COMMONWEALTH OF VIRGINIA

~~Information Technology Resource Management~~IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (~~ITRM~~IMSAC)

GUIDANCE DOCUMENT
Digital Identity ~~Electronic Authentication~~Assertions

~~Virginia Information Technologies Agency (VITA)~~

Table of Contents

Formatted: Font: 5 pt

1 Publication Version Control

The following table contains a history of revisions to this publication.

Publication Version	Date	Revision Description
1.0	~~07/20~~10/12/2016	Initial Draft of Document

Formatted Table

2 Reviews

- The initial version of the document was prepared by staff from the Virginia Information Technologies Agency (VITA) for the Secretary of Technology, under the direction from the Identity Management Standards Advisory Council (IMSAC).~~The initial version of the document was prepared by the staff analysts for the Identity Management Standards Advisory Council, within Commonwealth Data Governance, Enterprise Architecture, Virginia Information Technologies Agency.~~

Formatted: List Paragraph, Indent: Left: 0", Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Normal, No bullets or numbering

- The document will be reviewed in a manner compliant with the Commonwealth of Virginia's Administrative Process Act, § 2.2-4000 et seq.~~The document will be reviewed in a manner compliant with the Commonwealth of Virginia's ITRM Policies, Standards, and Guidelines and §2.2-437.C, *Code of Virginia*:~~

Formatted: List Paragraph, Indent: Left: 0", Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

- ~~*Proposed guidance documents and general opportunity for oral or written submittals as to those guidance documents shall be posted on the Virginia Regulatory Town Hall and published in the Virginia Register of Regulations as a general notice following the processes and procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§2.2-4000 et seq.). The Advisory Council [IMSAC] shall allow at least 30 days for the submission of written comments following the posting and publication and shall hold at least one meeting dedicated to the receipt of oral comment no less than 15 days after the posting and publication. The Advisory Council shall also develop methods for the identification and notification of interested parties and specific means of seeking input from interested persons and groups. The Advisory Council shall send a copy of such notices,*~~

~~*comments, and other background material relative to the development of the recommended guidance documents to the Joint Commission on Administrative Rules.*~~

Formatted: Font: Italic

Formatted: Indent: Left: 0"

3 Purpose and Scope

Pursuant to § 2.2-436 and § 2.2-437, *Code of Virginia*, this guidance document was developed by the Identity Management Standards Advisory Council (IMSAC), on behalf of the Secretary of Technology, to establish minimum specifications for Digital Identity Systems so as to warrant liability protection pursuant to the Electronic Identity Management Act ("the Act"), Chapter 50 of Title 59.1. The guidance document, as defined in § 2.2-4001, was prepared to provide information or guidance of general applicability to the public for interpreting or implementing the Act. The guidance document was not developed as a Commonwealth of Virginia Information Technology Resource Management (ITRM) Policy, Standard, and Guideline, pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive branch agencies of the Commonwealth of Virginia.

Formatted: Indent: Left: 0"

~~3~~4 Statutory Authority

The following section documents the statutory authority established in the *Code of Virginia* for the development of minimum specifications and standards for Assertions within a Digital Identity System. References to statutes below and throughout this document shall be to the *Code of Virginia*, unless otherwise specified.

Governing Statutes:

Secretary of Technology

§ 2.2-225. Position established; agencies for which responsible; additional powers
http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225/

Identity Management Standards Advisory Council

§ 2.2-437. Identity Management Standards Advisory Council
http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/

Commonwealth Identity Management Standards

§ 2.2-436. Approval of electronic identity standards
http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/

Electronic Identity Management Act

Chapter 50. Electronic Identity Management Act
http://law.lis.virginia.gov/vacode/title59.1/chapter50/

~~The following section documents the statutory authority established in the *Code of Virginia* for the development of minimum specifications and standards for electronic authentication. References to statutes below and throughout this document shall be to the *Code of Virginia*, unless otherwise specified.~~

~~Governing Statutes:~~

~~Secretary of Technology~~

~~§ 2.2-225. Position established; agencies for which responsible; additional powers~~
~~http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-225~~

~~Secretary of Transportation~~

~~§ 2.2-225. Position established; agencies for which responsible; additional powers~~
~~http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-225~~

~~Identity Management Standards Advisory Council~~
~~§ 2.2-437. Identity Management Standards Advisory Council~~
~~http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/~~

~~Commonwealth Identity Management Standards~~
~~§ 2.2-436. Approval of electronic identity standards~~
~~http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/~~

~~Electronic Identity Management Act~~
~~Chapter 50. Electronic Identity Management Act~~
~~http://law.lis.virginia.gov/vacode/title59.1/chapter50/~~

~~Chief Information Officer (CIO) of the Commonwealth~~
~~§ 2.2-2007. Powers of the CIO~~
~~http://lis.virginia.gov/cgi-bin/legp604.exe?000+cod+2.2-2007~~

~~Virginia Information Technologies Agency~~
~~§ 2.2-2010. Additional powers of VITA~~
~~http://lis.virginia.gov/cgi-bin/legp604.exe?000+cod+2.2-2010~~

45 Definitions

Terms used in this document comply with definitions in the Public Review version of the National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3), and align with adopted definitions in § 59.1-550, *Code of Virginia* (COV), and the Commonwealth of Virginia's ITRM Glossary (ITRM Glossary). [1]

Active Attack: An online attack where the attacker transmits data to the claimant, credential service provider, verifier, or relying Participant. Examples of active attacks include man-in-the-middle, impersonation, and session hijacking.

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.

Approved: Federal Information Processing Standard (FIPS) approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation.

Applicable Law: Laws, statutes, regulations, and rules of the jurisdiction in which the members of an Identity Trust Framework operates.

Applicant: A Participant undergoing the processes of Registration and Identity Proofing.

Assertion: A statement from a verifier to a relying Participant (RP) that contains identity information about a Subscriber. Assertions may also contain verified attributes.

Assertion Reference: A data object, created in conjunction with an Assertion, which identifies the verifier and includes a pointer to the full Assertion held by the verifier.

Assurance: In the context of [OMB M-04-04][2] and this document, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an 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.

[1] NIST SP 800-63-3 may be accessed at https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3 . At the time of the publication of this document, NIST SP 800-63-3 was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3.
§ 59.1-550, *Code of Virginia*, may be accessed at http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550/
The Commonwealth's ITRM Glossary may be accessed at http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/PSG_Sections/COV_ITRM_Glossary.pdf

[2] [OMB M-04-04] Office of Management and Budget, Memorandum 04-04: E-Authentication Guidance for Federal Agencies, accessible at https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf.

Formatted: Font: 9 pt

Formatted: Default Paragraph Font, Font: 9 pt

Assurance Model: Policies, processes, and protocols that define how Assurance will be established in an Identity Trust Framework.

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.

Attack: An attempt by an unauthorized individual to fool a verifier or a relying Participant into believing that the unauthorized individual in question is the Subscriber.

Attacker: A Participant who acts with malicious intent to compromise an Information System.

Attribute: A claim of a named quality or characteristic inherent in or ascribed to someone or something.

Authentication: The process of establishing confidence in the identity of users or Information Systems.

Authentication Protocol: A defined sequence of messages between a claimant and a verifier that demonstrates that the claimant has possession and control of a valid authenticator to establish his/her identity, and optionally, demonstrates to the claimant that he or she is communicating with the intended verifier.

Authentication Protocol Run: An exchange of messages between a claimant and a verifier that results in authentication (or authentication failure) between the two Participants.

Authentication Secret: A generic term for any secret value that could be used by an attacker to impersonate the Subscriber in an authentication protocol. These are further divided into short-term authentication secrets, which are only useful to an attacker for a limited period of time, and long-term authentication secrets, which allow an attacker to impersonate the Subscriber until they are manually reset. The authenticator secret is the canonical example of a long term authentication secret, while the authenticator output, if it is different from the authenticator secret, is usually a short term authentication secret.

Authenticator: Something that the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. In previous versions of this guideline, this was referred to as a token.

Authenticator Assurance Level (AAL): A metric describing robustness of the authentication process proving that the claimant is in control of a given Subscriber's authenticator(s).

Authenticator Output: The output value generated by an authenticator. The ability to generate valid authenticator outputs on demand proves that the claimant possesses and controls the authenticator. Protocol messages sent to the verifier are dependent upon the authenticator output, but they may or may not explicitly contain it.

Authenticator Secret: The secret value contained within an authenticator.
Authenticity: The property that data originated from its purported source.

Bearer Assertion: An Assertion that does not provide a mechanism for the Subscriber to prove that he or she is the rightful owner of the Assertion. The RP has to assume that the Assertion was issued to the Subscriber who presents the Assertion or the corresponding Assertion reference to the RP.

Bit: A binary digit: 0 or 1.

Biometrics: Automated recognition of individuals based on their behavioral and biological characteristics. In this document, biometrics may be used to unlock authenticators and prevent repudiation of Registration.

Certificate Authority (CA): A trusted entity that issues and revokes public key certificates.

Certificate Revocation List (CRL): A list of revoked public key certificates created and digitally signed by a Certificate Authority. [RFC 5280][3]

Challenge-Response Protocol: An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a secret (such as by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the verifier. The verifier can independently verify the response generated by the claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the claimant possesses and controls the secret.

Claimant: A Participant whose identity is to be verified using an authentication protocol.
Claimed Address: The physical location asserted by an individual (e.g. an applicant) where he/she can be reached. It includes the residential street address of an individual and may also include the mailing address of the individual. For example, a person with a foreign passport, living in the U.S., will need to give an address when going through the Identity Proofing process. This address would not be an "address of record" but a "claimed address."

Claimed Identity: A declaration by the applicant of their current Personal Name, date of birth and address. [GPG45][4]

[3] [RFC 5280] Official Internet Protocol Standards, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008, accessible at http://www.rfc-editor.org/info/rfc5280.

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA): An interactive feature added to web-forms to distinguish use of the form by humans as opposed to automated agents. Typically, it requires entering text corresponding to a distorted image or from a sound stream.

Cookie: A character string, placed in a web browser's memory, which is available to websites within the same Internet domain as the server that placed them in the web browser.

Credential: An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to an authenticator possessed and controlled by a Subscriber. While common usage often assumes that the credential is maintained by the Subscriber, this document also uses the term to refer to electronic records maintained by the CSP which establish a binding between the Subscriber's authenticator(s) and identity.

Credential Service Provider (CSP): A trusted entity that issues or registers Subscriber authenticators and issues electronic credentials to Subscribers. The CSP may encompass Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third Participant, or may issue credentials for its own use.

Cross Site Request Forgery (CSRF): An attack in which a Subscriber who is currently authenticated to an RP and connected through a secure session, browses to an attacker's website which causes the Subscriber to unknowingly invoke unwanted actions at the RP. For example, if a bank website is vulnerable to a CSRF attack, it may be possible for a Subscriber to unintentionally authorize a large money transfer, merely by viewing a malicious link in a webmail message while a connection to the bank is open in another browser window.

Cross Site Scripting (XSS): A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user supplied data from requests or forms without sanitizing the data so that it is not executable.

Cryptographic Key: A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, key requirements must meet the minimum requirements stated in Table 2 of NIST SP 800-57 Part 1. See also Asymmetric keys, Symmetric key.

Cryptographic Authenticator: An authenticator where the secret is a cryptographic key.

[4] [GPG 45] UK Cabinet Office, Good Practice Guide 45, Identity proofing and verification of an individual, November 3, 2014, accessible at https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual.

Data Integrity: The property that data has not been altered by an unauthorized entity.

Derived Credential: A credential issued based on proof of possession and control of an authenticator associated with a previously issued credential, so as not to duplicate the Identity Proofing process.

Digital Identity System: An Information System that supports Electronic Authentication and the management of a person's Identity in a digital environment. [Referenced in § 59.1-550, COV]

Digital Signature: An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation.

Eavesdropping Attack: An attack in which an attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the claimant.

Electronic Authentication: The process of establishing confidence in user identities electronically presented to an Information System.

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.

Extensible Mark-up Language (XML): Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them.

Federal Bridge Certification Authority (FBCA): The FBCA is the entity operated by the Federal Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI Policy Authority to create, sign, and issue public key certificates to Principal CAs.

Federal Information Security Management Act (FISMA): Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and Information Systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Federal Information Processing Standard (FIPS): Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.[5]

Federation: A process that allows for the conveyance of identity and authentication information across a set of networked systems. These systems are often run and controlled by disparate Participants in different network and security domains. [NIST SP 800-63C]

Governance Authority: Entity responsible for providing policy level leadership, oversight, strategic direction, and related governance activities within an Identity Trust Framework.

Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:

- (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and
- (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.

Holder-of-Key Assertion: An Assertion that contains a reference to a symmetric key or a public key (corresponding to a private key) held by the Subscriber. The RP may authenticate the Subscriber by verifying that he or she can indeed prove possession and control of the referenced key.

Identity: A set of attributes that uniquely describe a person within a given context.

Identity Assurance Level (IAL): A metric describing degree of confidence that the applicant's claimed identity is their real identity.

Identity Proofing: The process by which a CSP and a Registration Authority (RA) collect and verify information about a person for the purpose of issuing credentials to that person.

Identity Provider (IdP): The party that manages the subscriber's primary authentication credentials and issues Assertions derived from those credentials generally to the credential service provider (CSP).

Identity Trust Framework: A Digital Identity System with established identity, security, privacy, technology, and enforcement rules and policies adhered to by certified identity providers that are members of the Identity Trust Framework. Members of an Identity Trust Framework include Identity Trust Framework operators and identity providers. Relying Participants may be, but are not required to be, a member of an Identity Trust Framework in order to accept an identity credential issued by a certified identity provider to verify an identity credential holder's identity. [§ 59.1-550, COV]

[5] Federal Information Processing Standard (FIPS), accessible at http://www.nist.gov/itl/fips.cfm.

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [NIST Interagency/Internal Report (IR) 7298 r. 2]

Kerberos: A widely used authentication protocol developed at MIT. In “classic” Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to- KDC exchange. Longer password length and complexity provide some mitigation to this vulnerability, although sufficiently long passwords tend to be cumbersome for users.

Knowledge Based Authentication: Authentication of an individual based on knowledge of information associated with his or her claimed identity in public databases. Knowledge of such information is considered to be private rather than secret, because it may be used in contexts other than authentication to a verifier, thereby reducing the overall assurance associated with the authentication process.

Man-in-the-Middle Attack (MitM): An attack on the authentication protocol run in which the attacker positions himself or herself in between the claimant and verifier so that he can intercept and alter data traveling between them.

Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection, but not non-repudiation protection.

Multi-Factor: A characteristic of an authentication system or an authenticator that uses more than one authentication factor. The three types of authentication factors are something you know, something you have, and something you are.

Network: An open communications medium, typically the Internet, that is used to transport messages between the claimant and other Participants. Unless otherwise stated, no assumptions are made about the security of the network; it is assumed to be open and subject to active (i.e., impersonation, man-in-the-middle, session hijacking) and passive (i.e., eavesdropping) attack at any point between the Participants (e.g., claimant, verifier, CSP or RP).

Nonce: A value used in security protocols that is never repeated with the same key. For example, nonces used as challenges in challenge-response authentication protocols must not be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable.

Off-line Attack: An attack where the attacker obtains some data (typically by eavesdropping on an authentication protocol run or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing.

Online Attack: An attack against an authentication protocol where the attacker either assumes the role of a claimant with a genuine verifier or actively alters the authentication channel.

Online Guessing Attack: An attack in which an attacker performs repeated logon trials by guessing possible values of the authenticator output.

Operational Authority: Entity responsible for operations, maintenance, management, and related functions of an Identity Trust Framework.

Participant Requirements: A set of rules and policies in an Identity Trust Framework addressing identity, security, privacy, technology, and enforcement, which are assigned to each member type in a Digital Identity System. Member types include Registration Authorities (RAs), Identity Providers (IdPs), Credential Service Providers (CSPs), Verifiers, and Relying Parties (RPs). [§ 59.1-550, COV]

Passive Attack: An attack against an authentication protocol where the attacker intercepts data traveling along the network between the claimant and verifier, but does not alter the data (i.e., eavesdropping).

Password: A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings.

Personal Identification Number (PIN): A password consisting only of decimal digits.

Personal Identity Verification (PIV) Card: Defined by [FIPS 201] as a physical artifact (e.g., identity card, smart card) issued to federal employees and contractors that contains stored credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

Personally Identifiable Information (PII): As defined by OMB Circular A-130, Personally Identifiable Information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Pharming: An attack in which an attacker corrupts an infrastructure service such as DNS (Domain Name Service) causing the Subscriber to be misdirected to a forged verifier/RP, which could cause the Subscriber to reveal sensitive information, download harmful software or contribute to a fraudulent act.

Phishing: An attack in which the Subscriber is lured (usually through an email) to interact with a counterfeit verifier/RP and tricked into revealing information that can be used to masquerade as that Subscriber to the real verifier/RP.

Physical In-Person: Method of Identity Proofing in which Applicants are required to physically present themselves and identity evidence to a representative of the Registration Authority or Identity Trust Framework. [NIST SP 800-63-2]

Possession and control of an authenticator: The ability to activate and use the authenticator in an authentication protocol.

Practice Statement: A formal statement of the practices followed by the Participants to an authentication process (i.e., RA, CSP, or verifier). It usually describes the policies and practices of the Participants and can become legally binding.

Private Credentials: Credentials that cannot be disclosed by the CSP because the contents can be used to compromise the authenticator.

Private Key: The secret part of an asymmetric key pair that is used to digitally sign or decrypt data.

Protected Session: A session wherein messages between two participants are encrypted and integrity is protected using a set of shared secrets called session keys. A participant is said to be authenticated if, during the session, he, she or it proves possession of a long term authenticator in addition to the session keys, and if the other Participant can verify the identity associated with that authenticator. If both participants are authenticated, the protected session is said to be mutually authenticated.

Pseudonymous Identifier: A meaningless, but unique number that does not allow the RP to infer the Subscriber but which does permit the RP to associate multiple interactions with the Subscriber’s claimed identity.

Public Credentials: Credentials that describe the binding in a way that does not compromise the authenticator.

Public Key: The public part of an asymmetric key pair that is used to verify signatures or encrypt data.

Public Key Certificate: A digital document issued and digitally signed by the private key of a Certificate 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 also [RFC 5280].

Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration: The process through which an applicant applies to become a Subscriber of a CSP and an RA validates the identity of the applicant on behalf of the CSP.

Registration Authority (RA): A trusted entity that establishes and vouches for the identity or attributes 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).

Relying Party (RP): An entity that relies upon the Subscriber's authenticator(s) and credentials or a verifier's Assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.

Remote: (As in remote authentication or remote transaction) An information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single organization's security controls. Note: Any information exchange across the Internet is considered remote.

Replay Attack: An attack in which the attacker is able to replay previously captured messages (between a legitimate claimant and a verifier) to masquerade as that claimant to the verifier or vice versa.

Risk Assessment: The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.

Salt: A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker.

Secondary Authenticator: A temporary secret, issued by the verifier to a successfully authenticated Subscriber as part of an Assertion protocol. This secret is subsequently used, by the Subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer Assertions, Assertion references, and Kerberos session keys.

Secure Sockets Layer (SSL): An authentication and security protocol widely implemented in browsers and web servers. SSL has been superseded by the newer Transport Layer Security (TLS) protocol; TLS 1.0 is effectively SSL version 3.1.

Security Assertion Mark-up Language (SAML): An XML-based security specification developed by the Organization for the Advancement of Structured Information Standards (OASIS) for exchanging authentication (and authorization) information between trusted entities over the Internet.

SAML Authentication Assertion: A SAML Assertion that conveys information from a verifier to an RP about a successful act of authentication that took place between the verifier and a Subscriber.

Session Hijack Attack: An attack in which the attacker is able to insert himself or herself between a claimant and a verifier subsequent to a successful authentication exchange between the latter two Participants. The attacker is able to pose as a Subscriber to the verifier or vice versa to control session data exchange. Sessions between the claimant and the relying Participant can also be similarly compromised.

Shared Secret: A secret used in authentication that is known to the claimant and the verifier.

Social Engineering: The act of deceiving an individual into revealing sensitive information by associating with the individual to gain confidence and trust.

Special Publication (SP): A type of publication issued by NIST. Specifically, the Special Publication 800-series reports on the Information Technology Laboratory's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

Strongly Bound Credentials: Credentials that describe the binding between a user and authenticator in a tamper-evident fashion.

Subscriber: A Participant who has received a credential or authenticator from a CSP.

Symmetric Key: A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.

Token: See Authenticator.

Token Authenticator: See Authenticator Output.

Token Secret: See Authenticator Secret.

Transport Layer Security (TLS): An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by [RFC 5246]. TLS is similar to the older Secure Sockets Layer (SSL) protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations specifies how TLS is to be used in government applications.

Trust Anchor: A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g. in a public key certificate).

Unverified Name: A Subscriber name that is not verified as meaningful by Identity Proofing.

Valid: In reference to an ID, the quality of not being expired or revoked.

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 and control of one or two authenticators using an authentication protocol. To do this, the verifier may also need to validate credentials that link the authenticator(s) and identity and check their status.

Verifier Impersonation Attack: A scenario where the attacker impersonates the verifier in an authentication protocol, usually to capture information that can be used to masquerade as a claimant to the real verifier.

Virtual In-Person Proofing: A remote identity person proofing process that employs technical and procedural measures that provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing encounter. [NIST SP 800-63A]

Weakly Bound Credentials: Credentials that describe the binding between a user and authenticator in a manner than can be modified without invalidating the credential.

Zeroize: Overwrite a memory location with data consisting entirely of bits with the value zero so that the data is destroyed and not recoverable. This is often contrasted with deletion methods that merely destroy reference to data within a file system rather than the data itself.

Zero-knowledge Password Protocol: A password based authentication protocol that allows a claimant to authenticate to a Verifier without revealing the password to the verifier. Examples of such protocols are EKE, SPEKE and SRP.~~Terms used in this document comply with definitions in the Public Review version of the National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3), and align with adopted definitions in § 59.1-550, *Code of Virginia*, and the Commonwealth of Virginia's ITRM Glossary (ITRM Glossary).~~ ~~[6]~~

~~Active Attack: An online attack where the attacker transmits data to the claimant, credential service provider, verifier, or relying party. Examples of active attacks include man-in-the-middle, impersonation, and session hijacking.~~

~~[6] NIST SP 800-63-3 may be accessed at https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3 . At the time of the publication of this document, NIST SP 800-63-3 was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3.~~
~~§ 59.1-550, *Code of Virginia*, may be accessed at http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550/~~
~~The Commonwealth's ITRM Glossary may be accessed at~~
~~http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/PSG_Sections/COV_ITRM_Glossary.pdf~~

~~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.~~

~~Approved: Federal Information Processing Standard (FIPS) approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation.~~

~~Applicant: A party undergoing the processes of registration and identity proofing.~~

~~Assertion: A statement from a verifier to a relying party (RP) that contains identity information about a subscriber. Assertions may also contain verified attributes.~~

~~Assertion Reference: A data object, created in conjunction with an assertion, which identifies the verifier and includes a pointer to the full assertion held by the verifier.~~

~~Assurance: In the context of [OMB M-04-04][7] and this document, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an 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.~~

~~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.~~

~~Attack: An attempt by an unauthorized individual to fool a verifier or a relying party into believing that the unauthorized individual in question is the subscriber.~~

~~Attacker: A party who acts with malicious intent to compromise an information system.~~

~~Attribute: A claim of a named quality or characteristic inherent in or ascribed to someone or something.~~

~~Authentication: The process of establishing confidence in the identity of users or information systems.~~

~~Authentication Protocol: A defined sequence of messages between a claimant and a verifier that demonstrates that the claimant has possession and control of a valid authenticator to~~

~~[7] [OMB M-04-04] Office of Management and Budget, Memorandum 04-04: E-Authentication Guidance for Federal Agencies, accessible at https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf.~~

~~establish his/her identity, and optionally, demonstrates to the claimant that he or she is communicating with the intended verifier.~~

~~Authentication Protocol Run: An exchange of messages between a claimant and a verifier that results in authentication (or authentication failure) between the two parties.~~

~~Authentication Secret: A generic term for any secret value that could be used by an attacker to impersonate the subscriber in an authentication protocol. These are further divided into short-term authentication secrets, which are only useful to an attacker for a limited period of time, and long-term authentication secrets, which allow an attacker to impersonate the subscriber until they are manually reset. The authenticator secret is the canonical example of a long term authentication secret, while the authenticator output, if it is different from the authenticator secret, is usually a short term authentication secret.~~

~~Authenticator: Something that the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. In previous versions of this guideline, this was referred to as a token.~~

~~Authenticator Assurance Level (AAL): A metric describing robustness of the authentication process proving that the claimant is in control of a given subscriber's authenticator(s).~~

~~Authenticator Output: The output value generated by an authenticator. The ability to generate valid authenticator outputs on demand proves that the claimant possesses and controls the authenticator. Protocol messages sent to the verifier are dependent upon the authenticator output, but they may or may not explicitly contain it.~~

~~Authenticator Secret: The secret value contained within an authenticator.~~
~~Authenticity: The property that data originated from its purported source.~~

~~Bearer Assertion: An assertion that does not provide a mechanism for the subscriber to prove that he or she is the rightful owner of the assertion. The RP has to assume that the assertion was issued to the subscriber who presents the assertion or the corresponding assertion reference to the RP.~~

~~Bit: A binary digit: 0 or 1.~~

~~Biometrics: Automated recognition of individuals based on their behavioral and biological characteristics. In this document, biometrics may be used to unlock authenticators and prevent repudiation of registration.~~

~~Certificate Authority (CA): A trusted entity that issues and revokes public key certificates.~~

~~Certificate Revocation List (CRL): A list of revoked public key certificates created and digitally signed by a Certificate Authority. [RFC 5280]~~[8]

~~Challenge-Response Protocol: An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a secret (such as by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the verifier. The verifier can independently verify the response generated by the claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the claimant possesses and controls the secret.~~

~~Claimant: A party whose identity is to be verified using an authentication protocol.~~

~~Claimed Address: The physical location asserted by an individual (e.g. an applicant) where he/she can be reached. It includes the residential street address of an individual and may also include the mailing address of the individual. For example, a person with a foreign passport, living in the U.S., will need to give an address when going through the identity proofing process. This address would not be an "address of record" but a "claimed address."~~

~~Claimed Identity: A declaration by the applicant of their current Personal Name, date of birth and address. [GPG45]~~[9]

~~Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA): An interactive feature added to web-forms to distinguish use of the form by humans as opposed to automated agents. Typically, it requires entering text corresponding to a distorted image or from a sound stream.~~

~~Cookie: A character string, placed in a web browser's memory, which is available to websites within the same Internet domain as the server that placed them in the web browser.~~

~~Credential: An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to an authenticator possessed and controlled by a subscriber. While common usage often assumes that the credential is maintained by the subscriber, this document also uses the term to refer to electronic records maintained by the CSP which establish a binding between the subscriber's authenticator(s) and identity.~~

~~[8] [RFC 5280] Official Internet Protocol Standards, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008, accessible at http://www.rfc-editor.org/info/rfc5280.~~

~~[9] [GPG 45] UK Cabinet Office, Good Practice Guide 45, Identity proofing and verification of an individual, November 3, 2014, accessible at https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual.~~

~~Credential Service Provider (CSP): A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. The CSP may encompass Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.~~

~~Cross Site Request Forgery (CSRF): An attack in which a subscriber who is currently authenticated to an RP and connected through a secure session, browses to an attacker's website which causes the subscriber to unknowingly invoke unwanted actions at the RP. For example, if a bank website is vulnerable to a CSRF attack, it may be possible for a subscriber to unintentionally authorize a large money transfer, merely by viewing a malicious link in a webmail message while a connection to the bank is open in another browser window.~~

~~Cross Site Scripting (XSS): A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user supplied data from requests or forms without sanitizing the data so that it is not executable.~~

~~Cryptographic Key: A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, key requirements shall meet the minimum requirements stated in Table 2 of NIST SP 800-57 Part 1. See also Asymmetric keys, Symmetric key.~~

~~Cryptographic Authenticator: An authenticator where the secret is a cryptographic key.~~

~~Data Integrity: The property that data has not been altered by an unauthorized entity.~~

~~Derived Credential: A credential issued based on proof of possession and control of an authenticator associated with a previously issued credential, so as not to duplicate the identity proofing process.~~
~~Digital Signature: An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation.~~

~~Eavesdropping Attack: An attack in which an attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the claimant.~~

~~Electronic Authentication: The process of establishing confidence in user identities electronically presented to an information system.~~

~~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.~~

~~Extensible Mark-up Language (XML): Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them.~~

~~Federal Bridge Certification Authority (FBCA): The FBCA is the entity operated by the Federal Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI Policy Authority to create, sign, and issue public key certificates to Principal CAs.~~

~~Federal Information Security Management Act (FISMA): Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.~~

~~Federal Information Processing Standard (FIPS): Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.~~[~~10~~]

~~Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:~~

- ~~(One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and~~
- ~~(Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.~~

~~Holder-of-Key Assertion: An assertion that contains a reference to a symmetric key or a public key (corresponding to a private key) held by the subscriber. The RP may authenticate the subscriber by verifying that he or she can indeed prove possession and control of the referenced key.~~

~~Identity: A set of attributes that uniquely describe a person within a given context.~~

~~Identity Assurance Level (IAL): A metric describing degree of confidence that the applicant's claimed identity is their real identity.~~

~~Identity Proofing: The process by which a CSP and a Registration Authority (RA) collect and verify information about a person for the purpose of issuing credentials to that person.~~

[~~10~~] ~~Federal Information Processing Standard (FIPS), accessible at http://www.nist.gov/itl/fips.cfm.~~

~~Kerberos: A widely used authentication protocol developed at MIT. In “classic” Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to- KDC exchange. Longer password length and complexity provide some mitigation to this vulnerability, although sufficiently long passwords tend to be cumbersome for users.~~

~~Knowledge Based Authentication: Authentication of an individual based on knowledge of information associated with his or her claimed identity in public databases. Knowledge of such information is considered to be private rather than secret, because it may be used in contexts other than authentication to a verifier, thereby reducing the overall assurance associated with the authentication process.~~

~~Man-in-the-Middle Attack (MitM): An attack on the authentication protocol run in which the attacker positions himself or herself in between the claimant and verifier so that he can intercept and alter data traveling between them.~~

~~Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection, but not non-repudiation protection.~~

~~Multi-Factor: A characteristic of an authentication system or an authenticator that uses more than one authentication factor. The three types of authentication factors are something you know, something you have, and something you are.~~

~~Network: An open communications medium, typically the Internet, that is used to transport messages between the claimant and other parties. Unless otherwise stated, no assumptions are made about the security of the network; it is assumed to be open and subject to active (i.e., impersonation, man-in-the-middle, session hijacking) and passive (i.e., eavesdropping) attack at any point between the parties (e.g., claimant, verifier, CSP or RP).~~

~~Nonce: A value used in security protocols that is never repeated with the same key. For example, nonces used as challenges in challenge-response authentication protocols must not be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable.~~

~~Off-line Attack: An attack where the attacker obtains some data (typically by eavesdropping on an authentication protocol run or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing.~~

~~Online Attack: An attack against an authentication protocol where the attacker either assumes the role of a claimant with a genuine verifier or actively alters the authentication channel.~~

~~Online Guessing Attack: An attack in which an attacker performs repeated logon trials by guessing possible values of the authenticator output.~~

~~Passive Attack: An attack against an authentication protocol where the attacker intercepts data traveling along the network between the claimant and verifier, but does not alter the data (i.e., eavesdropping).~~

~~Password: A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings.~~

~~Personal Identification Number (PIN): A password consisting only of decimal digits.~~

~~Personal Identity Verification (PIV) Card: Defined by [FIPS 201] as a physical artifact (e.g., identity card, smart card) issued to federal employees and contractors that contains stored credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).~~

~~Personally Identifiable Information (PII): As defined by OMB Circular A-130, Personally Identifiable Information means information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.~~

~~Pharming: An attack in which an attacker corrupts an infrastructure service such as DNS (Domain Name Service) causing the subscriber to be misdirected to a forged verifier/RP, which could cause the subscriber to reveal sensitive information, download harmful software or contribute to a fraudulent act.~~

~~Phishing: An attack in which the subscriber is lured (usually through an email) to interact with a counterfeit verifier/RP and tricked into revealing information that can be used to masquerade as that subscriber to the real verifier/RP.~~

~~Possession and control of an authenticator: The ability to activate and use the authenticator in an authentication protocol.~~

~~Practice Statement: A formal statement of the practices followed by the parties to an authentication process (i.e., RA, CSP, or verifier). It usually describes the policies and practices of the parties and can become legally binding.~~

~~Private Credentials: Credentials that cannot be disclosed by the CSP because the contents can be used to compromise the authenticator.~~

~~Private Key: The secret part of an asymmetric key pair that is used to digitally sign or decrypt data.~~

~~Protected Session: A session wherein messages between two participants are encrypted and integrity is protected using a set of shared secrets called session keys. A participant is said to be authenticated if, during the session, he, she or it proves possession of a long term authenticator in addition to the session keys, and if the other party can verify the identity associated with that authenticator. If both participants are authenticated, the protected session is said to be mutually authenticated.~~

~~Pseudonymous Identifier: A meaningless, but unique number that does not allow the RP to infer the subscriber but which does permit the RP to associate multiple interactions with the subscriber's claimed identity.~~

~~Public Credentials: Credentials that describe the binding in a way that does not compromise the authenticator.~~

~~Public Key: The public part of an asymmetric key pair that is used to verify signatures or encrypt data.~~

~~Public Key Certificate: A digital document issued and digitally signed by the private key of a Certificate 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 also [RFC 5280].~~

~~Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.~~

~~Registration: The process through which an applicant applies to become a subscriber of a CSP and an RA validates the identity of the applicant on behalf of the CSP.~~

~~Registration Authority (RA): A trusted entity that establishes and vouches for the identity or attributes 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).~~

~~Relying Party (RP): An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.~~

~~Remote: (As in remote authentication or remote transaction) An information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single organization's security controls. Note: Any information exchange across the Internet is considered remote.~~

~~Replay Attack: An attack in which the attacker is able to replay previously captured messages (between a legitimate claimant and a verifier) to masquerade as that claimant to the verifier or vice versa.~~

~~Risk Assessment: The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.~~

~~Salt: A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker.~~

~~Secondary Authenticator: A temporary secret, issued by the verifier to a successfully authenticated subscriber as part of an assertion protocol. This secret is subsequently used, by the subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer assertions, assertion references, and Kerberos session keys.~~

~~Secure Sockets Layer (SSL): An authentication and security protocol widely implemented in browsers and web servers. SSL has been superseded by the newer Transport Layer Security (TLS) protocol; TLS 1.0 is effectively SSL version 3.1.~~

~~Security Assertion Mark-up Language (SAML): An XML-based security specification developed by the Organization for the Advancement of Structured Information Standards (OASIS) for exchanging authentication (and authorization) information between trusted entities over the Internet.~~

~~SAML Authentication Assertion: A SAML assertion that conveys information from a verifier to an RP about a successful act of authentication that took place between the verifier and a subscriber.~~

~~Session Hijack Attack: An attack in which the attacker is able to insert himself or herself between a claimant and a verifier subsequent to a successful authentication exchange between the latter two parties. The attacker is able to pose as a subscriber to the verifier or vice versa to control session data exchange. Sessions between the claimant and the relying party can also be similarly compromised.~~

~~Shared Secret: A secret used in authentication that is known to the claimant and the verifier.~~

~~Social Engineering: The act of deceiving an individual into revealing sensitive information by associating with the individual to gain confidence and trust.~~

~~Special Publication (SP): A type of publication issued by NIST. Specifically, the Special Publication 800-series reports on the Information Technology Laboratory's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.~~

~~Strongly Bound Credentials: Credentials that describe the binding between a user and authenticator in a tamper-evident fashion.~~

~~Subscriber: A party who has received a credential or authenticator from a CSP.~~

~~Symmetric Key: A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.~~

~~Token: See Authenticator.~~

~~Token Authenticator: See Authenticator Output.~~

~~Token Secret: See Authenticator Secret.~~

~~Transport Layer Security (TLS): An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by [RFC 5246]. TLS is similar to the older Secure Sockets Layer (SSL) protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations specifies how TLS is to be used in government applications.~~

~~Trust Anchor: A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g. in a public key certificate).~~

~~Trust Framework: In identity management, means a digital identity system with established identity, security, privacy, technology, and enforcement rules and policies adhered to by certified identity providers that are members of the identity trust framework. Members of an identity trust framework include identity trust framework operators and identity providers. Relying parties may be, but are not required to be, a member of an identity trust framework in order to accept an identity credential issued by a certified identity provider to verify an identity credential holder's identity. [§ 59.1-550, Code of Virginia]~~

~~Unverified Name: A subscriber name that is not verified as meaningful by identity proofing.~~

~~Valid: In reference to an ID, the quality of not being expired or revoked.~~

~~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 and control of one or two authenticators using an authentication protocol. To do this, the verifier may also need to validate credentials that link the authenticator(s) and identity and check their status.~~

~~Verifier Impersonation Attack: A scenario where the attacker impersonates the verifier in an authentication protocol, usually to capture information that can be used to masquerade as a claimant to the real verifier.~~

~~Weakly Bound Credentials: Credentials that describe the binding between a user and authenticator in a manner than can be modified without invalidating the credential.~~

~~Zeroize: Overwrite a memory location with data consisting entirely of bits with the value zero so that the data is destroyed and not recoverable. This is often contrasted with deletion methods that merely destroy reference to data within a file system rather than the data itself.~~

~~Zero-knowledge Password Protocol: A password based authentication protocol that allows a claimant to authenticate to a Verifier without revealing the password to the verifier. Examples of such protocols are EKE, SPEKE and SRP.~~

~~5~~6 Background

In 2015, Virginia's General Assembly passed the Electronic Identity Management Act (Chapter 50 of Title 59.1, *Code of Virginia*) to address demand in the state's digital economy for secure, privacy enhancing ~~electronic authentication~~Electronic Authentication and identity management. Growing numbers of "communities of interest" have advocated for stronger, scalable and interoperable identity solutions to increase consumer protection and reduce liability for principal actors in the identity ecosystem – Identity Providers, Credential Service Providers and Relying Parties.

To address the demand contemplated by the Electronic Identity Management Act, the General Assembly also created the Identity Management Standards Advisory Council (IMSAC) to advise the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents, pursuant to §2.2-436. A copy of the IMSAC Charter has been provided in **Appendix 1**.~~The following guidance document has been developed by the Virginia Information Technologies Agency (VITA), acting on behalf of the Secretary of Technology and Chief Information Officer of the Commonwealth, at the direction of IMSAC. IMSAC was created by the General Assembly as part of the Act and advises the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to §2.2-436. A copy of the IMSAC Charter has been provided in **Appendix 1**.~~

The Advisory Council recommends to the Secretary of Technology guidance documents relating to (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions; (ii) the minimum specifications and standards that should be included in an ~~identity~~ Identity Trust Framework, as defined in §59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§59.1-550 et seq.); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in §59.1-550.

Purpose Statement

This guidance document, as defined in § 2.2-4001, was developed by the Identity Management Standards Advisory Council (IMSAC), on behalf of the Secretary of Technology, to provide information or guidance of general applicability to the public for interpreting or implementing the Electronic Identity Management Act. Specifically, the document establishes ~~The purpose of this document is to establish~~ minimum specifications for ~~electronic~~ Assertions ~~authentication within~~in ~~an identity management system~~a Digital Identity System. ~~The document assumes that the identity management system will be supported by a trust framework, compliant with~~

~~Applicable Law.[11]~~ The minimum specifications have been ~~stated based on language in~~designed to be conformant with NIST SP 800-63C~~-3~~.

The document defines ~~minimum requirements~~Assertion types, core components, presentation methods, security, and ~~process flows, assurance levels and~~ privacy ~~and security~~ provisions for Assertions ~~for electronic authentication~~. The document assumes that specific business, legal, and technical requirements for ~~electronic authentication~~Assertions will be established in the ~~Trust Framework~~Identity Trust Framework for each distinct ~~identity management system~~Digital Identity System, and that these requirements will be designed based on the Electronic Authentication model, Identity Assurance Level (IAL), and Authenticator Assurance Level (AAL) requirements for the system.

The document limits its focus to ~~electronic authentication~~Assertions. Minimum specifications for other components of ~~an identity management system~~a Digital Identity System ~~will be~~have been defined in separate IMSAC guidance documents in this series, pursuant to §2.2-436 and §2.2-437.

~~6~~7 Minimum Specifications

National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3) defines an "~~electronic authentication~~Assertion" in a Digital Identity System as "A statement from a verifier to a relying party (RP) that contains identity information about a Subscriber. Assertions may also contain verified attributes~~the process of establishing confidence in the identity of users or information systems~~."[12] Information ~~systems~~ Systems may use the authenticated identity to determine if that user is authorized to perform an electronic transaction.

This document establishes minimum specifications for ~~electronic authentication~~Assertions within a Digital Identity System conformant with, and using language from, NIST SP 800-63-3. However, the minimum specifications defined in this document have been developed to accommodate requirements for ~~electronic authentication~~Assertions established under other national and international standards.[13] The minimum specifications in this document also

~~[11] For the purpose of this guidance document, the term "Applicable Law" shall mean laws, statutes, regulations, and rules of the jurisdiction in which each participant in an identity management system~~ member of an Identity Trust Framework ~~operates.~~

[12] The Public Review version of National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3) may be accessed at https://pages.nist.gov/800-63-3/sp800-63-3.html. At the time of the publication of this document, NIST SP 800-63-3 was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3.

[13] The minimum specifications defined in this document align with the State Identity Credential and Access Management (SICAM) Guidance and Roadmap, published by the National Association of State Chief Information Officers (NASCIO): http://www.nascio.org/Portals/0/Publications/Documents/SICAM.pdf; and the Identity Ecosystem Framework (IDEF), published by the Identity Ecosystem Steering Group (IDESG): https://www.idesg.org/The-ID-Ecosystem/Identity-Ecosystem-Framework/IDEF-Core-Documents.

assume that specific business, legal, and technical requirements for ~~an identity management system~~a Digital Identity System will be documented in the ~~trust framework~~Identity Trust Framework for that system. Minimum specifications for other components of ~~an identity management system~~a Digital Identity System have been documented in separate guidance documents in the IMSAC series, pursuant to §2.2-436 and §2.2-437.

Electronic Authentication Model

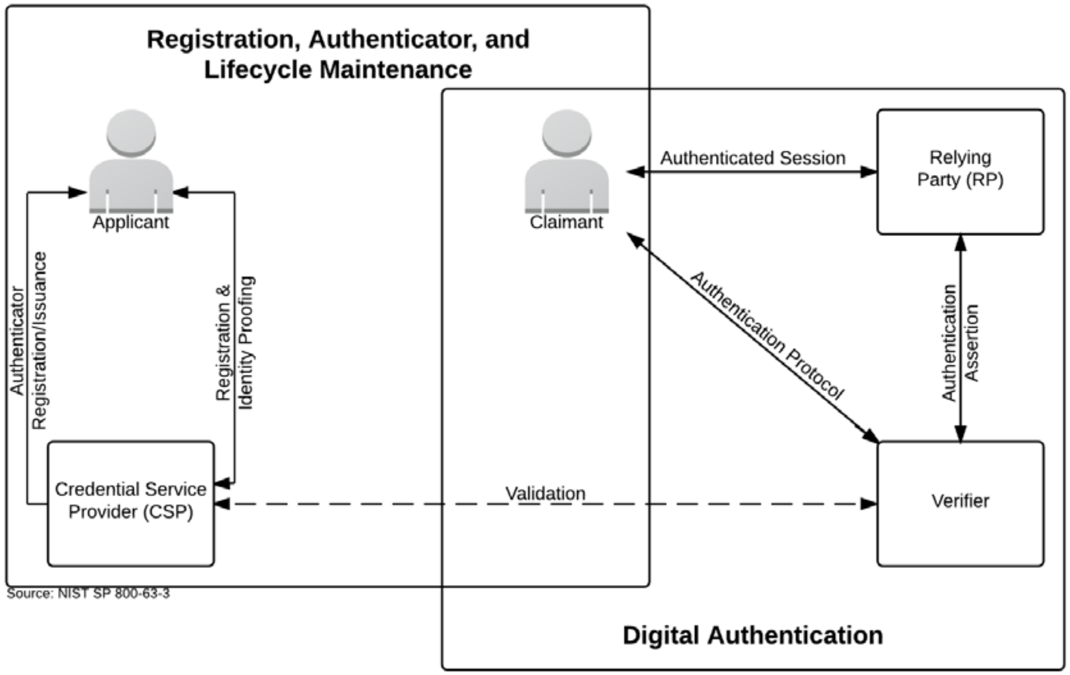
Assertions play an integral role in Electronic ~~authentication~~ Authentication, ~~is~~ the process of establishing confidence in individual identities presented to a ~~digital system~~Digital Identity System. Digital Identity S~~S~~ystems ~~can use~~implement Assertions as part of the process to authenticate a person's Identity. In turn, the authenticated identity ~~to~~ may be used to determine if that ~~individual~~ person is authorized to perform an online transaction. The minimum specifications in this document assume that the authentication and transaction take place across a network.

~~The electronic authentication model~~The minimum specifications for Assertions defined in this document reflect the Electronic Authentication model ~~defined in these minimum specifications reflects current technologies and architectures~~ used primarily by governmental entities. More complex models that separate functions among a broader range of parties are also available and may have advantages in some classes of applications. While a simpler model ~~has been defined in~~serves as the basis for these minimum specifications, it does not preclude ~~participant~~members in ~~identity management system~~Digital Identity Systems from separating these functions. Minimum specifications for the Electronic Authentication model reflected in this document have been defined in *IMSAC Guidance Document: Electronic Authentication*, and a graphic of the model has been shown in **Figure 1**.

Formatted: Font: Italic

Formatted: Font: Bold

Figure 1. Electronic Authentication Model



Source: NIST SP 800-63-3, accessible at https://pages.nist.gov/800-63-3/sp800-63-3.html

Note: Figure 1 illustrates the model for Electronic Authentication in a Digital Identity System, as documented in NIST SP 800-63-3 (Public Review), containing all components, requirements, and specifications recommended by IMSAC. However, the minimum specifications defined in this document have been developed to accommodate requirements for Assertions established under other national and international standards.

Formatted: Width: 11", Height: 8.5"

Formatted: Centered

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

Assertions

An Assertion contains a set of claims or statements about an authenticated Subscriber. Assertions can be categorized along multiple orthogonal dimensions, including the characteristics of using the Assertion or the protections on the Assertion itself.

The core set of claims inside an Assertion should include (but may not be limited to):

- Issuer: Identifier for the party that issued the Assertion (usually the IdP)
- Subject: Identifier for the party that the Assertion is about (the Subscriber), usually within the namespace control of the issuer (IdP)
- Audience: Identifier for the party intended to consume the Assertion, primarily the RP
- Issuance: Timestamp indicating when the Assertion was issued by the IdP
- Expiration: Timestamp indicating when the Assertion expires and will no longer be accepted as valid by the RP (Note: This is not the expiration of the session at the RP)
- Authentication Time: Timestamp indicating when the IdP last verified the presence of the Subscriber at the IdP through a primary Authentication event
- Identifier: Random value uniquely identifying this Assertion, used to prevent attackers from manufacturing malicious Assertions which would pass other validity checks

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

These core claims, particularly the issuance and expiration claims, apply to the Assertion about the Authentication event itself, and not to any additional Identity Attributes associated with the Subscriber, even when those claims are included within the Assertion. A Subscriber's Attributes may expire or be otherwise invalidated independently of the expiration or invalidation of the Assertion.

Assertions may include other additional Identity Attributes. Privacy requirements for presenting Attributes in Assertions have been provided below in this document. The RP may fetch additional Identity Attributes from the IdP in a separate transaction using an authorization Credential issued alongside the Assertion.

Although details vary based on the exact Authentication or federation protocols in use, an Assertion should be used only to represent a single log-in event at the RP. After the RP consumes the Assertion, session management at the RP comes into play and the Assertion is no longer used directly. The expiration of the Assertion must not represent the expiration of the session at the RP.

Assertion Possession Category

An Assertion can be classified based on whether possession of the Assertion itself is sufficient for representing the subject of the Assertion, or if additional proof is necessary alongside the Assertion.

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

Holder-of-Key Assertions

A Holder-of-Key Assertion contains a reference to a Symmetric Key or a Public Key (corresponding to a Private Key) possessed by and representing the Subscriber. An RP may decide when to require the Subscriber to prove possession of the key, depending on the policy of the RP. However, the RP must require the Subscriber to prove possession of the key that is referenced in the Assertion in parallel with presentation of the Assertion itself in order for the Assertion to be considered Holder-Of-Key. Otherwise, an Assertion containing reference to a key which the user has not proved possession of will be considered a Bearer Assertion.

The key referenced in a Holder-of-Key represents the Subscriber, not the client. This key may be distinct from any key used by the Subscriber to Authenticate to the IdP. In proving possession of the Subscriber's secret, the Subscriber also proves with a certain degree of assurance that they are the rightful subject of the Assertion. It is more difficult for an attacker to use a stolen Holder-of-Key Assertion issued to a Subscriber, since the attacker would need to steal the referenced key material as well.

Note that the reference to the key material in question is asserted by the issuer of the Assertion as are any other claims therein, and reference to a given key must be trusted at the same level as all other claims within the Assertion itself. The Assertion must not include an unencrypted Private or Symmetric Key to be used with Holder-of-Key presentation.

Bearer Assertions

A bearer Assertion can be presented by any party as proof of the bearer's identity, without reference to external materials. If an attacker is able to capture or manufacture a valid Assertion representing a Subscriber, and that attacker is able to successfully present that Assertion to the RP, then the attacker will be able to impersonate the Subscriber at that RP.

Note that mere possession of a bearer Assertion is not always enough to impersonate a Subscriber. For example, if an Assertion is presented in the indirect federation model (Section 6.1), additional controls may be placed on the transaction (such as identification of the RP and Assertion injection protections) that help to further protect the RP from fraudulent activity.

Assertion Protection Category

Regardless of the possession mechanism used to obtain them, Assertions must include an appropriate set of protections to the Assertion data itself to prevent attackers from manufacturing valid Assertions or re-using captured Assertions at disparate RPs.

Assertion Identifier

Assertions must contain sufficient Entropy to prevent an attacker from manufacturing a valid Assertion and using it with a target RP. Assertions may accomplish this by use of an embedded Nonce, timestamp, Assertion identifier, or a combination of these or other techniques. In the

Formatted: Font: 13 pt

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

absence of additional Cryptographic protections, this source of randomness must function as a shared secret between the IdP and the RP to uniquely identify the Assertion in question.

Signed Assertion

Assertions may be Cryptographically signed by the IdP, and the RP must validate the signature of each such Assertion based on the IdP's key. This signature must cover all vital fields of the Assertion, including its issuer, audience, subject, expiration, and any unique identifiers.

The signature may be asymmetric based on the published Public Key of the IdP. In such cases, the RP may fetch this Public Key in a secure fashion at runtime (such as through an HTTPS URL hosted by the IdP), or the key may be provisioned out of band at the RP (during configuration of the RP). The signature may be symmetric based on a key shared out of band between the IdP and the RP. In such circumstances, the IdP must use a different shared key for each RP. All signatures must use approved signing methods.

Encrypted Assertion

Assertions may be encrypted in such a fashion as to allow only the intended audience to decrypt the claims therein. The IdP must encrypt the payload of the Assertion using the RP's Public Key. The IdP may fetch this Public Key in a secure fashion at runtime (such as through an HTTPS URL hosted by the RP), or the key may be provisioned out of band at the IdP (during registration of the RP). All encrypted objects must use approved encryption methods.

Audience Restriction

All Assertions should use audience restriction techniques to allow an RP to recognize whether or not it is the intended target of an issued Assertion. All RPs must check the audience of an Assertion, if provided, to prevent the injection and replay of an Assertion generated for one RP at another RP.

Pairwise Pseudonymous Identifiers

In some circumstances, it is desirable to prevent the Subscriber's account at the IdP from being linked through one or more RPs through use of a common identifier. In these circumstances, pairwise Pseudonymous Identifiers must be used within the Assertions generated by the IdP for the RP, and the IdP must generate a different identifier for each RP. (See Pairwise Pseudonymous Identifier Generation for more information.)

When unique Pseudonymous Identifiers are used with RPs alongside of Identity Attribute bundles, it may still be possible for multiple colluding RPs to fully identify and correlate a Subscriber across Digital Identity Systems using these attributes. For example, given that two independent RPs will each see the same Subscriber identified with a different pairwise Pseudonymous Identifier, the RPs could still determine that the Subscriber is the same person by comparing their name, email address, Physical Address, or other identifying Attributes carried alongside the pairwise Pseudonymous Identifier. Privacy policies may prohibit such correlation, but pairwise Pseudonymous Identifiers can increase effectiveness of these policies by increasing the administrative effort in managing the Attribute correlation.

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

Note that in a proxied federation model, ultimate IdP may be unable to generate a pairwise Pseudonymous Identifier for the ultimate RP, since the proxy could blind the IdP from knowing which RP is being accessed by the Subscriber. In such situations, the pairwise Pseudonymous Identifier is usually between the IdP and the federation proxy itself. The proxy, acting as an IdP, can itself provide pairwise Pseudonymous Identifiers to downstream RPs. Depending on the protocol, the federation proxy may need to map the pairwise Pseudonymous Identifiers back to the associated identifiers from upstream IdPs in order to allow the Identity protocol to function. In such cases, the proxy will be able to track and determine which pairwise Pseudonymous Identifiers represent the same Subscriber at different RPs.

Pairwise Pseudonymous Identifier Generation

Pairwise Pseudonymous Identifiers must be opaque and unguessable, containing no identifying information about the Subscriber. Additionally, the identifiers must only be known by and used by one IdP-RP pair. An IdP may generate the same identifier for a Subscriber at multiple RPs at the request of those RPs, but only if:

- Those RPs have a demonstrable relationship that justifies an operational need for the correlation, such as a shared security domain or shared legal ownership, and
- All RPs sharing an identifier consent to being correlated in such a manner.

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

The RPs must conduct a privacy risk assessment to consider the privacy risks associated with requesting a common identifier. The IdP must ensure that only intended RPs are correlated; otherwise, a rogue RP could learn of the Pseudonymous Identifier for a correlation by fraudulently posing as part of that correlation.

Assertion Presentation

Formatted: Font: 13 pt

Assertions may be presented in either a back-channel or front-channel manner from the IdP to the RP. Each model has its benefits and drawbacks, but both require the proper validation of the Assertion. Assertions may also be proxied to facilitate federation between IdPs and RPs under specific circumstances. The IdP must transmit only those Attributes that were explicitly requested by the RP. RPs must conduct a privacy risk assessment when determining which attributes to request.

The Subscriber must be able to view the Attribute values to be transmitted, although masking mechanisms must be employed, as necessary, to mitigate the risk of unauthorized exposure of sensitive information (e.g. shoulder surfing). The Subscriber must receive explicit notice and be able to provide positive confirmation before any attributes about the Subscriber are transmitted to any RP.

At a minimum, the notice should be provided by the party in the position to provide the most effective notice and obtain confirmation. If the protocol in use allows for optional Attributes, the Subscriber must be given the option to decide whether to transmit those Attributes to the

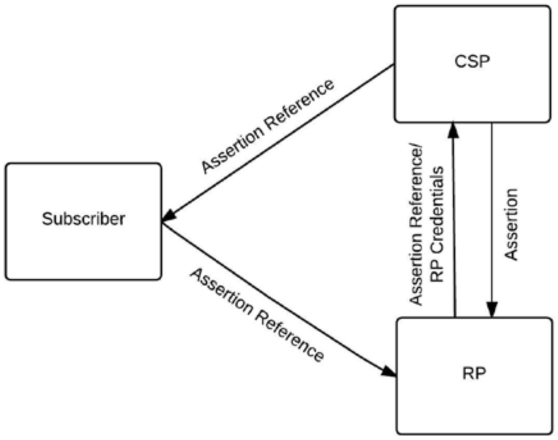
Formatted: Position: Vertical: -0.04", Relative to: Paragraph

RP. A IdP may employ mechanisms to remember and re-transmit the exact Attribute bundle to the same RP.

Back-Channel Presentation

In the back-channel model, the Subscriber is given an Assertion reference to present to the RP, generally through the front channel. The Assertion reference itself contains no information about the Subscriber and must be resistant to tampering and fabrication by an attacker. The RP presents the Assertion reference to the IdP, usually along with authentication of the RP itself, to fetch the Assertion. **Figure 2** shows the back-channel presentation model.

Figure 2. Back-Channel Assertion Presentation



Source: NIST SP 800-63C

In the back-channel model, the Assertion itself is requested directly from the IdP to the RP, minimizing chances of interception and manipulation by a third party (including the Subscriber themselves). This method also allows the RP to query the CSP for additional attributes about the Subscriber not included in the Assertion itself, since back-channel communication can continue to occur after the initial authentication transaction has completed.

The back-channel method also requires more network transactions than the front-channel model, but the information is limited to the only required parties. Since an RP is expecting to get an Assertion only from the IdP directly, the attack surface is reduced since it is more difficult to inject Assertions directly into the RP.

The Assertion Reference:

- Must be limited to use by a single RP
- Must be single-use
- Should be time limited with a short lifetime of seconds or minutes

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Centered

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

- Should be presented along with authentication of the RP

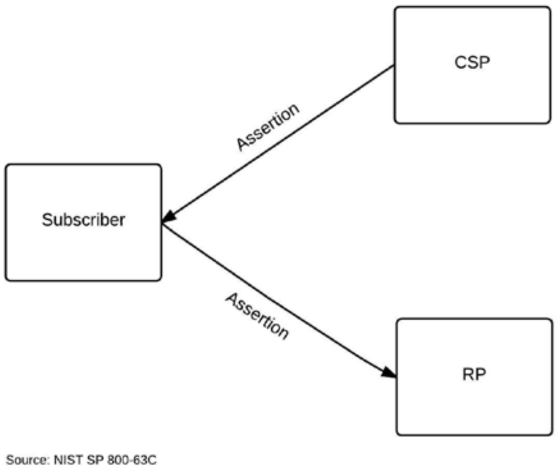
The RP must protect itself against injection of manufactured or captured Assertion references by use of cross-site scripting protection or other accepted techniques. Claims within the Assertion must be validated including issuer verification, signature validation, and audience restriction.

Conveyance of the Assertion reference from the IdP to the Subscriber as well as from the Subscriber to the RP must be made over an authenticated protected channel. Conveyance of the Assertion reference from the RP to the IdP as well as the Assertion from the IdP to the RP must be made over an authenticated protected channel. Presentation of the Assertion reference at the IdP should require Authentication of the RP before issuance of an Assertion.

Front-Channel Presentation

In the front-channel model, the IdP creates an Assertion and sends it to the Subscriber after successful Authentication. The Assertion is used by the Subscriber to authenticate to the RP. This is often handled by mechanisms within the Subscriber's browser. **Figure 3** shows the front-channel presentation model.

Figure 3: Front-Channel Assertion Presentation



Source: NIST SP 800-63C

In the front-channel method, an Assertion is visible to the Subscriber, which could potentially cause leakage of system information included in the Assertion. Since the Assertion is under the control of the Subscriber, the front-channel presentation method also allows the Subscriber to submit a single Assertion to unintended parties, perhaps by a browser replaying an Assertion at multiple RPs. Even if the Assertion is audience restricted and rejected by RPs, its presentation at

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Centered

Formatted: Font: Bold

Formatted: Position: Vertical: -0.04", Relative to: Paragraph unintended RPs could lead to leaking information about the Subscriber and their online activities.

Though it is possible to intentionally create an Assertion designed to be presented to multiple RPs, this method can lead to lax audience restriction of the Assertion itself, which in turn could lead to privacy and security breaches for the Subscriber across these RPs. Such multi-RP use is not recommended. Instead, RPs are encouraged to fetch their own individual Assertions.

The RP must protect itself against injection of manufactured or captured Assertions by use of cross-site scripting protection or other accepted techniques. Claims within the Assertion must be validated including issuer verification, signature validation, and audience restriction. Conveyance of the Assertion from the IdP to the Subscriber as well as from the Subscriber to the RP must be made over an authenticated protected channel.

Assertion Proxying

In some implementations, a proxy accepts an Assertion from the IdP and creates a derived Assertion when interacting directly with the RP, acting as an intermediary between the Subscriber, the IdP, and the RP. From the perspective of the true IdP, the proxy is a single RP. From the perspective of the true RPs, the proxy is a single IdP.

There are several common reasons for such proxies:

- Portals that provide users access to multiple RPs that require user authentication
- Web caching mechanisms that are required to satisfy the RP's access control policies, especially when mutually-authenticated TLS with the Subscriber is used
- Network monitoring and/or filtering mechanisms that terminate TLS in order to inspect and manipulate the traffic

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Conveyance of all information must be made over authenticated protected channels.

Assertion Security

Formatted: Font: 13 pt

IdPs, RPs, Subscribers, and parties outside of a typical Assertions transaction may be malicious or become compromised. An attacker might have an interest in modifying or replacing an Assertion to obtain a greater level of access to a resource or service provided by an RP. They might be interested in obtaining or modifying Assertions and Assertion references to impersonate a Subscriber or access unauthorized data or services.

Furthermore, it is possible that two or more entities may be colluding to attack another party. An attacker may attempt to subvert Assertion protocols by directly compromising the integrity or confidentiality of the Assertion data. For the purpose of these types of threats, authorized parties who attempt to exceed their privileges may be considered attackers.

Common attacks against Assertion transmission transactions include the following:

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

- Assertion Manufacture/Modification: An attacker generates a forged Assertion or modifies the content of an existing Assertion (such as the authentication or attribute statements), causing the RP to grant inappropriate access to the Subscriber. For example, an attacker may modify the Assertion to extend the validity period and keep using an Assertion; or a Subscriber may modify the Assertion to have access to information that they should not be able to view.
- Assertion Disclosure: Assertions may contain authentication and attribute statements that include sensitive Subscriber information. Disclosure of the Assertion contents can make the Subscriber vulnerable to other types of attacks.
- Assertion Repudiation by the IdP: An Assertion may be repudiated by an IdP if the proper mechanisms are not in place. For example, if an IdP does not digitally sign an Assertion, the IdP can claim that it was not generated through the services of the IdP.
- Assertion Repudiation by the Subscriber: Since it is possible for a compromised or malicious IdP to issue Assertions to the wrong party, a Subscriber can repudiate any transaction with the RP that was authenticated using only a bearer Assertion.
- Assertion Redirect: An attacker uses the Assertion generated for one RP to obtain access to a second RP.
- Assertion Reuse: An attacker attempts to use an Assertion that has already been used once with the intended RP.

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

In some cases, the Subscriber is issued some secret information so that they can be recognized by the RP. The knowledge of this information distinguishes the Subscriber from attackers who wish to impersonate the them. In the case of Holder-of-Key Assertions, this secret could already have been established with the IdP prior to the initiation of the Assertion protocol.

In other cases, the IdP will generate a temporary secret and transmit it to the authenticated Subscriber for this purpose. When this secret is used to authenticate to the RP, this temporary secret will be referred to as a secondary authenticator. Secondary authenticators include Assertions in the direct model, session keys in Kerberos, Assertion references in the indirect model, and cookies used for authentication.

Threats to the secondary authenticator include the following:

- Secondary Authenticator Manufacture: An attacker may attempt to generate a valid secondary authenticator and use it to impersonate a Subscriber.
- Secondary Authenticator Capture: An attacker may use a session hijacking attack to capture the secondary authenticator when the IdP transmits it to the Subscriber after the primary authentication step, or the attacker may use a man-in-the-middle attack to obtain the secondary authenticator as it is being used by the Subscriber to authenticate to the RP. If, as in the indirect model, the RP needs to send the secondary authenticator back to the IdP in order to check its validity or obtain the corresponding Assertion data, an attacker may similarly subvert the communication protocol between the IdP and the RP to capture a secondary authenticator. In any of the above scenarios, the secondary authenticator can be used to impersonate the Subscriber.

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

Finally, in order for the Subscriber's authentication to the RP to be useful, the binding between the secret used to authenticate to the RP and the Assertion data referring to the Subscriber needs to be strong. In Assertion substitution, a Subscriber may attempt to impersonate a more privileged Subscriber by subverting the communication channel between the IdP and RP, for example by reordering the messages, to convince the RP that their secondary authenticator corresponds to Assertion data sent on behalf of the more privileged Subscriber.

Threat Mitigation Strategies

Mitigation techniques are described below for each of the threats described in the last subsection:

- Assertion Manufacture/Modification: To mitigate this threat, the following mechanisms are used:
  - The Assertion is digitally signed by the IdP. The RP checks the digital signature to verify that it was issued by a legitimate IdP.
  - The Assertion is sent over a protected session such as TLS. In order to protect the integrity of Assertions from malicious attack, the IdP is authenticated.
  - The Assertion contains a non-guessable random identifier.

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: List Paragraph, Indent: Left: 0.5", Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1"

- Assertion Disclosure: To mitigate this threat, one of the following mechanisms are used:
  - The Assertion is sent over a protected session to an authenticated RP. Note that, in order to protect Assertions against both disclosure and manufacture/modification using a protected session, both the RP and the IdP need to be validated.
  - Assertions are signed by the IdP and encrypted for a specific RP. It should be noted that this provides all the same guarantees as a mutually authenticated protected session, and may therefore be considered equivalent. The general requirement for protecting against both Assertion disclosure and Assertion manufacture/modification may therefore be described as a mutually authenticated protected session or equivalent between the IdP and the RP.

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: List Paragraph, Indent: Left: 0.5", Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1"

- Assertion Repudiation by the IdP: To mitigate this threat, the Assertion is digitally signed by the IdP using a key that supports non-repudiation. The RP checks the digital signature to verify that it was issued by a legitimate IdP.

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

- Assertion Repudiation by the Subscriber: To mitigate this threat, the IdP issues holder-of-key Assertions, rather than bearer Assertions. The Subscriber can then prove possession of the asserted key to the RP. If the asserted key matches the Subscriber's presented key, it will be proof to all parties involved that it was the Subscriber who authenticated to the RP rather than a compromised IdP impersonating the Subscriber.
- Assertion Redirect: To mitigate this threat, the Assertion includes the identity of the RP for which it was generated. The RP verifies that incoming Assertions include its identity as the recipient of the Assertion.

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

- Assertion Reuse: To mitigate this threat, the following mechanisms are used:
  - The Assertion includes a timestamp and has a short lifetime of validity. The RP checks the timestamp and lifetime values to ensure the Assertion is currently valid.
  - The RP keeps track of Assertions that were consumed within a (configurable) time window to ensure that an Assertion is not used more than once within that time window.
- Secondary Authenticator Manufacture: To mitigate this threat, one of the following mechanisms is used:
  - The secondary authenticator may contain sufficient entropy that an attacker without direct access to the IdP's random number generator cannot guess the value of a valid secondary authenticator.
  - The secondary authenticator may contain timely Assertion data that is signed by the IdP or integrity protected using a key shared between the IdP and the RP.
- Secondary Authenticator Capture: To mitigate this threat, adequate protections are in place throughout the lifetime of any secondary authenticators used in the Assertion protocol:
  - In order to protect the secondary authenticator while it is in transit between the IdP and the Subscriber, the secondary authenticator is sent via a protected session established during the primary authentication of the Subscriber.
  - In order to protect the secondary authenticator from capture as it is submitted to the RP, the secondary authenticator is used in an authentication protocol which protects against eavesdropping and man-in-the-middle attacks.
  - In order to protect the secondary authenticator after it has been used, it is never transmitted over an unprotected session or to an unauthenticated party while it is still valid.
- Assertion Substitution: To mitigate this threat, one of the following mechanisms is used:
  - Responses to Assertion requests contain the value of the Assertion reference used in the request or some other nonce that was cryptographically bound to the request by the RP.
  - Responses to Assertion requests are bound to the corresponding requests by message order, as in HTTP, provided that Assertions and requests are protected by a protocol such as TLS that can detect and disallow malicious reordering of packets.

Assertion Examples

The following represent three (3) types of Assertion technologies: Security Assertion Markup Language (SAML) Assertions, Kerberos tickets, and OpenID Connect tokens.

Security Assertion Markup Language (SAML)

SAML is an XML-based framework for creating and exchanging authentication and Attribute information between trusted entities over the internet. As of this writing, the latest specification for [SAML] is SAML v2.0, issued 15 March 2005.

The building blocks of SAML include:

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: List Paragraph, Indent: Left: 0.5", Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1"

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: List Paragraph, Indent: Left: 0.5", Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1"

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: List Paragraph, Indent: Left: 0.5", Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1"

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: List Paragraph, Indent: Left: 0.5", Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1"

Formatted: Font: 13 pt

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

- Assertion XML schema which defines the structure of the Assertion
- SAML Protocols which are used to request Assertions and artifacts
- Bindings that define the underlying communication protocols (such as HTTP or SOAP) and can be used to transport the SAML Assertions.

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

The three components above define a SAML profile that corresponds to a particular use case such as “Web Browser SSO.” SAML Assertions are encoded in an XML schema and can carry up to three types of statements:

- Authentication statements include information about the Assertion issuer, the authenticated Subscriber, validity period, and other authentication information. For example, an Authentication Assertion would state the Subscriber “John” was authenticated using a password at 10:32 p.m. on 06-06-2004.
- Attribute statements contain specific additional characteristics related to the Subscriber. For example, subject “John” is associated with attribute “Role” with value “Manager.”
- Authorization statements identify the resources the Subscriber has permission to access. These resources may include specific devices, files, and information on specific web servers. For example, subject “John” for action “Read” on “Webserver1002” given evidence “Role.”

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Kerberos Tickets

The Kerberos Network Authentication Service [RFC 4120] was designed to provide strong authentication for client/server applications using symmetric-key cryptography on a local, shared network. Extensions to Kerberos can support the use of public key cryptography for selected steps of the protocol. Kerberos also supports confidentiality and integrity protection of session data between the Subscriber and the RP. Even though Kerberos uses Assertions, since it is designed for use on shared networks it is not truly a federation protocol.

Kerberos supports authentication of a Subscriber over an untrusted, shared local network using one or more IdPs. The Subscriber implicitly authenticates to the IdP by demonstrating the ability to decrypt a random session key encrypted for the Subscriber by the IdP. (Some Kerberos variants also require the Subscriber to explicitly authenticate to the IdP, but this is not universal.)

In addition to the encrypted session key, the IdP also generates another encrypted object called a Kerberos ticket. The ticket contains the same session key, the identity of the Subscriber to whom the session key was issued, and an expiration time after which the session key is no longer valid. The ticket is confidentiality and integrity protected by a pre-established that is key shared between the IdP and the RP during an explicit setup phase.

To authenticate using the session key, the Subscriber sends the ticket to the RP along with encrypted data that proves that the Subscriber possesses the session key embedded within the

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

Kerberos ticket. Session keys are either used to generate new tickets, or to encrypt and authenticate communications between the Subscriber and the RP.

To begin the process, the Subscriber sends an authentication request to the Authentication Server (AS). The AS encrypts a session key for the Subscriber using the Subscriber's long term Credential. The long term Credential may either be a secret key shared between the AS and the Subscriber, or in the PKINIT variant of Kerberos, a Public Key Certificate. It should be noted that most variants of Kerberos based on a Shared Secret key between the Subscriber and IdP derive this key from a user generated password. As such, they are vulnerable to offline dictionary attack by a passive eavesdropper.

In addition to delivering the session key to the Subscriber, the AS also issues a ticket using a key it shares with the Ticket Granting Server (TGS). This ticket is referred to as a Ticket Granting Ticket (TGT), since the verifier uses the session key in the TGT to issue tickets rather than to explicitly authenticate the verifier. The TGS uses the session key in the TGT to encrypt a new session key for the Subscriber and uses a key it shares with the RP to generate a ticket corresponding to the new session key. The Subscriber decrypts the session key and uses the ticket and the new session key together to authenticate to the RP.

OpenID Connect

OpenID Connect is an internet-scale federated identity and authentication protocol built on top of the OAuth 2.0 authorization framework and the JSON Object Signing and Encryption (JOSE) cryptographic system. As of this writing, the latest specification is version 1.0 with errata, dated November 8, 2014.

OpenID Connect builds on top of the OAuth 2.0 authorization protocol to enable the Subscriber to authorize the RP to access the Subscriber's identity and authentication information. The RP in both OpenID Connect and OAuth 2.0 is known as the client.

In a successful OpenID Connect transaction, the IdP issues an ID Token, which is a signed Assertion in JSON Web Token (JWT) format. The client parses the ID Token to learn about the Subscriber and primary authentication event at the IdP. This token contains at minimum the following claims about the Subscriber and authentication event:

- `iss` : HTTPS URL identifying the IdP that issued the Assertion
- `sub` : IdP-specific subject identifier representing the Subscriber
- `aud` : IdP-specific audience identifier, equal to the OAuth 2.0 client identifier of the client at the IdP
- `exp` : Timestamp at which the Identity token expires and after which must not be accepted the client
- `iat` : Timestamp at which the Identity token was issued and before which must not be accepted by the client

Formatted: Font: Courier, 10 pt, Font color: Red, Highlight

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: (Default) Courier, 10 pt, Font color: Red, Highlight

Formatted: Font: Courier, 10 pt, Font color: Red, Highlight

Formatted: Font: Courier, 10 pt, Font color: Red, Highlight

Formatted: Font: Courier, 10 pt, Font color: Red, Highlight

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

In addition to the Identity token, the IdP also issues the client an OAuth 2.0 access token which can be used to access the UserInfo Endpoint at the IdP. This endpoint returns a JSON object representing a set of claims about the Subscriber, including but not limited to their name, email address, physical address, phone number, and other profile information.

While the information inside the ID Token is reflective of the authentication event, the information in the UserInfo Endpoint is generally more stable and could be more general purpose. Access to different claims from the UserInfo Endpoint is governed by the use of a specially defined set of OAuth scopes, `openid`, `profile`, `email`, `phone`, and `address`. An additional scope, `offline_access`, is used to govern the issuance of refresh tokens, which allow the RP to access the UserInfo Endpoint when the Subscriber is not present.

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

~~In addition, certain registration, identity proofing, and issuance processes performed by the credential service provider (CSP) may be delegated to an entity known as the registration authority (RA) or identity manager (IM). A close relationship between the RA/IM and CSP is typical, and the nature of this relationship may differ among RAs, IMs, and CSPs. The minimum specifications defined in this document assume that relationships between participants and their requirements are established in the trust framework for the identity management system.~~

~~Electronic authentication begins with registration (also referred to as enrollment). The usual sequence for registration proceeds as follows. An applicant applies to a CSP. If approved, the CSP creates a credential and binds it to one or more authenticators. The credential includes an identifier, which can be pseudonymous, and one or more attributes that the CSP has verified. The authenticators may be issued by the CSP, generated/provided directly by the subscriber, or provided by a third party. The authenticator and credential may be used in subsequent authentication events.~~

~~The process used to verify an applicant's association with their real world identity is called identity proofing. The strength of identity proofing is described by a categorization called the identity assurance level (IAL, see subsection on Assurance Level Model below in this document). Minimum specifications for identity proofing and verification during the registration process have been established in *ITRM Guidance Document: Identity Proofing and Verification*.~~

~~At IAL 1, identity proofing is not required, therefore any attribute information provided by the subscriber is self-asserted and not verified. At IAL 2 and 3, identity proofing is required, but the CSP may assert verified attribute values, verified attribute claims, pseudonymous identifiers, or nothing. This information assists Relying Parties (RPs) in making access control or authorization decisions. RPs may decide that their required IAL is 2 or 3, but may only need specific attributes, and perhaps attributes that retain an individual's pseudonymity. A relying party may also employ a federated identity approach where the RP outsources all identity proofing, attribute collection, and attribute storage to a CSP.~~

~~In these minimum specifications, the party to be authenticated is called a claimant and the party verifying that identity is called a verifier. When a claimant successfully demonstrates possession and control of one or more authenticators to a verifier through an authentication protocol, the verifier can verify that the claimant is a valid subscriber. The verifier passes on an assertion about the subscriber, who may be either pseudonymous or non-pseudonymous, to the RP. That assertion includes an identifier, and may include identity information about the subscriber, such as the name, or other attributes that were verified in the enrollment process (subject to the policies of the CSP and the trust framework for the system). When the verifier is also the RP, the assertion may be implicit. The RP can use the authenticated information provided by the verifier to make access control or authorization decisions.~~

~~Authentication establishes confidence in the claimant's identity, and in some cases in the claimant's attributes. Authentication does not determine the claimant's authorizations or access privileges; this is a separate decision. RPs will use a subscriber's authenticated identity~~

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

~~and attributes with other factors to make access control or authorization decisions. Nothing in this document precludes RPs from requesting additional information from a subscriber that has successfully authenticated.~~

~~The strength of the authentication process is described by a categorization called the authenticator assurance level (AAL). AAL 1 requires single-factor authentication and is permitted with a variety of different authenticator types. At AAL 2, authentication requires two authentication factors for additional security. Authentication at the highest level, AAL 3, requires the use of a hardware-based authenticator and one other factor.~~

~~As part of authentication, mechanisms such as device identity or geo-location may be used to identify or prevent possible authentication false positives. While these mechanisms do not directly increase the authenticator assurance level, they can enforce security policies and mitigate risks. In many cases, the authentication process and services will be shared by many applications and agencies. However, it is the individual agency or application acting as the RP that shall make the decision to grant access or process a transaction based on the specific application requirements.~~

~~Authentication Components and Process Flows~~

~~The various entities and interactions that comprise the electronic authentication model defined in these minimum specifications have been illustrated below in **Figure 1**. The left shows the enrollment, credential issuance, lifecycle management activities, and the stages an individual transitions, based on the specific phase of the identity proofing and authentication process.~~

~~The authentication process begins with the claimant demonstrating to the verifier possession and control of an authenticator that is bound to the asserted identity through an authentication protocol. Once possession and control have been demonstrated, the verifier confirms that the credential remains valid, usually by interacting with the CSP.~~

~~The exact nature of the interaction between the verifier and the claimant during the authentication protocol contributes to the overall security of the system. Well-designed protocols can protect the integrity and confidentiality of traffic between the claimant and the verifier both during and after the authentication exchange, and it can help limit the damage that can be done by an attacker masquerading as a legitimate verifier.~~

~~Additionally, mechanisms located at the verifier can mitigate online guessing attacks against lower entropy secrets like passwords and PINs by limiting the rate at which an attacker can make authentication attempts or otherwise delaying incorrect attempts. Generally, this is done by keeping track of and limiting the number of unsuccessful attempts, since the premise of an online guessing attack is that most attempts will fail.~~

~~The verifier is a functional role, but is frequently implemented in combination with the CSP and/or the RP. If the verifier is a separate entity from the CSP, it is often desirable to ensure~~

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

~~that the verifier does not learn the subscriber’s authenticator secret in the process of authentication, or at least to ensure that the verifier does not have unrestricted access to secrets stored by the CSP.~~

~~The usual sequence of interactions in the authentication process is as follows:~~

1. ~~An applicant applies to a CSP through a registration process.~~
2. ~~The CSP identity proofs that applicant. Upon successful proofing, the applicant becomes a subscriber.~~
3. ~~An authenticator and a corresponding credential are established between the CSP and the new subscriber.~~
4. ~~The CSP maintains the credential, its status, and the enrollment data collected for the lifetime of the credential. The subscriber maintains his or her authenticator.~~

~~Other sequences are less common, but could also achieve the same functional requirements. The right side of Figure 1 shows the entities and the interactions related to using an authenticator to perform electronic authentication. When the subscriber needs to authenticate to perform a transaction, he or she becomes a claimant to a verifier. The interactions are as follows:~~

1. ~~The claimant proves to the verifier that he or she possesses and controls the authenticator through an authentication protocol.~~
2. ~~The verifier interacts with the CSP to validate the credential that binds the subscriber’s identity to his or her authenticator and to optionally obtain claimant attributes.~~
3. ~~If the verifier is separate from the RP (application), the verifier provides an assertion about the subscriber to the RP, which may use the information in the assertion to make an access control or authorization decision.~~
4. ~~An authenticated session is established between the subscriber and the RP.~~

~~In all cases, the RP should request the attributes it requires from a CSP prior to authentication of the claimant. In addition, the claimant should be requested to consent to the release of those attributes prior to generation and release of an assertion.~~

~~In some cases, the verifier does not need to communicate in real time with the CSP to complete the authentication activity (e.g., some uses of digital certificates). Therefore, the dashed line between the verifier and the CSP represents a logical link between the two entities rather than a physical link. In some implementations, the verifier, RP and the CSP functions may be distributed and separated as shown in Figure 1; however, if these functions reside on the same platform, the interactions between the components are local messages between applications running on the same system rather than protocols over shared untrusted networks.~~

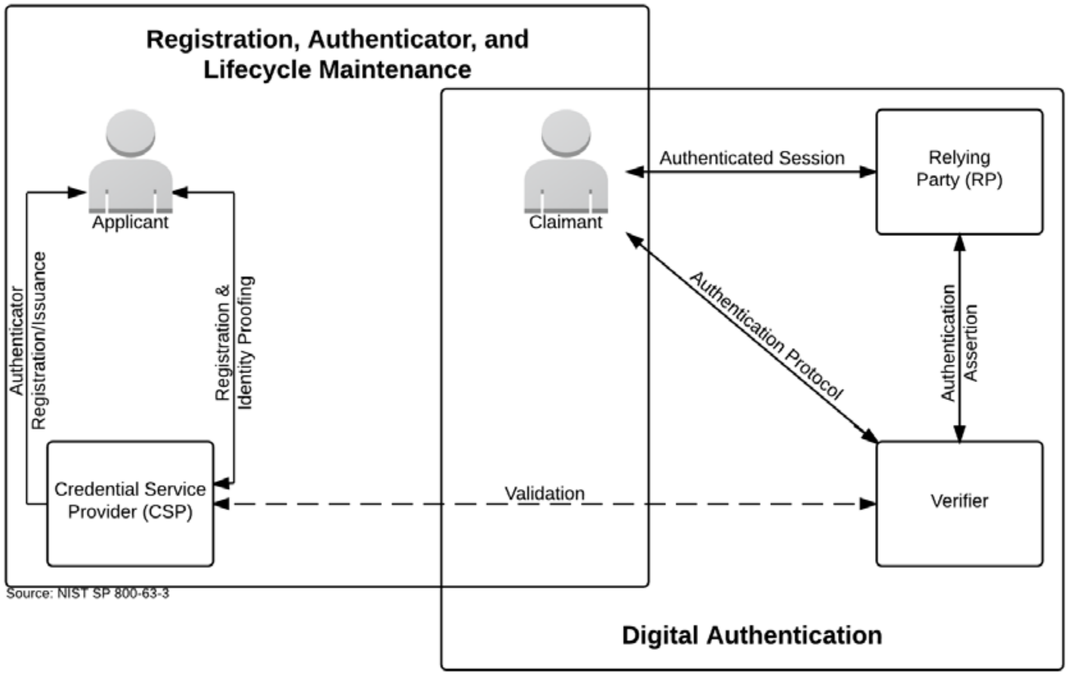
~~As noted above, CSPs maintain status information about issued credentials. CSPs may assign a finite lifetime to a credential in order to limit the maintenance period. When the status changes, or when the credentials near expiration, credentials may be renewed or re-issued; or, the credential may be revoked or destroyed. Typically, the subscriber authenticates to the CSP using his or her existing, unexpired authenticator and credential in order to request issuance of~~

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

~~a new authenticator and credential. If the subscriber fails to request authenticator and credential re-issuance prior to their expiration or revocation, he or she may be required to repeat the enrollment process to obtain a new authenticator and credential. Alternatively, the CSP may choose to accept a request during a grace period after expiration.~~

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

~~**Figure 1. Electronic Authentication Model**~~



~~Source: NIST SP 800-63-3, accessible at https://pages.nist.gov/800-63-3/sp800-63-3.html~~

~~Note: Figure 1 illustrates the model for electronic authentication in an identity management system, as documented in NIST SP 800-63-3 (Public Review), containing all components, requirements, and specifications recommended by IMSAC. However, the minimum specifications defined in this document have been developed to accommodate requirements for electronic authentication established under other national and international standards.~~

~~Authentication Protocols and Lifecycle Management~~

Formatted: Font: 13 pt

~~Authenticators~~

~~The established paradigm for electronic authentication identifies three factors as the cornerstone of authentication:~~

- ~~Something you know (for example, a password)~~
- ~~Something you have (for example, an ID badge or a cryptographic key)~~
- ~~Something you are (for example, a fingerprint or other biometric data)~~

~~Multi-factor authentication refers to the use of more than one of the factors listed above. The strength of authentication systems is largely determined by the number of factors incorporated by the system. Implementations that use two different factors are considered to be stronger than those that use only one factor; systems that incorporate all three factors are stronger than systems that only incorporate two of the factors. Other types of information, such as location data or device identity, may be used by an RP or verifier to evaluate the risk in a claimed identity, but they are not considered authentication factors.~~

~~In electronic authentication the claimant possesses and controls one or more authenticators that have been registered with the CSP and are used to prove the claimant's identity. The authenticator(s) contains secrets the claimant can use to prove that he or she is a valid subscriber, the claimant authenticates to a system or application over a network by proving that he or she has possession and control of an authenticator.~~

~~The secrets contained in authenticators are based on either public key pairs (asymmetric keys) or shared secrets (symmetric keys). A public key and a related private key comprise a public key pair. The private key is stored on the authenticator and is used by the claimant to prove possession and control of the authenticator. A verifier, knowing the claimant's public key through some credential (typically a public key certificate), can use an authentication protocol to verify the claimant's identity, by proving that the claimant has possession and control of the associated private key authenticator.~~

~~Shared secrets stored on authenticators may be either symmetric keys or passwords. While they can be used in similar protocols, one important difference between the two is how they relate to the subscriber. While symmetric keys are generally stored in hardware or software that the subscriber controls, passwords are intended to be memorized by the subscriber. As such, keys are something the subscriber has, while passwords are something he or she knows. Since passwords are committed to memory,~~

~~they usually do not have as many possible values as cryptographic keys, and, in many protocols, are severely vulnerable to network attacks that are more restricted for keys.~~

~~Moreover, the entry of passwords into systems (usually through a keyboard) presents the opportunity for very simple keyboard logging attacks, and may also allow those nearby to learn the password by watching it being entered. Therefore, keys and passwords demonstrate somewhat separate authentication properties (something you have rather than something you know). When using either public key pairs or shared secrets, the subscriber has a duty to maintain exclusive control of his or her authenticator, since possession and control of the authenticator is used to authenticate the claimant's identity.~~

~~The minimum specifications defined in this document assume that authenticators always contain a secret. Authentication factors classified as something you know are not necessarily secrets. Knowledge based authentication, where the claimant is prompted to answer questions that can be confirmed from public databases, also does not constitute an acceptable secret for electronic authentication. More generally, something you are does not generally constitute a secret. However, the requirements for some identity management systems may allow the use of biometrics as an authenticator.~~

~~Biometric characteristics are unique personal attributes that can be used to verify the identity of a person who is physically present at the point of verification. They include facial features, fingerprints, iris patterns, voiceprints, and many other characteristics. NIST recommends that biometrics be used in the enrollment process for higher levels of assurance to later help prevent a subscriber who is registered from repudiating the enrollment, to help identify those who commit enrollment fraud, and to unlock authenticators. The specific requirements for the use of biometrics must be defined in the trust framework for the system.~~

~~The minimum specifications in this document encourage identity management systems to use authentication processes and protocols that incorporate all three factors, as a means of enhancing system security. An electronic authentication system may incorporate multiple factors in either of two ways. The system may be implemented so that multiple factors are presented to the verifier, or some factors may be used to protect a secret presented to the verifier. If multiple factors are presented to the verifier, each will need to be an authenticator (and therefore contain a secret). If a single factor is presented to the verifier, the additional factors are used to protect the authenticator and need not themselves be authenticators.~~

~~Credentials~~

~~As described in the preceding sections, credentials bind an authenticator to the subscriber as part of the issuance process. Credentials are stored and maintained by the CSP. The claimant possesses an authenticator, but is not necessarily in possession of the electronic credentials. For example, database entries containing the user attributes are considered to be credentials for the purpose of this document but are possessed by the verifier.~~

~~Assertions~~

~~Upon completion of the electronic authentication process, the verifier generates an assertion containing the result of the authentication and provides it to the RP. If the verifier is implemented in combination with the RP, the assertion is implicit. If the verifier is a separate entity from the RP, as in typical federated identity models, the assertion is used to communicate the result of the authentication process, and optionally information about the subscriber, from the verifier to the RP.~~
~~Assertions may be communicated directly to the RP, or can be forwarded through the subscriber, which has further implications for system design. An RP trusts an assertion based on the source, the time of creation, and the corresponding trust framework that governs the policies and process of CSPs and RPs. The verifier is responsible for providing a mechanism by which the integrity of the assertion can be confirmed.~~

~~The RP is responsible for authenticating the source (e.g., the verifier) and for confirming the integrity of the assertion. When the verifier passes the assertion through the subscriber, the verifier must protect the integrity of the assertion in such a way that it cannot be modified by the subscriber. However, if the verifier and the RP communicate directly, a protected session may be used to provide the integrity protection. When sending assertions across a network, the verifier is responsible for ensuring that any sensitive subscriber information contained in the assertion can only be extracted by an RP that it trusts to maintain the information’s confidentiality.~~

~~Examples of assertions include:~~

- ~~SAML Assertions – SAML assertions are specified using a mark-up language intended for describing security assertions. They can be used by a verifier to make a statement to an RP about the identity of a claimant. SAML assertions may be digitally signed.~~
- ~~OpenID Connect Claims - OpenID Connect are specified using JavaScript Object Notation (JSON) for describing security, and optionally, user claims. JSON user info claims may be digitally signed.~~

- ~~Kerberos Tickets – Kerberos Tickets allow a ticket granting authority to issue session keys to two authenticated parties using symmetric key based encapsulation schemes.~~

~~Relying Parties~~

~~An RP relies on results of an authentication protocol to establish confidence in the identity or attributes of a subscriber for the purpose of conducting an online transaction. RPs may use a subscriber's authenticated identity (pseudonymous or non-pseudonymous), the IAL, AAL, and other factors to make access control or authorization decisions. The verifier and the RP may be the same entity, or they may be separate entities. If they are separate entities, the RP normally receives an assertion from the verifier. The RP ensures that the assertion came from a verifier trusted by the RP. The RP also processes any additional information in the assertion, such as personal attributes or expiration times.~~

Formatted: Font: Not Bold

Formatted: Font: 13 pt, Not Bold

Formatted: Font: Not Bold

~~Assurance Model~~

Formatted: Font: 13 pt, Not Bold

Formatted: Normal

Formatted: Font: Not Bold

~~The minimum specifications defined in this document for electronic authentication assume that the trust framework for an identity management system will define a specific assurance model for that system.[14] Therefore, the assurance model presented below, which is based on NIST SP 800-63-3, should be viewed as a recommended framework for electronic authentication. Other assurance models have been established in OMB M-04-04 and the State Identity, Credential, and Access Management (SICAM) guidelines, published by the National Association of Chief Information Officers (NASCIO). A crosswalk showing disparities in the NIST SP 800-63-3, OMB M-04-04, and SICAM assurance models has been provided in **Figure 2**.~~

~~Identity Assurance Level 1 – At this level, attributes provided in conjunction with the authentication process, if any, are self-asserted.~~

~~Identity Assurance Level 2 – IAL 2 introduces the need for either remote or in-person identity proofing. IAL 2 requires identifying attributes to have been verified in person or remotely using, at a minimum, the procedures given in NIST 800-63A.~~

~~Identity Assurance Level 3 – At IAL 3, in-person identity proofing is required. Identifying attributes must be verified by an authorized representative of the CSP through examination of physical documentation as described in NIST 800-63A.~~

~~Authenticator Assurance Level 1 - AAL 1 provides single factor electronic authentication, giving some assurance that the same claimant who participated in previous transactions is accessing the protected transaction or data. AAL 1 allows a wide range of available authentication technologies to be employed and requires only a single authentication factor to be used. It also permits the use of any of the authentication methods of higher authenticator assurance levels. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she possesses and controls the authenticator.~~

~~Authenticator Assurance Level 2 – AAL 2 provides higher assurance that the same claimant who participated in previous transactions is accessing the protected transaction or data. Two different authentication factors are required. Various types of authenticators, including multi-factor Software Cryptographic Authenticators, may be used as described in NIST 800-63B. AAL 2 also permits any of the authentication methods of AAL 3. AAL 2 authentication requires cryptographic mechanisms that protect the primary authenticator against compromise by the protocol threats for all threats at AAL 1 as well as verifier impersonation attacks. Approved cryptographic techniques are required for all assertion protocols used at AAL 2 and above.[15]~~

~~[14] Trust Framework~~Identity Trust Frameworks ~~for identity management system~~Digital Identity Systems ~~also should set requirements for how the assurance for each credential will be documented in the medata for the credential to support audit and compliance.~~

~~[15] Approved cryptographic techniques shall~~must ~~be FIPS approved, NIST recommended, or otherwise compliant with Commonwealth IT Information Security Standard (SEC501).~~

~~Authenticator Assurance Level 3 – AAL 3 is intended to provide the highest practical electronic authentication assurance. Authentication at AAL 3 is based on proof of possession of a key through a cryptographic protocol. AAL 3 is similar to AAL 2 except that only "hard" cryptographic authenticators are allowed. The authenticator is required to be a hardware cryptographic module validated at Federal Information Processing Standard (FIPS) 140 Level 2 or higher overall with at least FIPS 140 Level 3 physical security. AAL 3 authenticator requirements can be met by using the PIV authentication key of a FIPS 201 compliant Personal Identity Verification (PIV) Card.~~

~~Figure 2. Assurance Model Crosswalk~~

~~OMB M04-04 Level of Assurance~~	~~SICAM Assurance Level~~	~~NIST SP 800-63-3 IAL~~	~~NIST SP 800-63-3 AAL~~
~~1~~	~~1~~	~~1~~	~~1~~
~~2~~	~~2~~	~~2~~	~~2 or 3~~
~~3~~	~~3~~	~~2~~	~~2 or 3~~
~~4~~	~~4~~	~~3~~	~~3~~

~~http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/HostedEnvironmentInformationSecurityStandardSEC52501.pdf~~

Privacy and Security

The minimum specifications established in this document for privacy and security in the use of person information for ~~electronic authentication~~Electronic Authentication apply the Fair Information Practice Principles (FIPPs).[16] The FIPPs have been endorsed by the National Strategy for Trusted Identities in Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.[17]

The minimum specifications also adhere to the Identity Ecosystem Framework (IDEF) Baseline Functional Requirements (v.1.0) for privacy and security, adopted by the Identity Ecosystem Steering Group (IDESG) in October 2015 (**Appendix 2)**.

The minimum specifications for ~~identity proofing~~Assertions~~ and verification~~ apply the following FIPPs:

- Transparency: RAs and CSPs should be transparent and provide notice to Applicants regarding collection, use, dissemination, and maintenance of person information required during the ~~registration~~Registration, ~~identity proofing~~Identity Proofing and verification processes.
- Individual Participation: RAs and CSPs should involve the Applicant in the process of using person information and, to the extent practicable, seek consent for the collection, use, dissemination, and maintenance of that information. RAs and CSPs also should provide mechanisms for appropriate access, correction, and redress of person information.
- Purpose Specification: RAs and CSPs should specifically articulate the authority that permits the collection of person information and specifically articulate the purpose or purposes for which the information is intended to be used.
- Data Minimization: RAs and CSPs should collect only the person information directly relevant and necessary to accomplish the ~~registration~~Registration and related processes, and only retain that information for as long as necessary to fulfill the specified purpose.
- Use Limitation/Minimal Disclosure: RAs and CSPs should use person information solely for the purpose specified in the notice. Disclosure or sharing that information should be limited to the specific purpose for which the information was collected.
- Data Quality and Integrity: RAs and CSPs should, to the extent practicable, ensure that person information is accurate, relevant, timely, and complete.
- Security: RAs and CSPs should protect personal information through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

[16] The term "person information" refers to protected data for person entities, governed by Applicable Law. This includes Personally Identifiable Information (PII), Protected Health Information (PHI), Federal Tax Information (FTI), Protected Education Records, and related categories. Specific requirements for the privacy and security of person information should be defined by the ~~trust framework~~Identity Trust Framework for the ~~identity management system~~Digital Identity System.

[17] The FIPPs endorsed by NSTIC may be accessed at http://www.nist.gov/nstic/NSTIC-FIPPs.pdf . The FIPPs published in SICAM may be accessed at http://www.nascio.org/Portals/0/Publications/Documents/SICAM.pdf.

- Accountability and Auditing: RAs and CSPs should be accountable for complying with these principles, providing training to all employees and contractors who use person information, and auditing the actual use of person information to demonstrate compliance with these principles and all applicable privacy protection requirements.

~~7 Alignment Comparison~~

Formatted: Font: Bold, Font color: Text 1

Formatted: List Paragraph

~~The minimum specifications for electronic authentication defined in this document have been developed to align with existing national and international standards for electronic authentication and identity management. Specifically, the minimum specifications reflect basic requirements set forth in national standards at the federal and state level, ensuring compliance while accommodating other identity management standards and protocols. This document assumes that each identity management system will comply with those governing standards and protocols required by Applicable Law.~~

~~The following section outlines the alignment and disparities between the minimum specifications in this document and core national standards. A crosswalk documenting the alignment and areas of misalignment has been provided in Appendix 3.~~

~~NIST SP 800-63-3~~

~~The minimum specifications in this document conform with the basic requirements for electronic authentication set forth in NIST SP 800-63-3 (Public Review version). However, as the NIST guidance defines specific requirements for federal agencies, the minimum specifications in this document provide flexibility for identity management systems across industries in the private sector and levels of governance. This flexibility enables identity management systems to adhere to the specifications but do so in a manner appropriate and compliant with their governing trust frameworks.~~

~~State Identity and Access Management Credential (SICAM) Guidance and Roadmap~~

~~The minimum specifications in this document conform with the basic requirements for electronic authentication set forth by NASCIO in the SICAM Guidance and Roadmap. The NASCIO guidance defines specific requirements for state agencies. Similar to the contrast with the NIST guidance for federal agencies, the minimum specifications in this document provide flexibility for identity management systems across industries in the private sector and levels of governance.~~

~~IDESG Identity Ecosystem Framework (IDEF) Functional Model~~

~~The minimum specifications in this document conform with the core operations and basic requirements for privacy and security set forth by IDESG in the IDEF Functional Model and Baseline Functional Requirements. The IDESG/IDEF requirements apply the FIPPs but extend them to cover the Guiding Principles of the National Strategy for~~

~~Trusted Identities in Cyberspace (NSTIC). The minimum specifications in this document encourage adherence to the IDEF Functional Model, Baseline Functional Requirements and the NSTIC Guiding Principles.~~

Formatted: List Paragraph, Indent: Left: 0", Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Appendix 1. IMSAC Charter

COMMONWEALTH OF VIRGINIA
IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL
CHARTER

Advisory Council Responsibilities (§ 2.2-437.A; § 2.2-436.A)

The Identity Management Standards Advisory Council (the Advisory Council) advises the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to § 2.2-436.

The Advisory Council recommends to the Secretary of Technology guidance documents relating to (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions; (ii) the minimum specifications and standards that should be included in an ~~identity~~ Identity Trust Framework, as defined in § 59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-550 et seq.); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

Membership and Governance Structure (§ 2.2-437.B)

The Advisory Council's membership and governance structure is as follows:

1. The Advisory Council consists of seven members, to be appointed by the Governor, with expertise in electronic identity management and information technology. Members include a representative of the Department of Motor Vehicles, a representative of the Virginia Information Technologies Agency, and five representatives of the business community with appropriate experience and expertise. In addition to the seven appointed members, the Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex officio member of the Advisory Council.

2. The Advisory Council designates one of its members as chairman.

3. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure of the Governor, and may be reappointed.

4. Members serve without compensation but may be reimbursed for all reasonable and necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.

5. Staff to the Advisory Council is provided by the Office of the Secretary of Technology.

The formation, membership and governance structure for the Advisory Council has been codified pursuant to § 2.2-437.A, § 2.2-437.B, as cited above in this charter.

The statutory authority and requirements for public notice and comment periods for guidance documents have been established pursuant to § 2.2-437.C, as follows:

C. Proposed guidance documents and general opportunity for oral or written submittals as to those guidance documents shall be posted on the Virginia Regulatory Town Hall and published in the Virginia Register of Regulations as a general notice following the processes and procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§ 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written comments following the posting and publication and shall hold at least one meeting dedicated to the receipt of oral comment no less than 15 days after the posting and publication. The Advisory Council shall also develop methods for the identification and notification of interested parties and specific means of seeking input from interested persons and groups. The Advisory Council shall send a copy of such notices, comments, and other background material relative to the development of the recommended guidance documents to the Joint Commission on Administrative Rules.

This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the minutes of the meeting and related IMSAC documents, visit: https://vita.virginia.gov/About/default.aspx?id=6442474173

Appendix 2. IDESG Identity Ecosystem Framework (IDEF) Baseline Functional Requirements (v.1.0) for Privacy and Security

PRIVACY-1. DATA MINIMIZATION

Entities MUST limit the collection, use, transmission and storage of personal information to the minimum necessary to fulfill that transaction’s purpose and related legal requirements. Entities providing claims or attributes MUST NOT provide any more personal information than what is requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to accommodate information requests of variable granularity, to support data minimization.

PRIVACY-2. PURPOSE LIMITATION

Entities MUST limit the use of personal information that is collected, used, transmitted, or stored to the specified purposes of that transaction. Persistent records of contracts, assurances, consent, or legal authority MUST be established by entities collecting, generating, using, transmitting, or storing personal information, so that the information, consistently is used in the same manner originally specified and permitted.

PRIVACY-3. ATTRIBUTE MINIMIZATION

Entities requesting attributes MUST evaluate the need to collect specific attributes in a transaction, as opposed to claims regarding those attributes. Wherever feasible, entities MUST collect, generate, use, transmit, and store claims about USERS rather than attributes. Wherever feasible, attributes MUST be transmitted as claims, and transmitted credentials and identities MUST be bound to claims instead of actual attribute values.

PRIVACY-4. CREDENTIAL LIMITATION

Entities MUST NOT request USERS’ credentials unless necessary for the transaction and then only as appropriate to the risk associated with the transaction or to the risks to the parties associated with the transaction.

PRIVACY-5. DATA AGGREGATION RISK

Entities MUST assess the privacy risk of aggregating personal information, in systems and processes where it is collected, generated, used, transmitted, or stored, and wherever feasible, MUST design and operate their systems and processes to minimize that risk. Entities MUST assess and limit linkages of personal information across multiple transactions without the USER's explicit consent.

PRIVACY-6. USAGE NOTICE

Entities MUST provide concise, meaningful, and timely communication to USERS describing how they collect, generate, use, transmit, and store personal information.

PRIVACY-7. USER DATA CONTROL

Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete personal information.

PRIVACY-8. THIRD-PARTY LIMITATIONS

Wherever USERS make choices regarding the treatment of their personal information, those choices MUST be communicated effectively by that entity to any THIRD-PARTIES to which it transmits the personal information.

PRIVACY-9. USER NOTICE OF CHANGES

Entities MUST, upon any material changes to a service or process that affects the prior or ongoing collection, generation, use, transmission, or storage of USERS' personal information, notify those USERS, and provide them with compensating controls designed to mitigate privacy risks that may arise from those changes, which may include seeking express affirmative consent of USERS in accordance with relevant law or regulation.

PRIVACY-10. USER OPTION TO DECLINE

USERS MUST have the opportunity to decline ~~registration~~Registration; decline credential provisioning; decline the presentation of their credentials; and decline release of their attributes or claims.

PRIVACY-11. OPTIONAL INFORMATION

Entities MUST clearly indicate to USERS what personal information is mandatory and what information is optional prior to the transaction.

PRIVACY-12. ANONYMITY

Wherever feasible, entities MUST utilize identity systems and processes that enable transactions that are anonymous, anonymous with validated attributes, pseudonymous, or where appropriate, uniquely identified. Where applicable to such transactions, entities employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES collecting USER personal information. Organizations MUST request individuals' credentials only when necessary for the transaction and then only as appropriate to the risk associated with the transaction or only as appropriate to the risks to the parties associated with the transaction.

PRIVACY-13. CONTROLS PROPORTIONATE TO RISK

Controls on the processing or use of USERS' personal information MUST be commensurate with the degree of risk of that processing or use. A privacy risk analysis MUST be conducted by entities who conduct digital identity management functions, to establish what risks those functions pose to USERS' privacy.

PRIVACY-14. DATA RETENTION AND DISPOSAL

Entities MUST limit the retention of personal information to the time necessary for providing and administering the functions and services to USERS for which the information was collected, except as otherwise required by law or regulation. When no longer needed, personal information MUST be securely disposed of in a manner aligning with appropriate industry standards and/or legal requirements.

PRIVACY-15. ATTRIBUTE SEGREGATION

Wherever feasible, identifier data MUST be segregated from attribute data.

SECURE-1. SECURITY PRACTICES

Entities MUST apply appropriate and industry-accepted information security STANDARDS, guidelines, and practices to the systems that support their identity functions and services.

SECURE-2. DATA INTEGRITY

Entities MUST implement industry-accepted practices to protect the confidentiality and integrity of identity data—including authentication data and attribute values—during the execution of all digital identity management functions, and across the entire data lifecycle (collection through destruction).

SECURE-3. CREDENTIAL REPRODUCTION

Entities that issue or manage credentials and tokens MUST implement industry-accepted processes to protect against their unauthorized disclosure and reproduction.

SECURE-4. CREDENTIAL PROTECTION

Entities that issue or manage credentials and tokens MUST implement industry-accepted data integrity practices to enable individuals and other entities to verify the source of credential and token data.

SECURE-5. CREDENTIAL ISSUANCE

Entities that issue or manage credentials and tokens MUST do so in a manner designed to assure that they are granted to the appropriate and intended USER(s) only. Where ~~registration~~Registration and credential issuance are executed by separate entities, procedures for ensuring accurate exchange of ~~registration~~Registration and issuance information that are commensurate with the stated assurance level MUST be included in business agreements and operating policies.

SECURE-6. CREDENTIAL UNIQUENESS

Entities that issue or manage credentials MUST ensure that each account to credential pairing is uniquely identifiable within its namespace for authentication purposes.

SECURE-7. TOKEN CONTROL

Entities that authenticate a USER MUST employ industry-accepted secure authentication protocols to demonstrate the USER's control of a valid token.

SECURE-8. MULTIFACTOR AUTHENTICATION

Entities that authenticate a USER MUST offer authentication mechanisms which augment or are alternatives to a password.

SECURE-9. AUTHENTICATION RISK ASSESSMENT

Entities MUST have a risk assessment process in place for the selection of authentication mechanisms and supporting processes.

SECURE-10. UPTIME

Entities that provide and conduct digital identity management functions MUST have established policies and processes in place to maintain their stated assurances for availability of their services.

SECURE-11. KEY MANAGEMENT

Entities that use cryptographic solutions as part of identity management MUST implement key management policies and processes that are consistent with industry-accepted practices.

SECURE-12. RECOVERY AND REISSUANCE

Entities that issue credentials and tokens MUST implement methods for reissuance, updating, and recovery of credentials and tokens that preserve the security and assurance of the original ~~registration~~Registration and credentialing operations.

SECURE-13. REVOCATION

Entities that issue credentials or tokens MUST have processes and procedures in place to invalidate credentials and tokens.

SECURE-14. SECURITY LOGS

Entities conducting digital identity management functions MUST log their transactions and security events, in a manner that supports system audits and, where necessary, security investigations and regulatory requirements. Timestamp synchronization and detail of logs MUST be appropriate to the level of risk associated with the environment and transactions.

SECURE-15. SECURITY AUDITS

Entities MUST conduct regular audits of their compliance with their own information security policies and procedures, and any additional requirements of law, including a review of their logs, incident reports and credential loss occurrences, and MUST periodically review the effectiveness of their policies and procedures in light of that data.

~~Appendix 3. Electronic Authentication Standards Alignment Comparison Matrix~~

~~**Component**~~	~~**NIST 800-63-3 (Public Review)**~~	~~**SICAM**~~	~~**IDESG IDEF Functional Model**~~
~~Registration~~	~~Alignment: Defines protocols and process flows for applicant registration with a federal agency through an RA, IM or CSP~~	~~Alignment: Defines protocols and process flows for applicant registration with a state agency through an RA, IM or CSP~~	~~Alignment: Identifies core operations within standard registration process flows~~
	~~Misalignment: Federal protocols for applicant registration with federal agencies may not be appropriate across sectors or private industry~~	~~Misalignment: State protocols for applicant registration with state agencies may not be appropriate across sectors or private industry~~	~~Misalignment: Core operational definitions do not contain specific criteria for applicant registration~~
~~Identity Proofing & Verification~~	~~Alignment: Establishes rigorous requirements for identity proofing and verification by federal agencies~~	~~Alignment: Establishes rigorous requirements for identity proofing and verification by state agencies~~	~~Alignment: Defines core operations for identity proofing and verification~~
	~~Misalignment: Federal requirements for identity proofing and verification may not be appropriate across sectors or private industry~~	~~Misalignment: SICAM model identity proofing and verification may not be appropriate across sectors or private industry~~	~~Misalignment: Core operational definitions do not contain specific criteria for acceptable identity proofing and verification~~
~~Authenticators & Credentials~~	~~Alignment: Sets protocols and required flows for federal agencies to follow in issuing, maintaining and deprecating authenticators and credentials~~	~~Alignment: Sets protocols and required flows for state agencies to follow in issuing, maintaining and deprecating authenticators (tokens) and credentials~~	~~Alignment: Documents core operations for authenticators (tokens) and credentials~~
	~~Misalignment: Federal protocols for authenticators and credentials may not be appropriate across sectors or private industry~~	~~Misalignment: SICAM model for authenticators and credentials may not be appropriate across sectors or private industry~~	~~Misalignment: Core operational definitions do not contain specific criteria for authenticators (tokens) and credentials~~
~~Authentication Protocols & Assertions~~	~~Alignment: Provides clearly defined technical requirements for authentication protocols and assertions for federal agencies~~	~~Alignment: Provides clearly defined technical requirements for authentication protocols and assertions for state agencies~~	~~Alignment: Defines core operations for authentication protocols and assertions~~
	~~Misalignment: Federal authentication protocols and assertions may not be appropriate across sectors or private industry~~	~~Misalignment: SICAM model authentication protocols and assertions may not be appropriate across sectors or private industry~~	~~Misalignment: Core operational definitions do not contain specific criteria or technical requirements for authentication protocols and assertions~~
~~Role-Based Requirements for Authentication (RAs, CSPs, RPs, Verifiers)~~	~~Alignment: Establishes role-based requirements for federal agencies, RAs, CSPs, RPs, and Verifiers~~	~~Alignment: Establishes role-based requirements for state agencies, RAs, CPS, RPs, and Verifiers~~	~~Alignment: Identifies core, role-based operational requirements for RAs, CSPs, RPs, and Verifiers~~
	~~Misalignment: Federal role-based requirements may not be appropriate across sectors or private industry~~	~~Misalignment: State role-based requirements may not be appropriate across sectors or private industry~~	~~Misalignment: Core operational roles and responsibilities do not contain specific criteria for role-based requirements~~

Formatted: Normal, Tab stops: 1", Left

Formatted: Width: 8.5", Height: 11", Numbering: Continuous

Formatted: Left, Space Before: 0 pt, After: 0 pt, Tab stops: 1", Left

Formatted: Left, Tab stops: 1", Left

Formatted: Tab stops: 1", Left

Formatted: Tab stops: 1", Left

Formatted: Left, Tab stops: 1", Left

Formatted: Tab stops: 1", Left

Formatted: Tab stops: 1", Left

Formatted: Left, Tab stops: 1", Left

Formatted: Tab stops: 1", Left

Formatted: Tab stops: 1", Left

Formatted: Left, Tab stops: 1", Left

Formatted: Tab stops: 1", Left

Formatted: Tab stops: 1", Left

Formatted: Left, Space Before: 0 pt, After: 0 pt, Tab stops: 1", Left

Formatted: Tab stops: 1", Left

Formatted: Left, Tab stops: 1", Left

Formatted: Tab stops: 1", Left