



SAML Artifact Profile As an Adopted Scheme for E-Authentication

Version 1.0.0
June 28, 2004



Executive Summary

As part of the President's Management Agenda, the E-Authentication Initiative has been established to enable trust and confidence in E-Government transactions via the establishment of an integrated policy and technical infrastructure for electronic authentication. The result is the Authentication Service Component (ASC). The ASC is a federated architecture that is strategically designed to support different identity assurance schemes simultaneously. Some schemes support assertion-based authentication (i.e., authentication of PIN and Password credentials), while other schemes support certificate-based authentication (i.e., authentication of Public Key Infrastructure (PKI) digital certificates). Each scheme has its own specification for use. Since each scheme is different, ASC documentation must discuss each individual scheme in terms of its use within high-level ASC transaction flows and governance.

Security Assertion Markup Language (SAML) 1.0 Artifact Profile is one of the schemes supported by the ASC. SAML supports assertion-based authentication, and is predicated on the exchange of a SAML Artifact and a SAML Assertion between endpoints. In E-Authentication, an agency application (AA) and a credential service (CS) are the endpoints. This document highlights use of SAML 1.0 Artifact Profile at the transaction flow level. The ASC transaction flows discussed address two basic scenarios: (1) an end user begins at the E-Authentication Portal, and (2) the end user does subsequent transactions using single sign-on. In all cases, the flow and exchange of the SAML Artifact and SAML Assertion are shown. This ensures that those integrating SAML 1.0 Artifact Profile into the ASC understand its use in E-Authentication transaction flows.

Governance is discussed in context of SAML 1.0 Artifact Profile. Any architecture for government-wide authentication must provide some mechanism for the government to assert its authority over which agencies and credential service providers (CSPs) can participate. AAs and CSPs must communicate directly in SAML 1.0 Artifact Profile to exchange the SAML Artifact and SAML Assertion. To ensure only trusted parties communicate within this scheme, a Governing Authority is established to issue client and server digital certificates to them. Exchange of digital certificates by the parties effectively secures the channel of communication between them. The Governing Authority maintains records and issues certificates, but does not participate in end user authentication.

Finally, a special case known as Session Reset is discussed. After a period of time, an AA may want to re-authenticate an end user that that is already authenticated and using the AA. A different transaction flow is detailed that describes how this is accomplished. It also specifies the additional session reset parameter that needs to be present.

Table of Contents

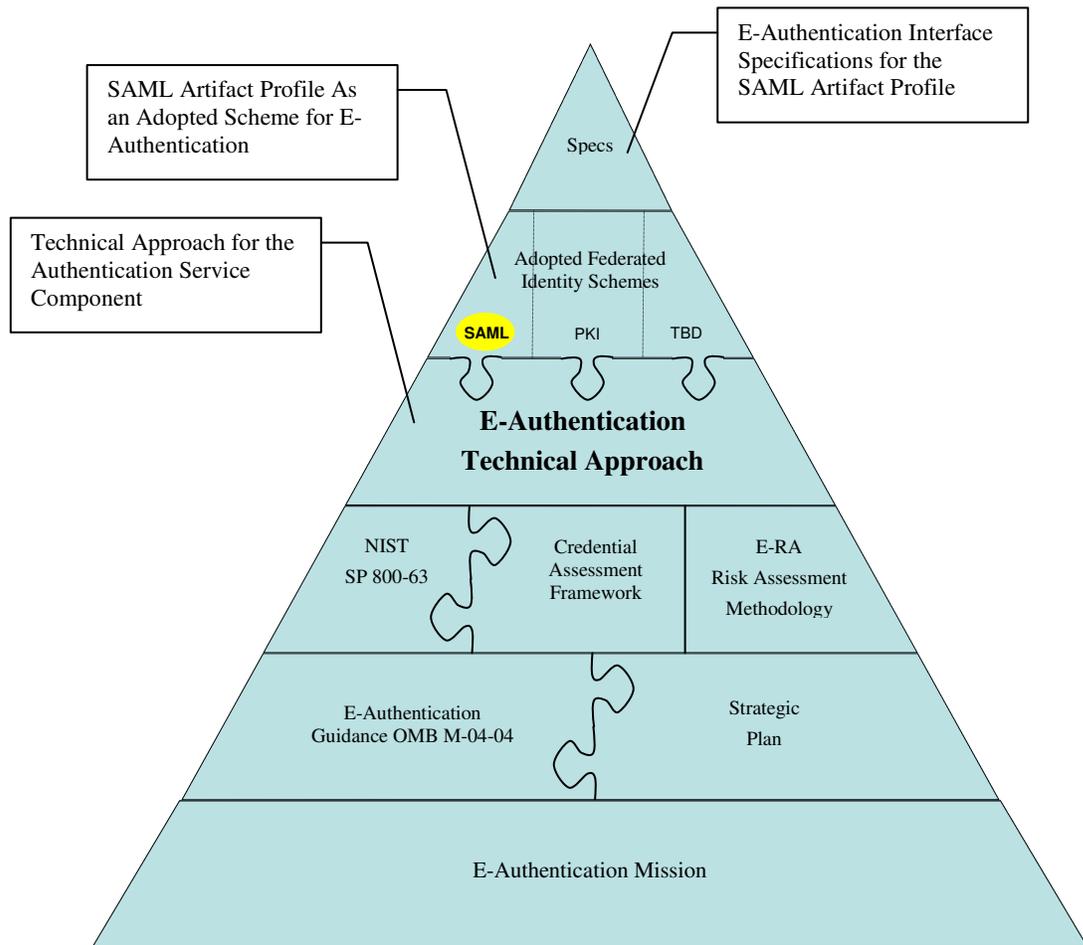
1	Introduction	1
2	Architecture Description	2
3	Single Sign-on	3
4	Governance.....	4
	Appendix A: Session Reset	5
	Appendix B: Glossary and Acronyms	6
	Appendix C: Document History and Editors.....	9

1 Introduction

This document provides an overview of the use of the Security Assertion Markup Language (SAML) 1.0 Artifact Profile in the E-Authentication Initiative. SAML 1.0 is one of the adopted schemes within the E-Authentication architectural framework. By integrating with the Authentication Service Component (ASC), an application owner can use a standard approach for authentication, rather than build or maintain an authentication structure. The SAML scheme described in this document supports assertion-based authentication. An alternative scheme, Public Key Infrastructure (PKI), supports certificate-based authentication.

This document is part of the ASC technical suite, which also includes the Technical Approach for the Authentication Service Component and the E-Authentication Interface Specifications for the SAML Artifact Profile. For complete comprehension, this document should be read after the Technical Approach and prior to the Interface Specifications. Figure 1 shows the documentation relationships for E-Authentication, and current versions of these documents are available on the E-Authentication website at <http://www.cio.gov/eauthentication/>.

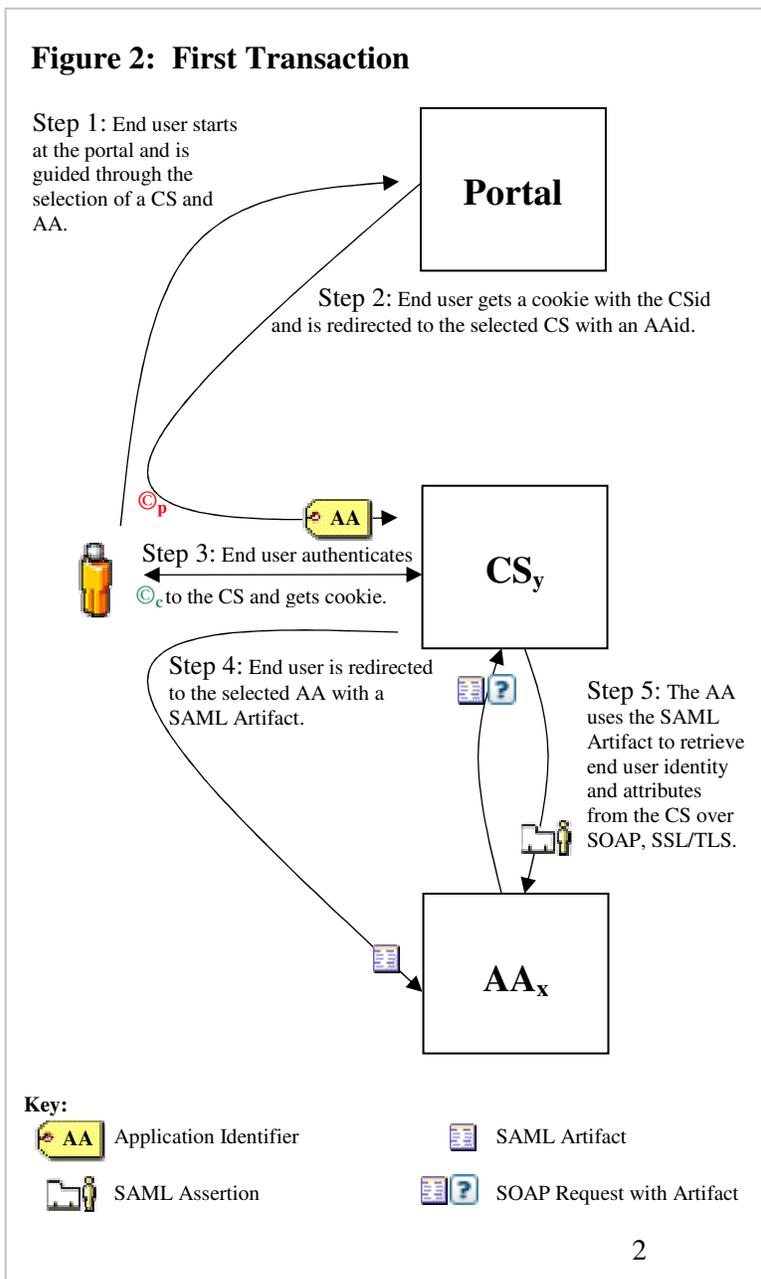
Figure 1: E-Authentication Document Hierarchy



2 Architecture Description

Figure 2 illustrates the initial process of authentication using SAML. In Step 1, the unauthenticated end user begins at the E-Authentication Portal (Portal). While interacting with the Portal, the end user makes two decisions, which Agency Application (AA) and which Credential Service (CS) to use. The Portal has access to the list of AAs and the assurance level required by each, as well as the list of CSs and the assurance level of their credentials.

Once the CS and AA are selected at the Portal in Step 2, the end user is redirected to the selected CS with an AA identifier (AAid). The AAid is simply a pointer or identifier to a particular AA; it is not sensitive and does not contain personal information. The AAid is included in the query string of the redirect, making it available to the CS. The Portal also assigns a session cookie with the CS identifier (CSid) to the end user indicating which CS the end user has selected for the required assurance level. The cookie is not sensitive and does not contain any personal information; it is used by the Portal to facilitate single sign-on in later transactions.



The CS then authenticates the end user in Step 3 and 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. Once the authentication is complete, the end user is redirected to the AA indicated by the AAid passed from the Portal.

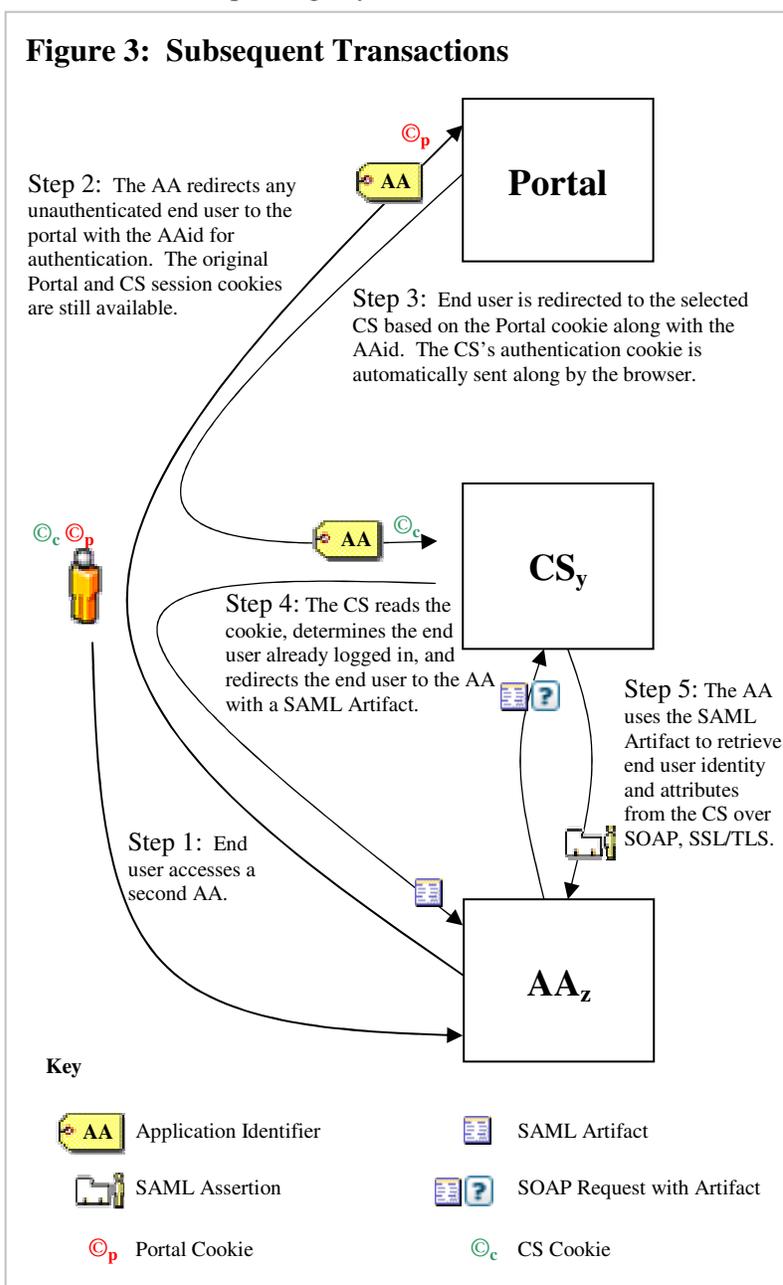
The redirection to the AA (Step 4) includes a SAML Artifact, which is used by the AA to retrieve SAML assertions (Step 5) containing the identity and attributes of the end user. Once the assertions are retrieved, the end user is authenticated and can begin interacting with the application.

The last two steps of the process are specified by the SAML Artifact Profile.

3 Single Sign-on

Figure 3 illustrates how single sign-on works in this scheme. After initial log into the first AA, the end user is seamlessly logged into any other AA of equal or lower authentication levels as needed. For privacy considerations, the end user is required to take an explicit action to opt into single sign-on for the current browser session.

Step 1 begins with an end user who has already logged into one application trying to access a second AA. In Step 2, the new AA redirects the end user to the Portal with its own AAid in the query string. Since the end user has already authenticated, the end user possesses a Portal cookie that indicates which CS was selected earlier. Since the AA provides the application identifier, and the Portal cookie provides the CS selection, the Portal can immediately redirect the end user to the CS (Step 3), as described in the previous section, without requesting any further information from the end user. In Step 4, the CS reads the cookie



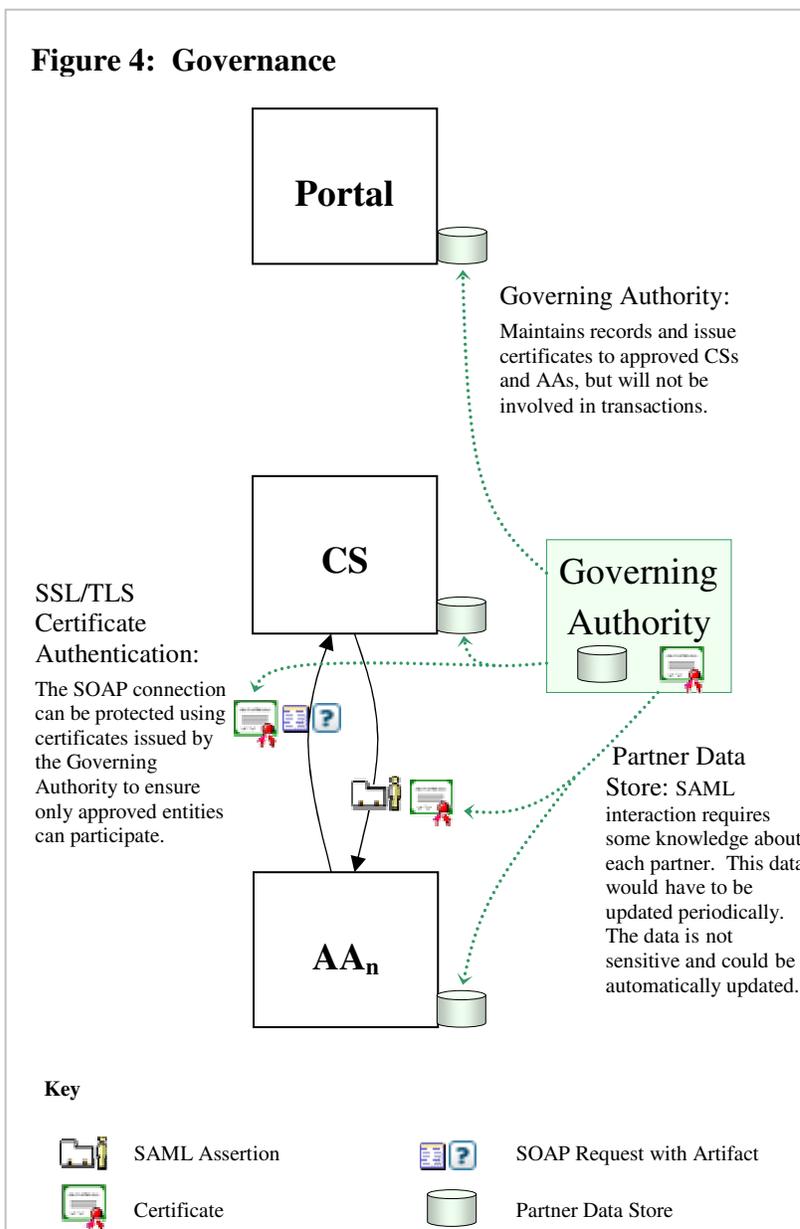
it assigned when it originally authenticated the end user to determine the end user's identity without requesting another authentication. Once the cookie is deciphered, the end user is redirected with the SAML Artifact as described in the previous section. Once again, there is no need to request any further information from the end user. Optionally, the CS could notify the end user that she is about to be logged into the AA and provide an opportunity to decline.

Finally, in Step 5, the end user ends up back at the AA, but this time with the SAML Artifact included in the query string. The AA can then use the Artifact to retrieve the SAML assertions from the CS, authenticating the end user. The redirects by the Portal and CS should be extremely fast, and be nearly imperceptible to the end user. The end user has simply typed or clicked on the Uniform Resource Locator (URL) of the AA and started to use it without needing to log in again.

4 Governance

Any architecture for government-wide authentication must provide some mechanism for the government to assert its authority over which entities can participate. This section describes those mechanisms for this scheme.

The SAML specification allows for the retrieval of CS assertions by an AA over a PKI authenticated Secure Sockets Layer (SSL)/Transport Layer Security (TLS) channel. A Governing Authority established by the government issues the PKI certificates, effectively controlling which entities can participate. Any CS attempting to make assertions without an appropriate certificate would not be trusted by AAs. Similarly, AAs attempting to retrieve assertions from CSs will not be trusted without the appropriate certificates. These certificates will be issued, renewed, or revoked periodically as determined by the Governing Authority. To simplify configuration, separate certification authorities (CAs) will be used for each assurance level.



SAML exchanges between two parties require each entity to have some knowledge about the other, such as partner identifiers and Simple Object Access Protocol (SOAP) URLs. The Governing Authority will maintain an authoritative copy of this information and make it available to the CSs and AAs. This information is not sensitive and not expected to change very often. Periodically, CSs and AAs will have to download the data and update their configurations, ideally automatically. The SAML specification is silent on the distribution of this information, the government will have to determine and document this mechanism. It is unlikely that Commercial off the Shelf (COTS) products will support this functionality natively; custom modules will probably be required.

The Governing Authority is not involved in authentication transactions; they will focus on the policy and assessment tasks. AAs and CSs will interact directly with each other for daily authentication transactions using their government issued certificates.

Appendix A: Session Reset

In some cases, an AA may want to re-authenticate after a time period (e.g., if the end user has been idle for a while and the AA wants to confirm that the end user is still at the machine, or the AA needs to do a particularly sensitive transaction, or the AA just wants a maximum time before re-authenticating). The SAML assertion from the CS contains a timestamp for the assertion as well as the authentication instant, so an AA can determine the time of authentication through the assertion. If an AA requires re-authentication, the architecture provides a mechanism known as session reset. The session reset requires the CS to re-authenticate the end user, even if the CS's own policies would not require a re-authentication at that time (e.g., the CS requires re-authentication every four hours, but the AA require it every two hours).

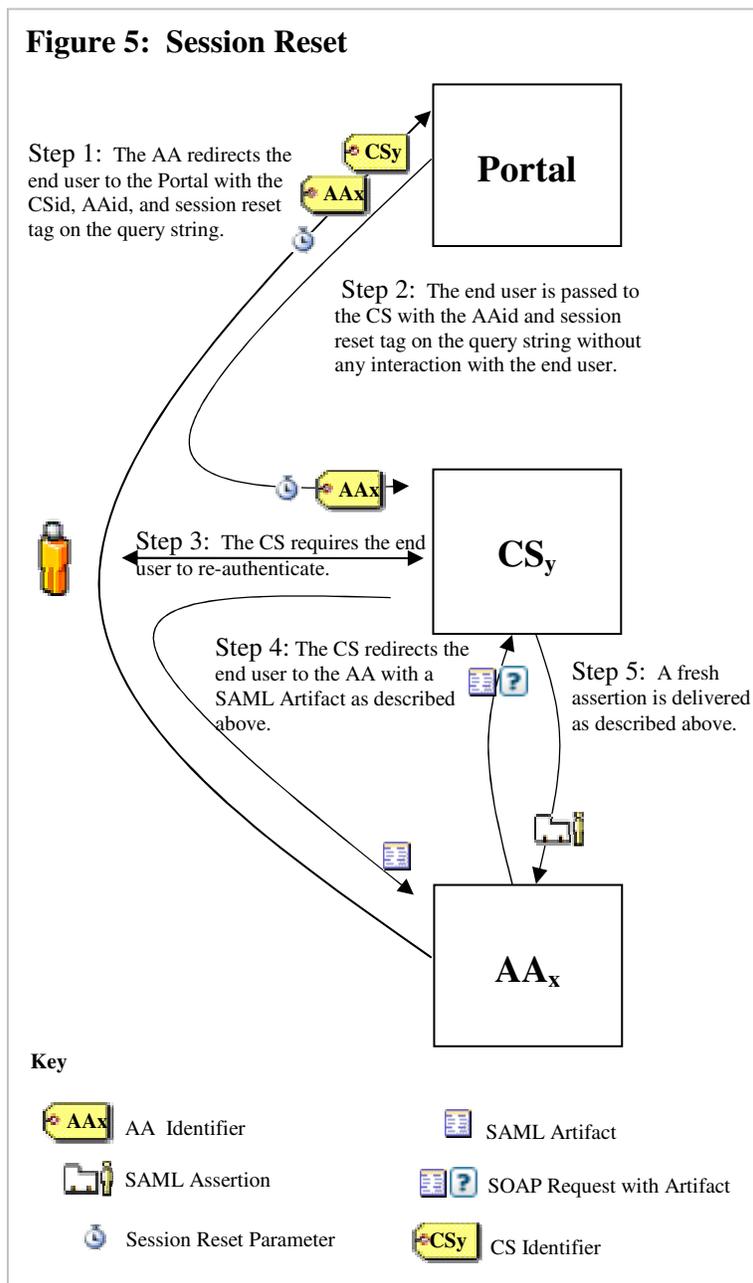


Figure 5 shows the chain of events for a session reset, which begins after the AA has received an assertion from the CS. If the AA wants a more recent authentication, it can request a session reset by redirecting the end user back to the Portal to re-authenticate. The redirection must include the CSid, the AAid, and the session reset identifier, as shown in Step 1. The Portal then redirects the end user to the CS with the AAid and session reset identifier in Step 2. The CS requires the end user to re-authenticate when the session reset parameter is present, shown in Step 3. Steps 4 and 5 follow the standard SAML Artifact Profile hand-off previously described.

The mechanism accounts for disparate and potentially incompatible session management policies by allowing individual AAs to require a reset of the end user's session with the selected CS. In order to take advantage of this functionality, the AA must be capable of inspecting the authentication instant field of the SAML assertion.

Appendix B: Glossary and Acronyms

Term	Definition
Agency Application (AA)	An online service provided by a government agency that requires a end user to be authenticated.
Certificate	X.509v3 digital certificates in a Public Key Infrastructure (PKI) for authentication, and can be used at any assurance level.
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.
Credential Service (CS)	A service of a Credential Service Provider (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 Provider (CSP)	An organization that offers one or more CSs. Sometimes known as an Electronic Certificate Provider (ECP).
E-Authentication Portal (Portal)	A website that helps an end user locate the CSs and AAs needed for completing transactions. The Portal also maintains information about CSs and AAs 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.
Governing Authority	Established by the government to issue certificates that allow Agency Applications to retrieve SAML assertions from CS over a client and server authenticated SSL channel, effectively controlling which entities can participate.
SAML Artifact	A SAML artifact of "small" bounded size is carried as part of a URL query string such that, when the artifact is conveyed to the source site, the artifact unambiguously references an assertion. The artifact is conveyed via redirection to the destination site, which then acquires the referenced assertion by some further steps. Typically, this involves the use of a registered SAML protocol binding. This technique is used in the browser/artifact profile of SAML.
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.
SAML Assertion	A piece of data produced by a SAML authority regarding either

Term	Definition
	an act of authentication performed on a subject, attribute information about the subject, or authorization permissions applying to the subject with respect to a specified resource.
Scheme	Schemes, such as SAML and Liberty, specify protocols and standards for federated identity mechanisms for different entities to share identities without requiring the end user to manage multiple accounts.
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 that's transferred over the SSL connection.
Security Assertion Markup Language (SAML)	XML-based framework for ensuring that transmitted communications are secure. SAML defines mechanisms to exchange authentication, authorization and nonrepudiation information, allowing single sign-on capabilities for Web services.
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 the end user's hard drive, but is only stored in temporary memory that is erased when the browser is closed.
Session Reset Parameter	Present on the query string, indicating that a re-authentication is requested.
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	After initial authentication with a Credential Service during a browser session, the end user is seamlessly logged into any other Agency Application of equal or lower authentication levels. For privacy considerations, the end user is required to take an explicit action to opt into single sign-on.
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.

Acronym	Abbreviation For
AA	Agency Application
AAid	Agency Application Identifier
ASC	Authentication Service Component
AWG	Architecture Working Group
CA	Certificate Authority
COTS	Commercial off the Shelf
CS	Credential Service
CSid	Credential Service Identifier
E-RA	Electronic Risk & Requirements Analysis
NIST	National Institute for Standards and Technology
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
RA	Registration Authority
RC	Release Candidate
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
SP	Special Publication
SSL	Secure Sockets Layer
TBD	To Be Determined
TLS	Transport Layer Security
URL	Uniform Resource Locator

Appendix C: Document History

Document History

Status	Release	Date	Comment	Audience
Pilot	0.0.1	11/3/03	Initial draft of the document, adapted from proposed SAML artifact architecture document proven in the E-Authentication Interoperability Lab.	Limited
RC1	1.0.0	05/17/04	<p>1) Added sentence describing “explicit opt-in”. (AWG Bullet 57)</p> <p>2) Diagram and text added to describe session reset. (AWG Bullet 18)</p> <p>3) Spelling of eAuthentication changed to E-Authentication.</p> <p>4) Added Glossary section to define terms. (AWG Bullet 12 & 64)</p>	Limited
RC2	1.0.0	05/26/04	<p>1) In section 3, step numbers were added to text describing figure 2.</p> <p>2) http://www.cio.gov/E-Authentication link changed to http://www.cio.gov/eauthentication.</p> <p>3) Inserted an additional paragraph into section 1 to introduce SAML and PKI as the two components for authentication.</p> <p>4) Added document reference callouts to the documents diagram in section 1.</p> <p>5) Dropped Appendix B, it's now handling in a more generic fashion in the Technical Approach.</p> <p>6) Added acronym list to Appendix B.</p>	Limited
RC3	1.0.0	06/28/04	<p>1) Document titles (NIST SP 800-63, OMB M-04-04) added to the document diagram.</p> <p>2) Session Reset Token changed to Session Reset Parameter.</p> <p>3) Figure 4 title changed to Session Reset, and the figure key formatting issue was fixed.</p> <p>4) Certification Authority definition added to the glossary.</p>	Limited

