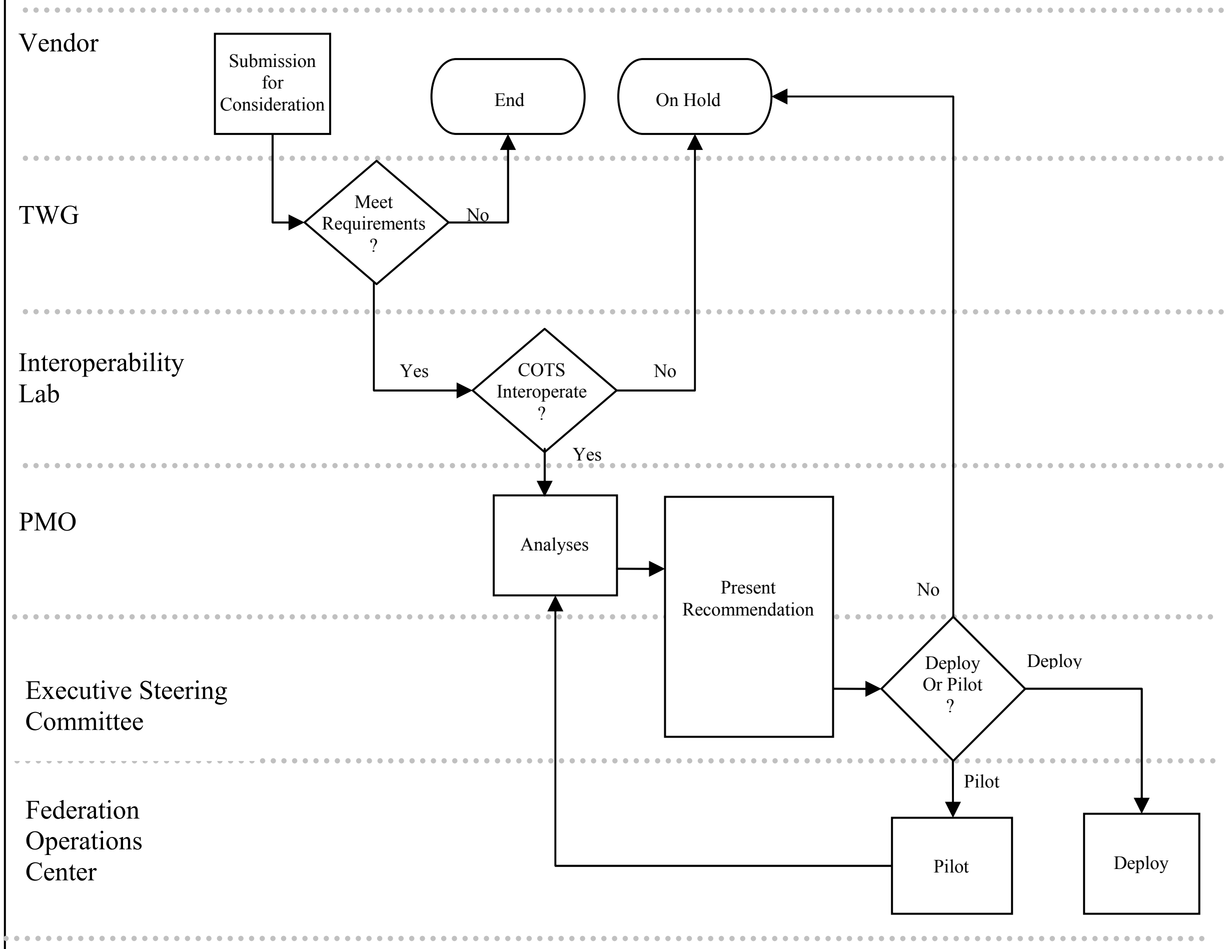

Start
Evaluate new Scheme against requirements
Assess COTS Interoperability
Adoption Lifecycle
Pilot
Adopt
Migrate, Translate, or Both.

Figure A-2 shows a process for adopting new schemes. The TWG evaluates new schemes against Federation requirements. The minimum requirements for an adopted scheme in the ASC are:

1. **Standards-based**: The scheme must be an industry standard approved by a recognized standards body. The PMO will not consider proprietary mechanisms. The PMO will consider de facto standards if deemed sufficiently mature by the TWG.
2. **Multi-domain (MD) SSO**: The scheme must provide a mechanism for MD SSO, which is the principal function for schemes in the architecture (i.e., required for the redirect of end users from the CS to the RP).
3. **Trust Mechanism**: The scheme must provide a trust mechanism as a pre-requisite to processing a message. Examples include mutual TLS authentication and message-level digital signature/verification. The specific mechanism varies from scheme to scheme.

Next, the Federation Interoperability Lab assesses the state of COTS interoperability and provides analyses to the PMO, including recommendations for using scheme translators. If sufficient interoperable COTS exist, and the scheme offers sufficient benefit to the government, the Executive Steering Committee (ESC) decides whether to deploy or pilot the scheme within the architecture.

Figure A-2: Scheme Adoption Process



APPENDIX B: RISK MITIGATION

Message exchange betweens ASC entities (especially between the CS to the RP) is a crucial part of the ASC. Therefore, like any good design, the ASC employs multiple layers of risk mitigation to ensure smooth redirects. Federation use of standards, testing of COTS products, testing of Federation member systems, configuration metadata, and E-GCA certificates, among other things, ensure secure, confidential, successful redirects. Each adopted scheme defines the specific risk mitigation mechanisms relevant to it[7]. That is, each adopted scheme may implement different risk mitigation mechanisms, as appropriate for its underlying identity standard and other factors.

In addition to risk mitigation mechanisms, the ASC requires exception handling to provide a consistent and helpful end user experience – especially for redirect exceptions. Exception handling indirectly supports risk mitigation in that exceptions are captured, terminated, and reported, rather than being allowed to continue and possibly causing harm or unintended results. The Federation defines a standard set of exceptions that Federation member systems must handle. Supported error codes may change and/or expand over time. Each adopted scheme include specific exception definitions, including applicable exception handling and reporting guidelines [8].

One example of an exception is a CS attempting to make an assertion to a higher assurance level RP. Such an exception requires improper metadata configuration. When the RP detects the problem, exception handling appropriate for the adopted scheme occurs, resulting in the end user seeing a page explaining the error, and allowing the end user to select another compatible CS (or compatible RP for the CS). In addition, the Federation member system logs the exceptions for subsequent review by Federation Operations Center (FOC). If the FOC determines that the CS-RP connection pair is valid, the FOC may disable the connection pair until they can fully debug the problem.

[7] Details are documented in each adopted scheme document and corresponding interface specification.
[8] Ibid

Appendix C: Secure Email

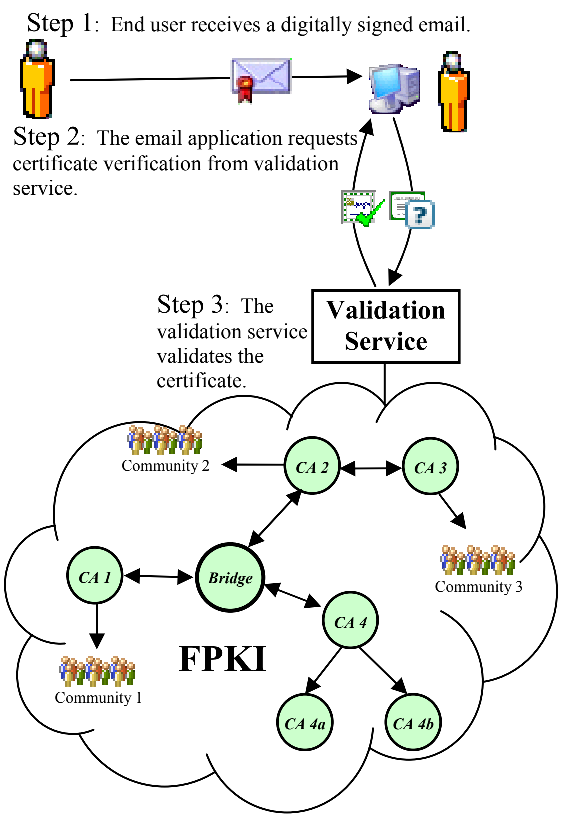
The ASC supports secure email by using the same certificate validation techniques described in section 4. Any S/MIME capable e-mail software product can be used to process signed and encrypted email.

The following sections describe options for validating the status of the certificate attached to the message. Each organization must determine which approach is appropriate for its needs.

C-1. E-Authentication Validation Service

Figure C-1 shows the use of the E-Authentication validation service[9] for certificate status checking. In Step 1, the end user receives a digitally signed email. In Step 2, the email software on the end user's computer requests certificate verification from the validation service to determine the certificate's status. This is the same validation service depicted in section 4, which determines the certificate status through the bridge[10]. In Step 3, the validation service validates the certificate.

Figure C-1: Validation Service


Step 1: End user receives a digitally signed email.
Step 2: The email application requests certificate verification from validation service.
Step 3: The validation service validates the certificate.
Validation Service
Community 2
CA 2
CA 3
Community 3
CA 1
Bridge
CA 4
FPKI
Community 1
CA 4a
CA 4b

In this approach, the end user's e-mail software must be capable of processing S/MIME, and be capable of using a certificate status protocol supported by the validation service. As described in section 4, these protocols may vary over time; examples include XKMS, OCSP, and SCVP.

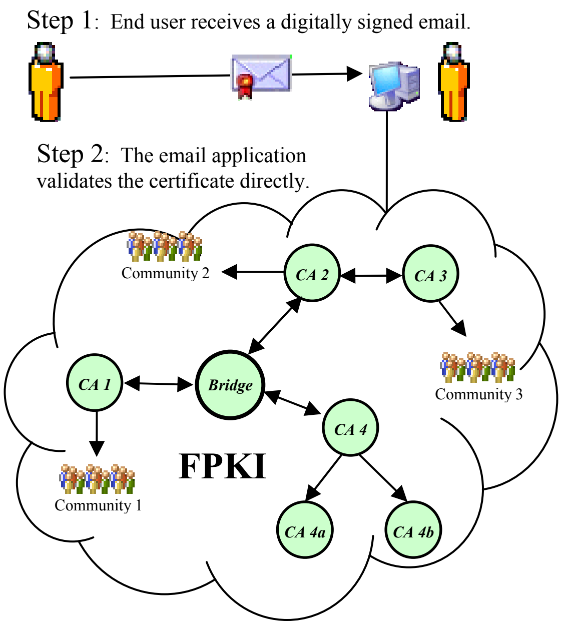
This option is not appropriate for RPs that trust CAs not cross-certified with the bridge.

[9] Validation Service software is sometimes identified as Certification Status Authority (CSA).
[10] The bridge is referred to as the Bridge Certification Authority (BCA).

C-2. Desktop Validation

Another approach is to run certificate validation software on the end user's desktop. The capability could be part of the email software, or be a software addition. Figure C-2 depicts this use case. In Step 1, the end user receives a digitally signed email. In Step 2, the end user's desktop validates the certificate through the bridge.

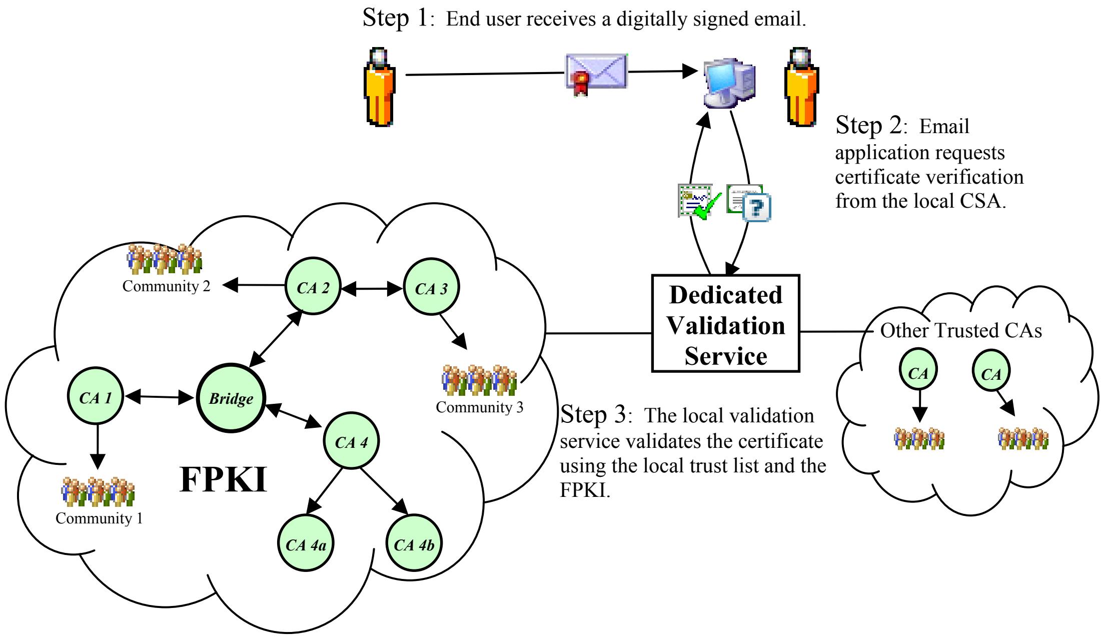
Figure C-2: Desktop Validation


Step 1: End user receives a digitally signed email.
Step 2: The email application validates the certificate directly.
Community 2
CA 2
CA 3
Community 3
CA 1
Bridge
CA 4
FPKI
Community 1
CA 4a
CA 4b

C-3. Dedicated Validation Service

For organizations that trust CAs not trusted government-wide, a dedicated validation service may be a good choice. The local validation service may be configured to trust other CAs as appropriate for that organization. Email software used in that organization is configured to rely on the dedicated validation service. The validation service must still be capable of interoperating within the bridge to ensure other Federation credentials are accepted. Figure C-3 depicts this use case. In Step 1, the end user receives a digitally signed email. The email software then requests certificate verification from the local validation service, as shown in Step 2. In Step 3, the local validation service validates the certificate using the local trust list and FPKI.

Figure C-3: Dedicated Validation Service



Step 1: End user receives a digitally signed email.

Step 2: Email application requests certificate verification from the local CSA.

Step 3: The local validation service validates the certificate using the local trust list and the FPKI.

C-4. Other Approaches

Organizations can combine or vary the previously described options to create other options. For example, a dedicated validation service could use the ASC validation service for any certificate it could not validate on its own, or a desktop validation engine could be configured with locally trusted CAs.

The key point is to ensure that e-mails are signed and encrypted using S/MIME, and that certificates comply with X.509 version 3. If those two standards are followed, then a variety of certificate validation approaches may be employed.

APPENDIX D: ELECTRONIC FORMS APPLICATIONS

D-1. Introduction

Some E-Government businesses use electronic forms applications rather than on-line web forms. These applications do not have the same characteristics as browser-based applications. This appendix shows an approach for using the ASC with forms applications.

Many forms applications support the use of PKI certificates to sign the form. The form server component can then validate the certificate (and thus the signature) using one of the certificate validation approaches described earlier in this document. This approach is straightforward and widely supported by forms software, but requires end users to have certificates. Section D-2 describes certificate-based submission of forms.

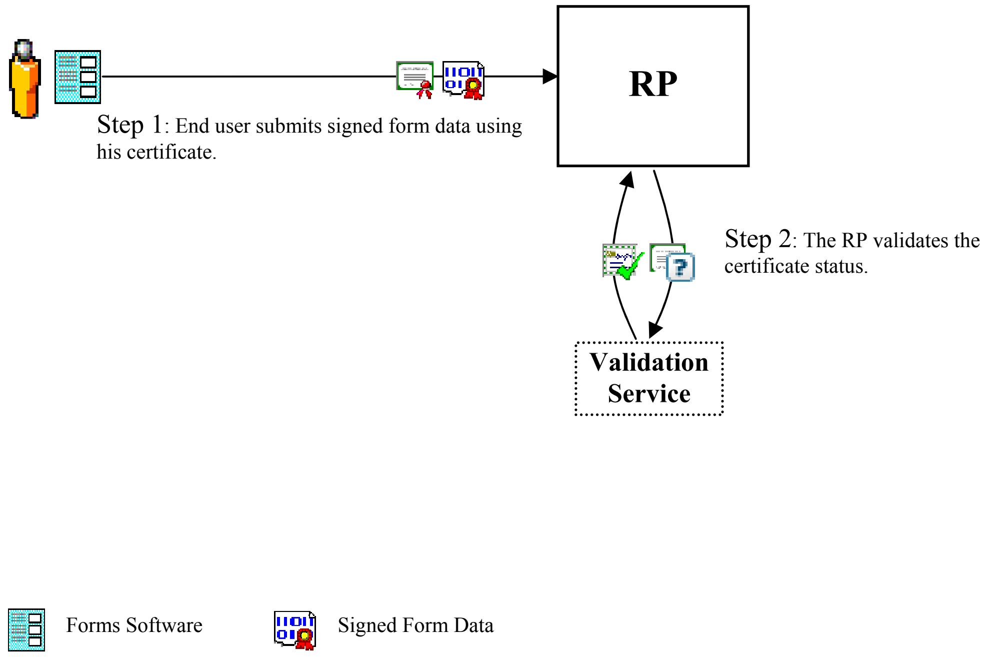
The use of PINs or Passwords to submit forms in a federated environment is more complex due to NIST restrictions against sharing secrets. The forms software cannot submit third party passwords to RPs directly. The approach described here uses the existing architecture by authenticating through a browser window, which requires no special interface for CSs, and maintains the scalability and privacy features of the ASC. This is the recommended approach for pin/password authentication of form data submissions using the ASC. As standards evolve, the ASC may be updated to accommodate additional approaches. In this approach, the browser window is not required until the form data is submitted. End users are still free to download forms without authenticating and may complete the forms offline. When the end user submits the form data, the form application opens a browser window and redirects the end user to the Portal, which in turn redirects the end user to their CS for authentication. Section D-3 describes this approach in more detail.

D-2. Certificate-Based Form Submission

This section describes how electronic forms work with certificate-based authentication. A significant number of electronic forms products support digital signatures using certificates, so this is the most straightforward way to submit signed forms.

Figure D-1 describes the sequence of events for this case. Using the form software, the end user signs the form data, and then submits it to the RP along with the certificate, as shown in Step 1. After verifying the signature, the RP uses a validation service to validate the certificate, as shown in Step 2. A number of approaches can be used to validate the certificate, see the previous appendix or section 4 for more information.

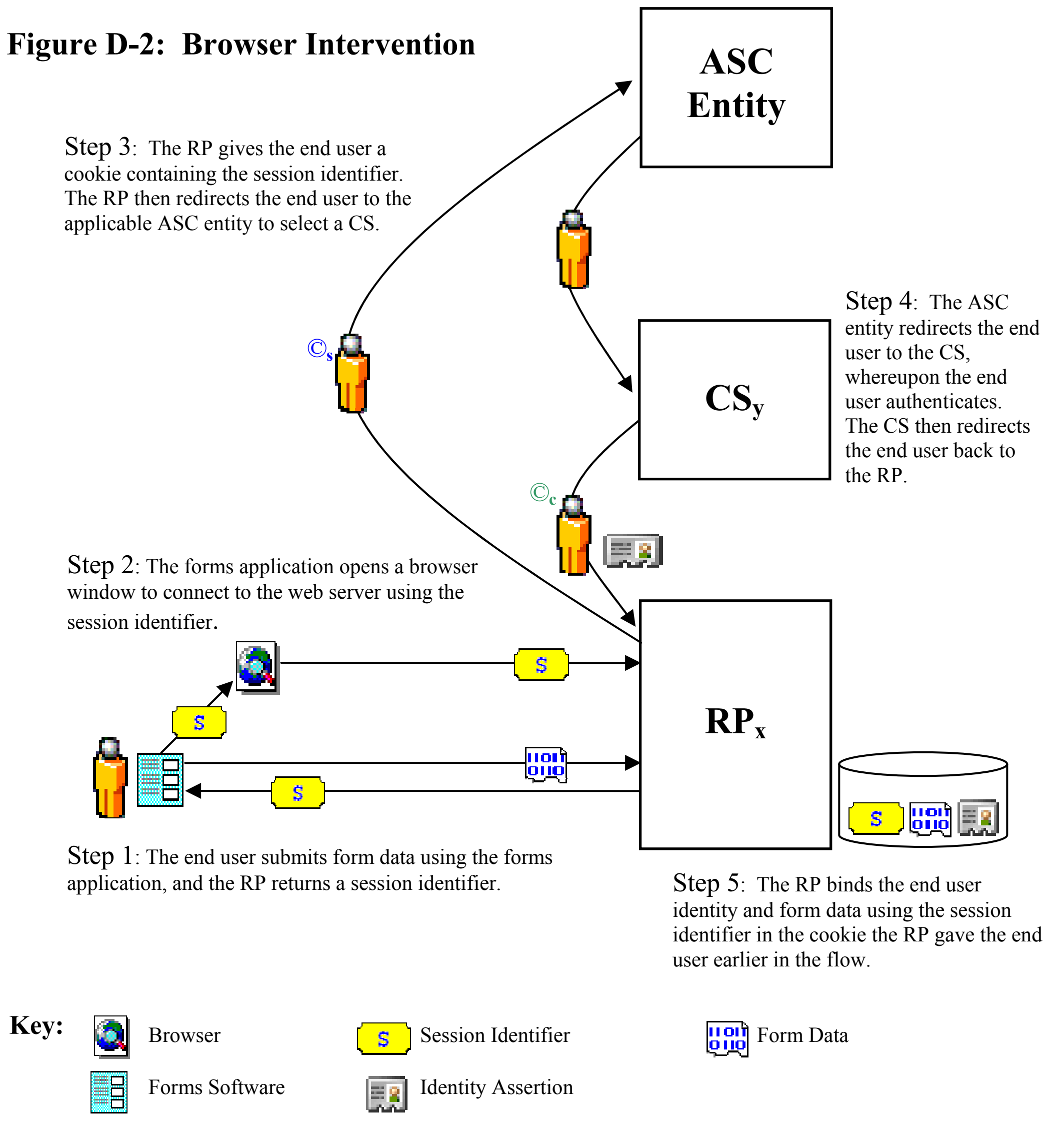
Figure D-1: Certificate-Based Form Submission


RP
Step 1: End user submits signed form data using his certificate.
Step 2: The RP validates the certificate status.
Validation Service
Key:
Forms Software
Signed Form Data

D-3. Browser Intervention

Figure D-2 shows the flow of events for authenticating a form submission not using digital certificates. The exact flow and processing is dependent upon the adopted scheme and implementation decisions, so this example is generic. Step 1 shows the end user submitting form data using a forms application. Upon receipt of the form data, the RP returns a session identifier to the forms application. In Step 2, the forms application opens a browser window with the RP's URL and the session identifier. In Step 3, the RP gives the end user a cookie that contains the session identifier. The RP then redirects the end user to an ASC entity for CS discovery service (it is possible the RP itself provides the CS discovery service, which precludes the need for this redirect). In Step 4, the end user selects a compatible CS, and the ASC entity redirects the end user to the CS. The end user authenticates to the CS. The CS then redirects the end user to the originating RP. In Step 5, the RP reads the session identifier from the cookie it gave to the end user earlier in the flow, allowing the RP to bind the asserted identity to the form submission. Allowing a browser window to intervene at the time of authentication allows forms applications to leverage all applicable Federation CSs, and minimizes the need to customize forms applications.

Figure D-2: Browser Intervention



Step 3: The RP gives the end user a cookie containing the session identifier. The RP then redirects the end user to the applicable ASC entity to select a CS.

Step 4: The ASC entity redirects the end user to the CS, whereupon the end user authenticates. The CS then redirects the end user back to the RP.

Step 2: The forms application opens a browser window to connect to the web server using the session identifier.

Step 1: The end user submits form data using the forms application, and the RP returns a session identifier.

Step 5: The RP binds the end user identity and form data using the session identifier in the cookie the RP gave the end user earlier in the flow.

Appendix E: Glossary

Term	Definition
Adopted Scheme	Precisely scoped identity scheme accepted for use by the Federation.
Approved	Acceptance by the E-Auth PMO to participate in the E-Authentication Federation, or other inclusion or use in the E-Authentication Federation.
Architecture Framework	IEEE STD 1471-2000 states "An architecture is the fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution." The ASC architectural framework is based on an open architecture that uses off-the-shelf components and conforms to approved standards. The ASC architectural framework accommodates the use of assertion based credentials (PIN and Passwords) as well as certificate-based credentials within the same environment. Over time, the architecture will leverage multiple emerging schemes such as the SAML and Liberty Alliance, and will not be built around a single scheme or commercial product.
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.
Assurance Level	Level of trust, as defined by the OMB M-04-04.
Attribute	A single, specific piece of information. An example is an identity attribute such as name.
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 (ASC)	A federated architecture that leverages credentials from multiple domains through certifications, guidelines, standards adoption and policies. The ASC accommodates assertion-based authentication (i.e., authentication of PINs and Passwords) and certificate-based authentication (i.e., public key certificates) within the same environment. Over time, the architecture will leverage multiple emerging schemes such as the SAML and Liberty Alliance, and will not be built around a single scheme or commercial product. In this light, the ASC is more precisely defined as an architectural framework.
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.

Term	Definition
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.
Authorization	An authenticated end user's right to perform transactions or access data of an application. RPs maintain full control over authorization.
Browser Session	The period of time the end user's browser is open. The browser session begins when the end user opens their browser and ends when it is closed. All session cookies are terminated when the Browser session ends.
Certificate Validation	Whenever a certificate is to be trusted, a check is conducted to ensure it is not revoked, expired, or otherwise invalid.
Certification Authority (CA)	A certification authority is an authority in a network that issues and manages security credentials and public keys for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate. Depending on the public key infrastructure implementation, the certificate includes the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner.
Claimant	A party whose identity is to be verified using an authentication protocol.
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
Composite Application	An application that relies on remote services to complete its transactions.
Cookie (Transient Cookie)	A message given to a web browser (e.g., end user's web browser) by an application (e.g., RP, CS, E-Authentication Portal, Scheme Translator). The ASC only uses transient cookies, which are stored in temporary memory and erased when the end user closes their web browser.
Credential	Digital documents used in authentication and access control that bind an identity or an attribute to a claimant's token or some other property, such as an end user's current network address. Note that this guidance distinguishes between credentials and tokens, while other documents may lump tokens with credentials.
Credential Assessment Framework (CAF)	Based on technical and policy guidance from Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST), the CAF provides a structured means of delivering assurances to Federal agencies as to the veracity, and thus dependability of identity credentials and tokens. This assurance is achieved by evaluating and assessing CSPs and their credential-issuing service(s) against criteria established in the CAF.

Term	Definition
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.
Credential Service (CS) Cookie	Once a CS authenticates an end user, the CS assigns a session cookie to the end user, which is also used to facilitate single sign-on. The contents and sensitivity of the CS cookie will vary among CSs. The combination of the Portal cookie and the CS cookie is the mechanism for architecture-wide single sign-on, regardless of the Multi Domain SSO scheme being used.
Credential Service Provider (CSP)	An organization that offers one or more CSs.
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.
E-Governance Certification Authorities (E-GCA)	Established by the government to issue certificates as applicable for the adopted scheme. Certificates that may be issued TLS authentication, digital signing, and digital encryption. E-GCA certificates effectively control which entities can participate in the Federation.
End User	Any citizen, government employee, contractor, or business that uses an RP. One of the principal goals of E-Authentication is to make the end user experience as simple as possible by improving the availability and ease of use of credentials.
Extensible	Something designed so that later designers can extend its capabilities.
Extensible Markup Language (XML)	Specification developed by the W3C. XML is a pared-down version of SGML, designed especially for Web documents. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.
Federal Bridge Cross-Certification	Allows a CA to interoperate within the "membrane" of the Bridge CA.
Federal Bridge Certification Authority (FBCA)	Allows PKIs to trust digital certificates issued by other entities that have been policy mapped and cross-certified with the FBCA. See http://www.cio.gov/fpkipa/.
Federal Enterprise Architecture (FEA)	Component-based architecture that facilitates expansion of E-Government by identifying opportunities to collaborate, consolidate, and leverage IT investments across government. The architecture includes several reference models, including Performance (PRM), Business (BRM), Service Component (SRM) and Technical (TRM).
Federal Public Key Infrastructure (FPKI)	Employs a Briidge Certification Authority to harmonize policies and procedures for CAs. See http://www.cio.gov/fpkipa/.
Federated	Two or more entities that linked or bound together.
Federated Identity	Agreement between ASC entities on a set of identifiers and/or attributes to use to refer to the Principal
Federation Portal (Portal)	A website that helps end users locate the CSs and RPs they need to complete their transactions. The Portal also maintains information about CSs and RPs referred to as metadata, which includes technical interface data as well as descriptive information. When the end user opts into single sign-on, the Portal assigns a session cookie. The Portal also generates TIDs that are used to track transactions across various components in the architecture.
Flexible	Capable of being changed.

Term	Definition
Hint List	A list of CAs sent to browsers during the TLS/SSL handshake. The browser uses the list to help the end user select the certificate to use for authentication. The E-Authentication Hint List consists of the names of every CA that is reachable from the FBCA.
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.
Liberty Alliance	See http://www.projectLiberty Alliance.org/specs/
Local Validation	Validation without use of an external service.
Managed Validation and Translation Service (MVTS)	A multi-Agency solution to enable active software applications with an interface to an approved federal PKI solution, and to provide long-term authentication support and transaction processing services. Specifically, MVTS provides: ▪ TCP/IP interfaces that accept validation requests for X.509v3 Public Key Infrastructure (PKI) certificates and process a status response indicating whether the certificate is valid or not, ▪ Certificate-based authentication support services that enable government applications to rely on the federal PKI(s), ▪ Information security and assurance support services and ▪ Translation services on certificates trusted by the Federal Bridge Certificate Authority into the various interface specifications adopted by the Federation for Security Assertion Markup Language (SAML) profile schemes.
Metadata	Information necessary for nodes (member systems) to technically interoperate. Metadata may encompass: • Federation specific information– scheme independent information pertaining to Federation members and Federation policies (e.g., assurance levels) • Scheme specific information – information that directly supports technical interoperability for a specific adopted scheme. Some or all of the metadata for this scheme may not be used for a different adopted scheme. Failure to completely and correctly configure metadata can preclude technical interoperation, or result in unexpected consequences or negative impacts to any number of nodes. Metadata is not considered secret information.
Online Certificate Status Protocol (OCSP)	An on-line protocol used to determine the status of a public key certificate. See [RFC 2560].
Personal Identification Number (PIN)	A password consisting only of decimal digits.

Term	Definition
Personally Identifiable Information (PII)	Any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains. This includes information that is used in a way that is personally identifiable, including linking it with identifiable information from other sources, or from which other personally identifiable information can easily be derived, including, but not limited to, name, address, phone number, fax number, email address, financial profiles, and social security number, and credit card information.
Pilot	A limited, controlled test.
Portal Cookie	Used by the Federation Portal to optionally track the CS selected by the end user in the browser session. The combination of the Portal cookie and the CS cookie is one mechanism for single sign-on.
Project 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.
Protocol	An agreed-upon format for communication between two ends points.
Public Key Certificate (Certificate)	X.509v3 digital certificates in a Public Key Infrastructure (PKI) for authentication can be used at any assurance level.
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
Reliable	The trustworthiness a system to do what it is expected or designed to do.
Relying Party (RP) (Also agency application, AA, in some adopted schemes)	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 Cookie	An RP may assign an end user an RP cookie to help track the RP session, or other application session information.
SAML Artifact Profile	The browser/artifact profile of SAML relies on a reference to the needed assertion traveling in a SAML artifact, which the destination site must dereference from the source site in order to determine whether the end user is authenticated. See http://www.oasis-open.org/specs/index.php#samlv1.0

Term	Definition
Scalable	Ability to handle a large increase in users, workload or transactions without undue strain.
Scheme	Schemes, such as SAML and Liberty Alliance, specify protocols and standards for federated identity mechanisms for different entities to share identities without requiring the end user to manage multiple accounts.
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.
Secure Sockets Layer (SSL) (See also: Transport Layer Security)	Protocol for transmitting private documents via the Internet by using a private key to encrypt data transferred over the SSL connection.
Secure/Multipurpose Internet Mail Extensions (S/MIME)	A standard that extends the MIME to support the signing and encryption of e-mail transmitted across the Internet.
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.
Session Cookie	Small transient file that contains information about an end user that disappears when the end user's browser is closed. Unlike a persistent cookie, a transient cookie is not stored on an end user’s hard drive, but is only stored in temporary memory that is erased when the browser is closed.
Shibboleth	Standards-based, open source middleware software which provides Web Single SignOn (SSO) across or within organizational boundaries. The Shibboleth software implements the OASIS SAML v1.1 specification, providing a federated Single-SignOn and attribute exchange framework. Shibboleth also provides extended privacy functionality allowing the browser user and their home site to control the Attribute information being released to each Service Provider. See http://shibboleth.internet2.edu/

Term	Definition
Simple Certificate Validation Protocol (SCVP)	Allows a client to offload certificate handling to a server. The server can provide the client with a variety of valuable information about the certificate, such as whether the certificate is valid, a certification path to a trust anchor, and revocation status. SCVP has many purposes, including simplifying client implementations and allowing companies to centralize trust and policy management.
Simple Object Access Protocol (SOAP)	Lightweight XML-based messaging protocol used to encode the information in Web service request and response messages before sending them over a network. It consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses. SOAP messages are independent of any operating system or protocol and may be transported using a variety of Internet protocols, including MIME and HTTP.
Single Sign-on	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.
Technology Neutral	Not favoring a particular technology. This is the basis of the E-Authentication Initiative's architecture framework.
Token	Something that the claimant possesses or knows (typically a key or password) that can be used to remotely authenticate the claimant's identity. Technically, the token includes an end user id and password that ensures token uniqueness within a credential domain.
Transaction Identifier (TID)	Mechanism for tracking transactions across various components in the architecture. TIDs will be generated by the Portal, and will be passed with the end user, via query string, as they are redirected from (1) the Portal to CSs, (2) from CSs to AAs, and, (3) once generated by the Portal, to the Portal by AAs or CSs. A new transaction occurs each time the Portal hands-off the end user to a CS for authentication or re-authentication.
Transitive Trust	A trust relationship with the property that if trust holds between a first element and a second and between the second element and a third, trust holds between the first and third elements.
Transport Layer Security (TLS)	An authentication and security protocol implemented in current browsers and web servers. TLS is defined by [RFC 2246] and [RFC 3546]. TLS is similar to the older Secure Socket Layer (SSL) protocol and is effectively SSL version 3.1.
Validation Service	A service that validates certificates remotely. The Validation Service is an end-to-end solution that spans server-side (i.e., the validation service provider's hosted service) and client-side (i.e., software integrated into the RP).

Term	Definition
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.
WS-Federation	See: http://www106.ibm.com/developerworks/webservices/library/ws-fed/
XML Key Management Specification (XKMS)	Defines a Web services interface to a PKI. This makes it easy for applications to interface with key-related services, like registration and revocation, and location and validation.

APPENDIX F: ACRONYMS

Acronym	Definition
AA	Agency Application
AAid	Agency Application Identifier
AS	Adopted Scheme
ASC	Authentication Service Component
AuthZ	Authorization
CA	Certification Authority
CDC	Common Domain Cookie
COTS	Commercial off the Shelf
CS	Credential Service
CSA	Certification Status Authority
CSid	Credential Service Identifier
CSP	Credential Service Provider
DNS	Domain Name Service
E-GCA	E-Governance Certification Authorities
E-RA	E-Authentication Risk Assessment
ESC	Executive Steering Committee
FBCA	Federal Bridge Certification Authority
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standards
FMD	Federation Membership Documents
FOC	Federation Operations Center
FPKI	Federal Public Key Infrastructure
FPKI PA	Federal Public Key Infrastructure Policy Authority
HSPD-12	Homeland Security Presidential Directive #12
HTTP	Hyper Text Transfer Protocol
MD SSO	Multi-Domain Single Sign-On
MVTS	Managed Validation and Translation Service
NIST	National Institute of Science and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMO	Program Management Office
RC	Release Candidate
RP	Relying Party
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAML	Security Assertion Markup Language
SCVP	Simple Certificate Validation Protocol
SP	Special Publication
SSL	Secure Sockets Layer
SSO	Single Sign-on
TBD	To Be Determined

Acronym	Definition
TID	Transaction Identifier
TLS	Transport Layer Security
TWG	Technical Working Group
U.S.	United States
WS	Web Services
XKMS	XML Key Management Specifications
XML	Extensible Markup Language