E-Authentication Glossary and Acronyms

1 Introduction

The purpose of this document is to identify terms and acronyms that can be found in documents produced by the E-Authentication Program Management Office and may be specific to the E-Authentication Identity Federation. The document is divided into two sections: Glossary and Acronyms.

2 Glossary

Term	Definition
Acceptance Test	Testing that each member system must complete to demonstrate compliance with all applicable Federation specifications and requirements. The acceptance testing approach differs between assertion-based systems and certificate-based systems. The E-Authentication Lab conducts assertion-based system acceptance testing, with Federation Member assistance as necessary. The Federation Member conducts certificate-based system acceptance testing using test procedures available from GSA.
Activation	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.
Address of Record	The official location where an individual can be found. The address of record always includes the residential street address of an individual and may also include the mailing address of the individual. In very limited circumstances, an Army Post Office box number, Fleet Post Office box number or the street address of next of kin or of another contact individual can be used when a residential street address for the individual is not available.
Adopted Scheme	Precisely scoped identity scheme accepted for use by the Federation.
Application Federated Service	A single relying party application behind an E-Authentication Enterprise Federated Service.
Approval	In context of E-Authentication Federation participation - authority to operate.
Approved	Acceptance by the E-Auth PMO to participate in the E-Authentication Identity Federation, or other inclusion or use in the E-Authentication Federation.
Architecture Framework	The Authentication Service Component (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.

Term	Definition
Assertion	A piece of data or statement provided by a CS to an RP regarding either an act of authentication performed on an end user, attribute information about the end user, or authorization data applying to the end user with respect to a specified resource. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol.
Assessment Package	A package of requested information submitted to GSA by CSPs who have been accepted for Credential Assessment. The package contains evidence of compliance with all applicable criteria.
Assurance Level	Level of trust, as defined by the OMB Guidance M-04-04 for E-Authentication. This guidance describes four identity authentication assurance levels for e-government transactions. Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. Assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. The four levels of assurance are: • Level 1: Little or no confidence in the asserted identity's validity. • Level 2: Some confidence in the asserted identity's validity. • Level 3: High confidence in the asserted identity's validity. • Level 4: Very high confidence in the asserted identity's validity.
Asymmetric Keys	Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.
Attribute	A single, specific piece of information. An example of an identity attribute is a name or date of birth.
Authentication	The process of establishing confidence in user identities. 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 the user 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 Protocol	A well specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.

Term	Definition
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 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. Member systems (i.e., agency applications and credential services) are integrated into the ASC, and technically interoperate with each other as necessary, in accordance with configuration settings. Member systems that are operational nodes in the production ASC are visible and accessible to end users, as appropriate, which allows end users to conduct transactions.
Authentication Session	Period of time that an end user remains trusted after authentication. Typically a credential service 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. The Application maintains full control over authorization.
Boarded	The point at which potential Federation prospect (CSP or RP application becomes a Federation Member because of the successful completion of all boarding checklist items.
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.
Certificate-based Member System	A Member system that issues or relies upon a public key digital certificate to identify an end user.
Certification Authority (CA)	A certification authority is the body 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.
Certificate Authority (CA) Hint Lists	The Federal PKI Policy Authority has established a "hint list" to assist the user in selecting an appropriate credential. This "hint list" contains Certificate Authority (CA) names (i.e., the issuer's domain name) that is sent to the user's web browser in the Certificate Request message of an SSL/TLS session during session establishment when PKI-based client authentication is required.

Term	Definition
Change Control Board (CCB)	The CCB is the E-Authentication PMO's governance entity empowered to review and approve changes to the production ASC.
Change Proposal	A change proposal is submitted to the CCB requesting approval to integrate the candidate's system into the production ASC.
Claimant	A party whose identity is to be verified using an authentication protocol.
CLIN	Contract Line Item Number
CO, ACO, COR	Contract Officer, Assistant Contract Officer, and Contract Officer's Representative (also referred to in some agency's as the COTR)
Common Domain Cookie (CDC)	Browser cookie used to track CSs authenticated to by the end user during a particular browser session. CSs read and update the CDC. RPs read the CDC.
Compatible	Two Federation Member systems may technically interoperate if: • The CS has an equal or higher assurance level than the RP, • The CS is can provide all optional attributes required by the RP, and • The CS and RP use the same interface specification version, or a scheme translator is available
Cookie (Transient Cookie)	A message given to a web browser (e.g., end user's web browser) by an 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 document uses "credential" broadly, referring to both electronic credentials and tokens.
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 Credential Assessment Framework (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.
Credential Assessment Profile (CAP)	A list of related criteria used to assess the Assurance Level of a Credential Service.
Credential Service (CS)	A service from CSP that provides electronic 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.

Term	Definition
Credential Service Provider (CSP)	A trusted entity that registers, creates, issues and administers identity tokens and electronic credentials to subscribers. The CSP may encompass Registration Authorities and verifiers that it operates. A CSP may be an independent third party such as a bank, educational institution or insurance company or a Government agency. The entity may issue credentials for its own use and extend for use on government online services.
Cryptographic Key	A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, keys must provide at least 80-bits of protection. This means that it must be as hard to find an unknown key or decrypt a message, given the information exposed to an eavesdropper by an authentication, as to guess an 80-bit random number.
Cryptographic Strength	A measure of the expected number of operations required to defeat a cryptographic mechanism. For the purposes of this document, this term is defined to mean that breaking or reversing an operation is at least as difficult computationally as finding the key of an 80-bit block cipher by key exhaustion that is it requires at least on the order of 279 operations.
Cryptographic Token	A token where the secret is a cryptographic key.
Cryptography	The discipline which embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification; prevent its unauthorized use or a combination thereof. [ANSI X9.31] Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and transformation of ciphertext into plaintext by decryption. [NIST SP 800-2]
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-Authentication Interoperability Lab (Lab)	The Lab conducts conformance testing of candidate systems to meet Federation interface specifications.
E-Authentication Program Management Office (PMO)	The PMO is the organization that performs E-Authentication program management, administration, and operations. All contracts, licensing, and participation agreements related to the Federation are executed and managed by the PMO under the General Services Administration (GSA).
E-GCA-Certificate (E-GCA Cert)	Public key certificate(s) issued to an assertion-based credential service and an assertion-based relying party. The certificates are issued by the E-Governance Certification Authorities, and are used by assertion-based nodes technically interoperating with each other to sign and encrypt messages as necessary. Test E-GCA certificates are required for sandbox testing and acceptance testing. Production E-GCA certificates are required for operation in the production ASC.

Term	Definition
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.
Electronic Credentials	Digital documents used in authentication that bind an identity or an attribute to a subscriber's token. Synonym: credential
Electronic Risk and Requirements Assessment (E-RA)	This is the tool that the E-Authentication Solution offers customer agencies to use to assess the authentication risks for its government IT systems (i.e., RPs). E-RA is fully aligned with the OMB M-04-04 E-Authentication Guidance. This approach identifies the risks associated with insufficient authentication of users, and it forms the basis for the definition of authentication requirements.
End User	Any citizen, Government employee, contractor, or business that uses a relying party application.
Enterprise Approach	The integration of a single agency-wide identity management service (Agency Portal) with the Federation, rather than integrating individual applications. Agency Portals consolidate authentication and policy enforcement for many applications within an organization.
Enterprise Federated Service (EFS):	An application hosting an E-Authentication service with several relying party applications behind the service. The application behind the hosted E-Authentication solution would use a vendor product single sign-on technology to move seamlessly from the centralized relying party to the subsequent applications.
Entropy	A measure of the amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits. Guessing entropy is a measure of the difficulty that an attacker has to guess the average password used in a system. When a password has n-bits of guessing entropy then an attacker has as much difficulty guessing the average password as in guessing an n-bit random quantity. The attacker is assumed to know the actual password frequency distribution.
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).

Term	Definition
Federal Identity and Credentialing Committee (FICC)	The FICC will make policy recommendations and develop the Federal Identity Credentialing Component of the Federal Enterprise Architecture, to include associated services (identity proofing, credential management, etc.), for the Federal Government. Objectives are: • Simplify and Unify Identity Authentication for Federal Employees • Create requirements for Physical Credentials, electronic credentials, and issuance. • Develop the Federal Identity Credentialing Component of the Federal Enterprise Architecture
Federal Public Key Infrastructure (FPKI)	Employs a Bridge Certification Authority to harmonize policies and procedures for CAs. See http://www.cio.gov/fpkipa/.
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The FPKI Policy Authority sets policy governing operation of the FBCA and approves applicants for cross certification with the FBCA. The FBCA allows discrete Public Key Infrastructures (PKI) to trust digital certificates issued by other entities that have been policy mapped and cross-certified with the FBCA. The FPKI PA is composed of organizations that wish to interoperate and exchange digital certificates that have been signed by their Certification Authority with the FBCA. Determinations by the FPKI Policy Authority apply to the issuance of cross-certificates to approved participants but does not prescribe how those entities are to rely on digital certificates for transactions; all entities are free to accept or reject any digital certificate issued by any other entity at their sole discretion, using available FPKI Policy Authority determinations to assist in making informed decisions.
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
Federated Identity Credential Services (FIDCS)	The suite of services as defined in this solicitation.
Federation Change Management	Policies and processes agreed to by Federation Members to review, approve, and roll out architecture changes to production.
Federation Membership List	The E-Authentication PMO maintains a Federation Membership List that includes RPs and CSs that have been evaluated for use by the Federal Government. Each RP on the Federation Membership List is assessed to a particular Assurance Level as defined by the OMB and NIST Guidance documents.
Federation Portal (Portal)	A website that helps end users locate the CSs and Relying Party application 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.
Flexible	Capable of being changed.

Term	Definition
Governing Authority	Established by the government to issue certificates that allow Agency Applications to retrieve SAML assertions from Credential Services over a client and server authenticated SSL channel, effectively controlling which entities can participate.
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.
Identity	A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique.
Identity Proofing	The process by which a CSP and an RA validate sufficient information to uniquely identify a person.
Integration	Including a Federation Member system into the production ASC so that it is visible to and usable by end users. Integration requires configuration of systems, as appropriate, to ensure proper communication between Federation Member systems.
Liberty Alliance Project	An organization with global membership that provides a comprehensive approach to identity through open standards, business and deployment guidelines and best practices for managing privacy. See http://www.projectLiberty Alliance.org
Lightweight Directory Access Protocol (LDAP)	An application protocol for querying and modifying directory services running over TCP/IP
Local (Certificate) Validation	Validation without use of an external service. Local validation products are usually installed on the same machine as the RP application and integrated into the application by way of a vendor supplied plug-in. The application may be a server-based application, such as a web server (e.g., IIS, Apache). The local validation product is dedicated to the application, or alternatively, to a set of related applications. Administration of local validation products is generally conducted by the application owner.
Managed (Hosted) Validation Service	Managed or ‘hosted’ validation services are administered by a third party service provider. The service provider supplies the application owner with a plug-in for the application, which offloads all or part of certificate validation to the hosted validation service. Managed validation services usually serve many applications from many different organizations.
Managed Validation and Translation Service (MVTS)	The Managed Validation and Translation Service is offered by the Federation, providing both Managed Validation Service and Step Down scheme translation that allows use of higher assurance PKI certificates at lower assurance assertion-based relying party systems.

Term	Definition
Managed Validation/Translation Service and Support (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.
Node	Synonym for “Federation Member system” in context of rolling out the system to or operating the system in the production Authentication Service Component (ASC) federated network of interconnected systems (nodes).
OASIS	The Organization for the Advancement of Structured Information Standards (OASIS) oversees SAML.
Online Certificate Status Protocol (OCSP)	An on-line protocol used to determine the status of a public key certificate. See [RFC 2560].
Open Systems Interconnection Basic Reference Model (OSI Model)	A layered, abstract description for communications and computer network protocol design. (*OSI Reference Model* or *OSI Model* for short)
Password	A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. See also PIN.
Path Discovery and Validation (PDVal)	Process by which an application determines the authenticity of a certificate. Path discovery entails building a chain of trust (i.e., path) from the relying party back to one ore more trusted certificate authorities (CAs). This chain of trust is composed of certificates from a series of related CAs. A certification path begins with a trusted CA and ends with a target certificate.

Term	Definition
Personal Identification Number (PIN)	A password consisting only of decimal digits.
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.
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.
Possession and control of a token	The ability to activate and use the token in an authentication protocol.
Proof of Possession (PoP) protocol	A protocol where a claimant proves to a verifier that he/she possesses and controls a token (e.g., a key or password).
Protocol	An agreed-upon format for communication between two ends points.
Protocol Run	An instance of the exchange of messages between a claimant and a verifier in a defined authentication protocol that results in the authentication (or authentication failure) of the claimant.
Public Key Certificate	A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. See www.ieft.org/rfc/rfc3280.txt.
Public Key Infrastructure (PKI)	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. 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 integrates digital certificates, public key cryptography, and certification authorities into a complete network security architecture. A typical PKI infrastructure 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
Registration	The process through which an end user applies to become a subscriber of a CSP and an RA validates the identity of that user on behalf of the CSP.

Term	Definition
Registration Authority	A trusted entity that establishes and vouches for the identity of a subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).
Relationship Manager (RM)	Individual in the PMO who works directly with Agency customers to acquire business and deploy services
Reliable	The trustworthiness a system to do what it is expected or designed to do.
Relying Party (RP) (Agency application, AA)	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.
Relying Party (RP)	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 reference 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
Sandbox Testing	The purpose of this testing is for a potential Federation Member to learn how to implement their system in accordance with Federation technical specifications. This is a learning experience meant to flush out issues and questions that can then be addressed and resolved early in the process, prior to engaging the Federation Lab for acceptance testing. Sandbox testing is conducted in an environment provided by the Federation. .
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.

Term	Definition
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)	An XML-based framework for communicating user authentication, entitlement and attribute information. SAML allows entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or an application. 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.
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.
Shared Secret	A secret used in authentication that is known to the claimant (user) and the verifier. There are two durations for a shared secret: • Session (temporary) secret – duration of the secret is limited to the duration of the user session. That is, the secret is created, used, and expired during a single user authentication session. • Long-term secret – duration of the secret persists ongoing, and is used from one user authentication session to another user authentication session.
Shibboleth	Standards-based, open source middleware software which provides Web Single Sign-n (SSO) across or within organizational boundaries. The Shibboleth software implements the OASIS SAML v1.1 specification, providing a federated Single Sign-on 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/
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.

Term	Definition
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 (SSO)	Once an end user has authenticated their identity at a CS, he or she may, by their choice, move among RPs compatible with the CS without re-authenticating. In other words, the end user is seamlessly logged into any other RP compatible with the CS. For privacy considerations, end users must take explicit actions to opt-in to SSO. SSO applies to assertion based Federation member systems only. In addition, SSO is in effect only for the duration of the end user's current browser session and authentication session. An end user must opt-in to SSO each time he or she opens a new web browser session. The ASC supports SSO as a core aspect of the federated architecture.
Subject	The person whose identity is bound in a particular credential.
Subscriber	A party who receives a credential or token from a CSP and becomes a claimant in an authentication protocol.
Technology Neutral	Not favoring a particular technology. This is the basis of the E-Authentication 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.
Transactions	Transaction: an interaction whereby an identity authentication is being attempted between a CSP and RP. Successful Transaction Level 1 & 2: a successfully delivered assertion from a CSP to an RP, regardless of any authorization decisions made by the RP. Failed Transaction Level 1 & 2: any assertion sent to an RP determined by the CSP to not have been successfully received by the RP. Validation Service Transaction: A successfully delivered response (positive or negative) from the service to the RP communicating the status of the presented certificate, regardless of any authorization decisions made by the application. Translation Service Transaction: a successfully delivered assertion to the RP as a result of a valid certificate from the Translation service, regardless of any authorization decisions made by the application. EAF-SAAS Transaction: a successfully delivered assertion from a CSP to the hosted RP service, regardless of any authorization decisions made by the application.

Term	Definition
Transaction Identifier (TID)	Mechanism for tracking transactions across various components in the architecture. TIDs will be generated by the E-Authentication Portal for SAML 1.0 and will be passed with the end user information, via query string, as they are redirected from (1) the Portal to CSs, (2) from CSs to RP Applications, and, (3) once generated by the Portal, to the Portal by RP Application 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. See www.ietf.org.
Trust List	A list of CAs that can be trusted in order to validate certificates issued by CAs external to the Relying Party application. The list is maintained and managed such that the certificates that are validated are carefully pre-screened for appropriate use within the environment of the relying party. By nature, trust lists require regular maintenance. In some cases, this can present scalability challenges. It is necessary to maintain the trust list so that compromised or obsolesced CAs are removed from the trust list, and new CAs are added to the trust list, as appropriate.
U. S. E-Authentication Identity Federation (Federation)	The Federation includes policy and standards, business rules, an architectural framework, credential services, relying parties, service delivery and acquisition, and a financial model for Federal government agencies. The Federation provides the ability for government agencies to rely on credentials issued and managed by other organizations – within and outside the Federal government.
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 AA).
Validation Service (MV)	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 Agency application).
Verified Name	A subscriber name that has been verified by identity proofing.
Verifier	An entity that verifies the claimant's identity by verifying the claimant's possession of a token using an authentication protocol. To do this, the verifier may also need to validate credentials that link the token and identity and check their status.
Web Browser	Web browsers communicate with web servers primarily using HTTP (hypertext transfer protocol) to obtain web pages. 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.

Term	Definition
x.509 Certificate Policy	This specification profiles the format and semantics of certificates and certificate revocation lists (CRLs) for the Internet PKI. For details visit http://www.ietf.org/rfc/rfc2459.txt or http://www.ietf.org/rfc/rfc3280.txt
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.

3 Acronyms

Acronym	Definition
AA	Agency Application
AAID	Agency Application Identifier
ANSI	American National Standards Institute
AS	Adopted Scheme
ASC	Authentication Service Component
ATO	Approval to Operate
AuthZ	Authorization
CA	Certification Authority
CAF	Credential Assessment Framework
CAP	Credential Assessment Profile
CCB	Change Control Board
CD	Compact Disc
CDC	Common Domain Cookie
COTS	Commercial off the Shelf
CP	Certification Policy
CS	Credential Service
CSA	Certification Status Authority
CSid	Credential Service Identifier
CSP	Credential Service Provider
DAA	Designated Approving Authority
DNS	Domain Name Service
EA	European Co-operation For Accreditation
EETP	End Entity Test Procedures
E-GCA	E-Government Certification Authorities
E-RA	Electronic Risk and Requirements Assessment
ESC	Executive Steering Committee
FBCA	Federal Bridge Certification Authority
FEA	Federal Enterprise Architecture
FICC	Public Key Infrastructure
FIDCS	Federated Identity Credential Services
FIPS	Federal Information Processing Standard
FMD	Federation Membership Documents

Acronym	Definition
FMDS	Federation Member Document Suite
FOC	Federation Operations Center
FPKI	Federal Public Key Infrastructure
FPKI OA	Federal Public Key Infrastructure Operational Authority
FPKI PA	Federal Public Key Infrastructure Policy Authority
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive #12
HTTP	Hyper Text Transfer Protocol
IdM	Identity Management
ISO	International Organization For Standardization
LOA	Letter of Authorization
MD SSO	Multi-Domain Single Sign-On
MVTS	Managed Validation/Translation Service
NIST	National Institute Of Standards And Technology
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OMB	Office Of Management And Budget
PDVal	Path Discovery and Validation
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
POC	Point of Contact(s)
PoP	Proof of Possession
RA	Registration Authority
RC	Release Candidate
RP	Relying Party
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAML	Security Assertion Markup Language
SAS	Statement On Auditing Standards
SCVP	Simple Certificate Validation Protocol
SOP	Standard Operating procedures
SORN	System of Records Notice
SP	Special Publication
SRS	Systems Requirements Specification
SSL	Secure Socket Layer
SSO	Single Sign-on
TBD	To Be Determined
TLS	Transport Layer Security
TWG	Technical Working Group
UI	User Interface
URL	Uniform Resource Locator
WS	Web Services
XKMS	XML Key Management Specifications

Acronym	Definition
XML	Extensible Markup Language