

COMMONWEALTH OF VIRGINIA



Information Technology Resource Management (ITRM)

GUIDANCE DOCUMENT Identity Proofing and Verification

Virginia Information Technologies Agency (VITA)

Table of Contents

1	Publication Version Control	1
2	Reviews	1
3	Statutory Authority	2
4	Definitions	3
5	Background	16
6	Minimum Specifications	18
7	Alignment Comparison	25

DRAFT

1 Publication Version Control

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

<u>Publication Version</u>	<u>Date</u>	<u>Revision Description</u>
1.0	05/02/2016	Initial Draft of Document
<u>1.0</u>	<u>05/02/2016</u>	<u>Document revised by IMSAC at public workshop</u>
<u>1.0</u>	<u>06/23/2016</u>	<u>Document revised by VITA staff based on comments from IMSAC during May 2, 2016, public workshop</u>

2 Reviews

- 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.
- The document was reviewed by IMSAC during a council workshop, May 2, 2016.
- 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:

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.

Comment [JG1]: Use a COV standards based approach to requiring regular review of the document. (N. Moe and M. Watson) IMSAC may direct staff to update the documents based on updates to standards documents, i.e. NIST 800-63, IDESG IDEF, etc. (L. Kimball)

3 Statutory Authority

The following section documents the statutory authority established in the *Code of Virginia* for the development of minimum specifications and standards for identity proofing and verification. 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>

4 Definitions

Terms used in this document comply with adopted definitions in the National Institute of Standards and Technology Special Publication 800-63-2 (NIST SP 800-63-2), § 59.1-550, Code of Virginia, and the Commonwealth of Virginia’s ITRM Glossary (ITRM Glossary).

Terms used in this document not published in NIST SP 800-63-2, § 59.1-550, or the ITRM Glossary align with the State Identity, Credential, and Access Management Guidance and Roadmap (SICAM), the Identity Ecosystem Steering Group’s Identity Ecosystem Framework Glossary (IDESG IDEF Glossary), or industry standard definitions. Source information has been provided with the definition for each term.¹

Comment [JG2]: Make sure all terms are either defined in Section 4 or with examples/footnotes within the document. (N. Moe)

<u>Active Attack</u>	An attack on the authentication protocol 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. [NIST 800-63-2]
<u>Address of Record</u>	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. [NIST 800-63-2]
<u>Approved</u>	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. [NIST 800-63-2]
<u>Applicant</u>	A party undergoing the processes of registration and identity proofing. [NIST 800-63-2]
<u>Assertion</u>	A statement from a Verifier to a Relying Party (RP) that contains identity information about a Subscriber. Assertions may also contain verified attributes. [NIST 800-63-2]
<u>Assertion Reference</u>	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. [NIST 800-63-2]
<u>Assurance</u>	In the context of OMB M-04-04 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.

¹NIST SP 800-63-2 may be accessed at <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>
 § 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
 The SICAM Guidance and Roadmap may be accessed at <http://www.nascio.org/Portals/0/Publications/Documents/SICAM.pdf>
 The IDESG IDEF Glossary may be accessed at https://wiki.idesg.org/wiki/index.php?title=IDEF_Glossary

	[NIST 800-63-2]
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. [NIST 800-63-2]
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. [NIST 800-63-2]
Attacker	A party who acts with malicious intent to compromise an information system. [NIST 800-63-2]
Attribute	A claim of a named quality or characteristic inherent in or ascribed to someone or something. (See term in [ICAM] for more information.) [NIST 800-63-2]
Authentication	The process of establishing confidence in the identity of users or information systems. [NIST 800-63-2]
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 token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier. [NIST 800-63-2]
Authentication Protocol Run	An exchange of messages between a Claimant and a Verifier that results in authentication (or authentication failure) between the two parties. [NIST 800-63-2]
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 token secret is the canonical example of a long term authentication secret, while the token authenticator, if it is different from the token secret, is usually a short term authentication secret. [NIST 800-63-2]
Authenticity	The property that data originated from its purported source. [NIST 800-63-2]
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. [NIST 800-63-2]
Bit	A binary digit: 0 or 1. [NIST 800-63-2]
Biometrics	Automated recognition of individuals based on their behavioral and biological characteristics.

	<u>Biometrics may be used to unlock authentication tokens and prevent repudiation of registration. [NIST 800-63-2]</u>
<u>Certificate Authority (CA)</u>	<u>A trusted entity that issues and revokes public key certificates. [NIST 800-63-2]</u>
<u>Certificate Revocation List (CRL)</u>	<u>A list of revoked public key certificates created and digitally signed by a Certificate Authority. See [RFC 5280]. [NIST 800-63-2]</u>
<u>Challenge-Response Protocol</u>	<u>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. [NIST 800-63-2]</u>
<u>Claimant</u>	<u>A party whose identity is to be verified using an authentication protocol. [NIST 800-63-2]</u>
<u>Claimed Address</u>	<u>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.” [NIST 800-63-2]</u>
<u>Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)</u>	<u>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. [NIST 800-63-2]</u>
<u>Cookie</u>	<u>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. Cookies are used for many purposes and may be assertions or may contain pointers to assertions. [NIST 800-63-2]</u>
<u>Credential</u>	<u>An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token 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</u>

	<u>between the Subscriber's token and identity. [NIST 800-63-2]</u>
<u>Credential Service Provider (CSP)</u>	<u>A trusted entity that issues or registers Subscriber tokens 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. [NIST 800-63-2]</u>
<u>Cross Site Request Forgery (CSRF)</u>	<u>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. [NIST 800-63-2]</u>
<u>Cross Site Scripting (XSS)</u>	<u>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. [NIST 800-63-2]</u>
<u>Cryptographic Key</u>	<u>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. [NIST 800-63-2]</u>
<u>Cryptographic Token</u>	<u>A token where the secret is a cryptographic key. [NIST 800-63-2]</u>
<u>Data Integrity</u>	<u>The property that data has not been altered by an unauthorized entity. [NIST 800-63-2]</u>
<u>Derived Credential</u>	<u>A credential issued based on proof of possession and control of a token associated with a previously issued credential, so as not to duplicate the identity proofing process. [NIST 800-63-2]</u>
<u>Digital Signature</u>	<u>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. [NIST 800-63-2]</u>
<u>Eavesdropping Attack</u>	<u>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. [NIST 800-63-2]</u>

<u>Electronic Authentication (E-Authentication)</u>	<u>The process of establishing confidence in user identities electronically presented to an information system. [NIST 800-63-2]</u>
<u>Entropy</u>	<u>A measure of the amount of uncertainty that an Attacker faces to determine the value of a secret. Entropy is usually stated in bits. [NIST 800-63-2]</u>
<u>Extensible Mark-up Language (XML)</u>	<u>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. [NIST 800-63-2]</u>
<u>Federal Bridge Certification Authority (FBCA)</u>	<u>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. [NIST 800-63-2]</u>
<u>Federal Information Security Management Act (FISMA)</u>	<u>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. [NIST 800-63-2]</u>
<u>Federal Information Processing Standard (FIPS)</u>	<u>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. See background information for more details. FIPS documents are available online through the FIPS home page: http://www.nist.gov/itl/fips.cfm [NIST 800-63-2]</u>
<u>Federated Identity Management</u>	<u>The use of trust relationships, or Trust Frameworks, between separate security domains (organizations) to provide appropriate and secure, seamless authentication for users. [SICAM]</u>
<u>Federation</u>	<u>An association comprising any number of service providers and Identity Providers. [IDESG IDEF Glossary]</u>
<u>Governance Authority</u>	<u>The authority responsible for providing policy level leadership, oversight, strategic direction and related governance activities within a Federated Identity Management system. [SICAM]</u>
<u>Guessing Entropy</u>	<u>A measure of the difficulty that an Attacker has to guess the average password used in a system. Entropy is stated in bits. When a password has n-bits of guessing entropy then an Attacker has as much difficulty guessing the average password as in guessing an n-bit</u>

	<u>random quantity. The Attacker is assumed to know the actual password frequency distribution. [NIST 800-63-2]</u>
<u>Hash Function</u>	<u>A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:</u> <u>1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and</u> <u>2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output. [NIST 800-63-2]</u>
<u>Holder-of-Key Assertion</u>	<u>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. [NIST 800-63-2]</u>
<u>HTTPS</u>	<u>Protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or Secure Sockets Layer. [Wikipedia]</u>
<u>Identity</u>	<u>A set of attributes that uniquely describe a person within a given context. [NIST 800-63-2]</u>
<u>Identity, Access and Credential Management (ICAM)</u>	<u>A comprehensive, strategic framework and architecture adopted by federal and state government for the management of digital identities, credentials, and access control protocols. [SICAM]</u>
<u>Identity Proofing</u>	<u>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. [NIST 800-63-2]</u>
<u>Identity Provider (IdP)</u>	<u>An entity that creates, maintains, and manages trusted identity information. [IDESG IDEF Glossary]</u>
<u>In-Person Identity Proofing</u>	<u>Method of identity proofing in which Applicants are required to present themselves and identity evidence to a representative of the Registration Authority. (Required for Level of Assurance 4 authentication.) [NIST 800-63-2]</u>
<u>Kerberos</u>	<u>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. [NIST 800-63-2]</u>

<u>Knowledge Based Authentication (KBA)</u>	<u>Authentication of an individual based on knowledge of information associated with his or her claimed identity in public or private 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. [NIST 800-63-2]</u>
<u>Level of Assurance (LoA)</u>	<u>The continuum for the degree of certainty in the user's identity established by the Registration Authority during the registration process. [Derived from industry standard definitions]</u> <u>The term Level of Assurance in this document aligns with the levels defined for federal agencies in the U.S. Office of Management and Budget Memorandum M04-04 and NIST SP 800-63-2 (i.e., Levels 1-4), as well as in SICAM, but provides for a more general framework to accommodate other identity management standards and protocols.</u>
<u>Man-in-the-Middle Attack (MitM)</u>	<u>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. [NIST 800-63-2]</u>
<u>Message Authentication Code (MAC)</u>	<u>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. [NIST 800-63-2]</u>
<u>Min-entropy</u>	<u>A measure of the difficulty that an Attacker has to guess the most commonly chosen password used in a system. Entropy is stated in bits. When a password has n-bits of min-entropy then an Attacker requires as many trials to find a user with that password as is needed to guess an n-bit random quantity. The Attacker is assumed to know the most commonly used password(s). [NIST 800-63-2]</u>
<u>Multi-Factor</u>	<u>A characteristic of an authentication system or a token that uses more than one authentication factor.</u> <u>The three types of authentication factors are something you know, something you have, and something you are. [NIST 800-63-2]</u>
<u>Network</u>	<u>An open communications medium, typically the Internet, that is used to transport messages between the Claimant and other parties.</u> <u>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). [NIST 800-63-2]</u>
<u>Nonce</u>	<u>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</u>

	<u>replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable. [NIST 800-63-2]</u>
<u>Off-line Attack</u>	<u>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. [NIST 800-63-2]</u>
<u>Online Attack</u>	<u>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. [NIST 800-63-2]</u>
<u>Online Guessing Attack</u>	<u>An attack in which an Attacker performs repeated logon trials by guessing possible values of the token authenticator. [NIST 800-63-2]</u>
<u>Operational Authority</u>	<u>The authority responsible for operations, maintenance, management and related functions within a Federated Identity Management system. [Derived from industry standard definitions]</u>
<u>Participant</u>	<u>A participating member of a Trust Framework for a Federated Identity Management system, including Registration Authorities, Credential Service Providers, and Relying Parties. [Derived from industry standard definitions]</u>
<u>Passive Attack</u>	<u>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). [NIST 800-63-2]</u>
<u>Password</u>	<u>A secret that a Claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. [NIST 800-63-2]</u>
<u>Personal Identification Number (PIN)</u>	<u>A password consisting only of decimal digits. [NIST 800-63-2]</u>
<u>Personal Identity Verification (PIV) Card</u>	<u>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). [NIST 800-63-2]</u>
<u>Personally Identifiable Information (PII)</u>	<u>Defined by GAO Report 08-536 as “Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.” [NIST 800-63-2]</u>
<u>Pharming</u>	<u>An attack in which an Attacker corrupts an infrastructure service such</u>

	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. [NIST 800-63-2]
<u>Phishing</u>	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. [NIST 800-63-2]
<u>Possession and control of a token</u>	The ability to activate and use the token in an authentication protocol. [NIST 800-63-2]
<u>Practice Statement</u>	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. [NIST 800-63-2]
<u>Privacy Enhancing Technology (PET)</u>	General term for a set of computer tools, applications and mechanisms which - when integrated in online services or applications, or when used in conjunction with such services or applications - allow online users to protect the privacy of their Personally Identifiable Information provided to and handled by such services or applications. [Wikipedia]
<u>Private Credentials</u>	Credentials that cannot be disclosed by the CSP because the contents can be used to compromise the token. [NIST 800-63-2]
<u>Private Key</u>	The secret part of an asymmetric key pair that is used to digitally sign or decrypt data. [NIST 800-63-2]
<u>Protected Session</u>	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 token in addition to the session keys, and if the other party can verify the identity associated with that token. If both Participants are authenticated, the protected session is said to be mutually authenticated. [NIST 800-63-2]
<u>Pseudonym</u>	A false name. All unverified names are assumed to be pseudonyms. [NIST 800-63-2]
<u>Public Credentials</u>	Credentials that describe the binding in a way that does not compromise the token. [NIST 800-63-2]
<u>Public Key</u>	The public part of an asymmetric key pair that is used to verify signatures or encrypt data. [NIST 800-63-2]

Comment [JG3]: Add definitions for privacy and security terms, such as "privacy enhancing," "non-linkability," etc. Collect additional terms and standard definitions from IMSAC members. (D. Burhop)

<u>Public Key Certificate</u>	<u>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. [NIST 800-63-2]</u>
<u>Public Key Infrastructure (PKI)</u>	<u>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. [NIST 800-63-2]</u>
<u>Registration</u>	<u>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. [NIST 800-63-2]</u>
<u>Registration Authority (RA)</u>	<u>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). [NIST 800-63-2]</u>
<u>Relying Party (RP)</u>	<u>An entity that relies upon the Subscriber's token 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. [NIST 800-63-2]</u>
<u>Remote</u>	<u>(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. [NIST 800-63-2]</u>
<u>Replay Attack</u>	<u>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. [NIST 800-63-2]</u>
<u>Risk Assessment</u>	<u>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. [NIST 800-63-2]</u>
<u>Salt</u>	<u>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. [NIST 800-63-2]</u>
<u>Secondary Authenticator</u>	<u>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. [NIST 800-63-2]</u>

<u>Secure Sockets Layer (SSL)</u>	<u>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. [NIST 800-63-2]</u>
<u>Security Assertion Mark-up Language (SAML)</u>	<u>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. See [SAML]. [NIST 800-63-2]</u>
<u>SAML Authentication Assertion</u>	<u>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. [NIST 800-63-2]</u>
<u>Session Hijack Attack</u>	<u>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. [NIST 800-63-2]</u>
<u>Shared Secret</u>	<u>A secret used in authentication that is known to the Claimant and the Verifier. [NIST 800-63-2]</u>
<u>Social Engineering</u>	<u>The act of deceiving an individual into revealing sensitive information by associating with the individual to gain confidence and trust. [NIST 800-63-2] Also, the ability to collect publically available information on individuals and engineering it in a way that enables discovery of passwords, PINs, and other identity secrets.</u>
<u>Special Publication (SP)</u>	<u>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. [NIST 800-63-2]</u>
<u>Strongly Bound Credentials</u>	<u>Credentials that describe the binding between a user and token in a tamper-evident fashion. [NIST 800-63-2]</u>
<u>Subscriber</u>	<u>A party who has received a credential or token from a CSP. [NIST 800-63-2]</u>
<u>Symmetric Key</u>	<u>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. [NIST 800-63-2]</u>
<u>Token</u>	<u>Something that the Claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the Claimant's identity. [NIST 800-63-2]</u>
<u>Token Authenticator</u>	<u>The output value generated by a token. The ability to generate valid token authenticators on demand proves that the Claimant possesses</u>

	and controls the token. Protocol messages sent to the Verifier are dependent upon the token authenticator, but they may or may not explicitly contain it. [NIST 800-63-2]
<u>Token Secret</u>	The secret value, contained within a token, which is used to derive token authenticators. [NIST 800-63-2]
<u>Transport Layer Security (TLS)</u>	An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by [RFC 2246], [RFC 3546], and [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. [NIST 800-63-2]
<u>Trust Anchor</u>	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). [NIST 800-63-2]
<u>Trust Framework</u>	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.” [§ 59.1-550] Trust frameworks consist of multiparty agreements among Participants in a Federated Identity Management system, which enforce requirements and ensure trust in the acceptance of identity credentials.
<u>Unlinkability</u>	A component in an identity management system that ensures that a user may make multiple uses of resources or services without others being able to link these uses together. Unlinkability requires that users are unable to determine whether the same user caused certain specific operations in the system. ² [International Organization for Standardization, ISO]
<u>Unverified Name</u>	An Applicant name that is not verified as meaningful by identity proofing. [NIST 800-63-2]
<u>Valid</u>	In reference to an ID, the quality of not being expired or revoked. [NIST 800-63-2]
<u>Verified Name</u>	An Applicant name that has been verified by identity proofing. [NIST 800-63-2]
<u>Verifier</u>	An entity that verifies the Claimant’s identity by verifying the Claimant’s possession and control of a token using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the token and identity and check their status. [NIST 800-63-2]

Comment [JG4]: Add definitions for privacy and security terms, such as “privacy enhancing,” “non-linkability,” etc. Collect additional terms and standard definitions from IMSAC members. (D. Burhop)

² ISO. 1999. Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408).

<u>Verifier Impersonation Attack</u>	<u>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. [NIST 800-63-2]</u>
<u>Weakly Bound Credentials</u>	<u>Credentials that describe the binding between a user and token in a manner than can be modified without invalidating the credential. [NIST 800-63-2]</u>
<u>Zeroize</u>	<u>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. [NIST 800-63-2]</u>
<u>Zero-knowledge Password Protocol</u>	<u>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. [NIST 800-63-2]</u>

5 Background

In 2015, Virginia’s General Assembly passed the Electronic Identity Management Act (Chapter 50, Code of Virginia) to address demand in the state’s digital economy for secure, privacy enhancing 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.

Comment [JG5]: Stronger “Why” statement with a focus on the opportunity afforded by the Act and IMSAC. (N. Moe)

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 **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

The purpose of this document is to establish minimum specifications for identity proofing and verification to enable registration and electronic authentication events within a **Federated Identity Management** system. The document assumes that the identity management system will be supported by a **Trust Framework**, compliant with Applicable Law.³

The document defines minimum requirements, components, process flows, levels of assurance and privacy and security provisions for identity proofing and verification. The document assumes that specific business, legal and technical requirements for identity proofing and verification will be established in the **Trust Framework** for each distinct identity management system, and that these requirements will be designed based on the specific **Level of Assurance** model supported by the system.

³ 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** of a **Federated Identity Management** system operates.

128 The document limits its focus to identity proofing and verification. Minimum specifications for
129 other components of an identity management system will be defined in separate IMSAC
130 guidance documents in this series, pursuant to §2.2-436 and §2.2-437.
131

DRAFT

6 Minimum Specifications

National Institute of Standards and Technology Special Publication 800-63-2 (NIST SP 800-63-2) defines “electronic authentication” (e-authentication) as “the process of establishing confidence in user identities electronically presented to an information system.”⁴ Information systems may use the authenticated identity to determine if that user is authorized to perform an electronic transaction.

E-authentication begins with *registration*. Registration generally consists of an *Applicant* applying to a *Registration Authority (RA)* to become a *Subscriber* of a *Credential Service Provider (CSP)*. The first step in the registration process involves identity proofing and verification of the Applicant by the RA. This process assumes a trusted relationship between the RA and CSP, with specific requirements for registration documented in the governing [Trust Framework](#) for the identity management system.

This document establishes minimum specifications for the identity proofing and verification components of a trust-based registration process. [Trust Frameworks](#) for identity management systems should document the business, legal and technical requirements for these components, as well as requirements for the remaining components of the system. Subsequent guidance documents in the IMSAC series will address other components of an identity management system, pursuant to §2.2-436 and §2.2-437.

Identity Proofing Requirements

Identity proofing and verification for registration should be designed to meet the specific requirements for each [Level of Assurance](#) defined by the governing [Trust Framework](#) for the identity management system.⁵ A trusted registration process ensures that (i) the RA and CSP have established the true identity of the Applicant, (ii) the registration protocols satisfy the requirements for each [Level of Assurance](#), (iii) [the RA and CSP maintain a record of the identity evidence and transaction flows to meet audit and compliance requirements](#), and (iv) [the RA and CSP implement enforcement mechanisms to ensure compliance with all applicable provisions established in the Trust Framework](#).

Comment [JG6]: Add language regarding maintenance of the record of the identity evidence. (M. Watson)

Comment [JG7]: Should there be a statement regarding enforcement? (L. Kimball)
Add a placeholder for enforcement. (T. Moran)

⁴ National Institute of Standards and Technology Special Publication 800-63-2 (NIST SP 800-63-2) may be accessed at <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>

⁵ The term “Level of Assurance” has been used in this document to describe the continuum for the degree of certainty in the user’s identity established by the RA during the registration process. The term aligns with the levels defined for federal agencies in the U.S. Office of Management and Budget Memorandum M04-04 and NIST SP 800-63-2 (i.e., Levels 1-4) but provides for a more general framework to accommodate other identity management standards and protocols.

166 At a minimum, identity proofing and verification requirements should establish that:
 167 • A person with the Applicant’s claimed attributes exists, and those attributes are sufficient to
 168 uniquely identify a single person;
 169 • The Applicant whose token is registered is in fact the person who is entitled to the identity;
 170 • It is difficult for the Claimant to later repudiate the registration and dispute an
 171 authentication using the Subscriber’s token.

172
 173 Registration, and the associated identity proofing and verification processes, may be completed
 174 through remote or in-person protocols. Provisions for remote versus in-person identity
 175 proofing and verification should be established in the [Trust Framework](#) for the identity
 176 management system and satisfy applicable [Level of Assurance](#) requirements.

177 Components and Process Flow

178
 179 The registration process, during which identity proofing and verification protocols are invoked,
 180 generally involve the following components:

- 181 • The Applicant’s assertion of an Identity Claim
- 182 • The Applicant’s presentation of evidence to prove the existence of the claimed identity
- 183 • The RA’s review and validation of the Applicant’s Identity Claim and supporting evidence
- 184 • The CSP’s verification of the Applicant’s Identity Claim
- 185 • The CSP’s issuance or registration of a credential bound to the Applicant’s identity token
- 186

187
 188 The process flow for implementing the components of the identity proofing and verification for
 189 registration generally consists of the following (**Figure 1**):

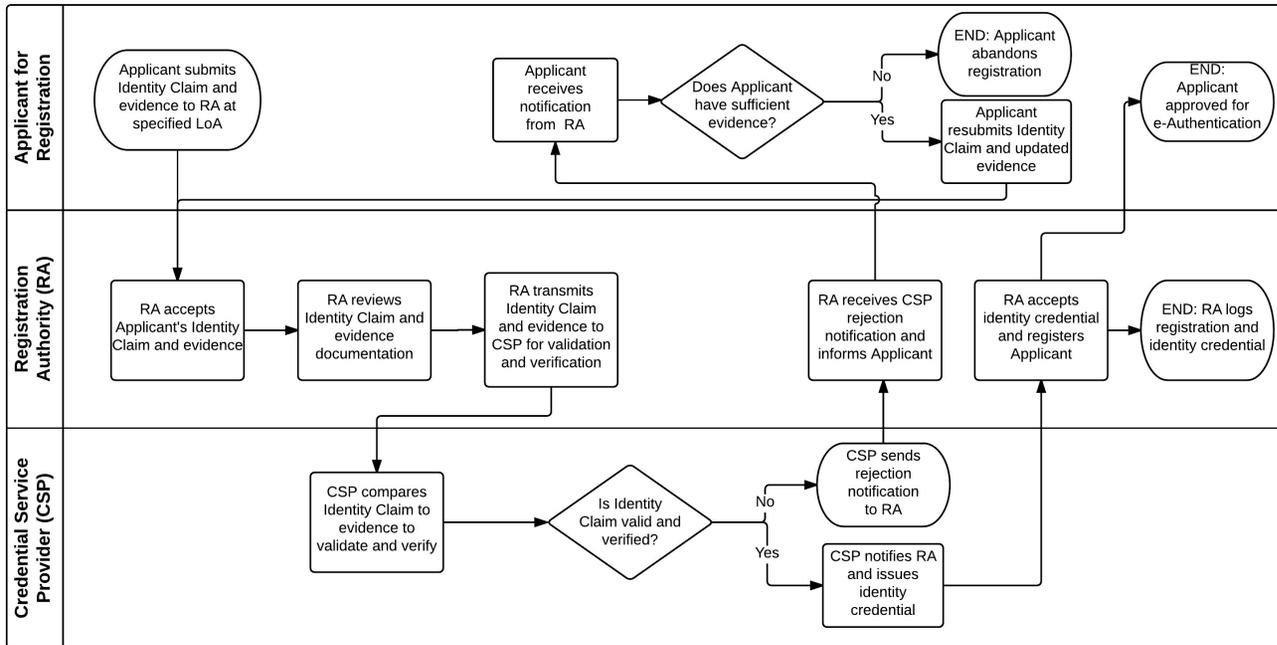
- 190 1. The Applicant asserts to the trusted RA an Identity Claim at a specified [Level of Assurance](#)
 191 (Identity Claim)
- 192 2. The Applicant provides the RA either remotely or in person, depending on [Level of](#)
 193 [Assurance](#) requirements, evidence to prove the existence of the claimed identity (Identity
 194 Proofing) [Note: Source of original identity document\(s\) must meet Level of Assurance and](#)
 195 [related compliance requirements set by the RA and defined in the Trust Framework](#)
- 196 3. The RA transmits the Identity Proofing evidence to the CSP to verify whether the evidence
 197 may be considered valid (Identity Validation)
- 198 4. The CSP compares the Applicant’s Identity Claim to information associated with the Identity
 199 Claim to determine whether it relates to the Applicant (Attribute Verification)⁶
- 200 5. Upon successful completion of the Attribute Verification process, the CSP issues to the RA a
 201 credential bound to a token for the Applicant, confirming the Applicant’s Identity Claim at
 202 the appropriate [Level of Assurance](#) (Credential Issuance or Registration)
- 203 6. [RA maintains a record of the evidence and transaction for the registration process.](#)

Comment [JG8]: Add a requirement statement regarding the source of the initial document. (M. Watson, K. Crepps, L. Kimball)

Comment [JG9]: Add language re maintenance of identity evidence. (M. Watson)

⁶ The Attribute Verification process may consist of multiple steps and factors, including attribute information, knowledge-based tests, biometrics, activity history, counter-fraud checks, etc., depending on [Level of Assurance](#) requirements. Specific Attribute Verification requirements should be defined in the governing [Trust Framework](#) for the identity management system. Minimum specifications for Attribute Verification will be addressed in a forthcoming guidance document in the IMSAC series, pursuant to §2.2-436 and §2.2-437.

Figure 1. Identity Proofing and Verification Process Flow



1 Levels of Assurance

2
3 The minimum specifications established in this document for identity proofing and verification
4 assume that **Trust Frameworks** for identity management systems will define a specific **Level of**
5 **Assurance** model.⁷ Therefore, the **Level of Assurance (LoA) Model** presented below should be
6 viewed as a recommended framework for identity proofing and verification in a registration
7 process. The LoA Model aligns with the Assurance Level Model published by the National
8 Association of State Chief Information Officers (NASCIO) in its State Identity Credential and
9 Access Management (SICAM) Guidance, **and** with OMB M04-04 and NIST SP 800-63 (**Figure 2**).⁸

10
11 **Level of Assurance 1**

12 LoA 1 has no identity proofing or verification requirement. Identity proofing and verification
13 protocols at LoA 1 provide only minimal assurance that the same Applicant is completing the
14 registration process.

15
16 Plaintext passwords or secrets are not transmitted across a network at LoA 1. However, this
17 level does not require cryptographic methods that block offline attacks by an eavesdropper. For
18 example, simple password challenge-response protocols are allowed. At LoA 1, long-term
19 shared authentication secrets may be revealed to verifiers. Assertions issued about Applicants
20 as a result of a successful identity proofing and verification are either cryptographically
21 authenticated by Relying Parties (using approved methods), or are obtained directly from a
22 trusted party via a secure registration protocol.

23
24 **Level of Assurance 2**

25 LoA 2 allows identity proofing and verification through a single factor remote network. At this
26 level, identity proofing and verification requirements are introduced, prompting the Applicant
27 to present identifying materials or information. A range of identity proofing and verification
28 technologies can be employed at LoA 2. This level allows any of the token methods of LoAs 3 or
29 4, as well as passwords and PINs. Successful identity proofing and verification requires the
30 Applicant to demonstrate control of the identity token through a secure registration protocol.

31
32 Long-term shared authentication secrets, if used, are never revealed to any party except the
33 Applicant and verifiers operated by the CSP; however, session (temporary) shared secrets may
34 be provided to independent verifiers by the CSP. Approved cryptographic techniques are
35 required. Assertions issued about Applicants as a result of a successful identity proofing and
36 verification are either cryptographically authenticated by Relying Parties (using approved
37 methods), or are obtained directly from a trusted party via a secure registration protocol.⁹

⁷ Trust Frameworks for identity management systems also should set requirements for how the LoA for each credential will be documented in the metadata for the credential to support audit and compliance.

⁸ The Assurance Level Model published by **NASCIO** in its SICAM Guidance **and Roadmap** may be accessed at <http://www.nascio.org/Portals/0/Publications/Documents/SICAM.pdf>.

⁹ The Commonwealth of Virginia has defined accepted cryptographic protocols in ITRM Information Security Policies, Standards, and Guidelines, which may be accessed at <http://www.vita.virginia.gov/default.aspx?id=537>

Formatted: Numbering: Continuous

Comment [JG10]: Add requirement statement addressing how the credential is denoted at an LOA and the audit provisions for maintaining that LOA reference. (M. Watson)

Comment [JG11R10]: See footnote

Comment [JG12]: Close the loop on what what constitutes approved cryptographic techniques, methods, etc. Reference adopted list. (M. Watson, L. Kimball)

Comment [JG13R12]: See footnote

Level of Assurance 3

Multi-factor remote network identity proofing and verification supported at this level. Identity proofing and verification procedures at LoA 3 require verification of identifying materials and information. LoA 3 is based on proof of possession of a key or a one-time password through a cryptographic protocol. Identity proofing and verification at this level requires cryptographic strength mechanisms that protect the primary identity token. A minimum of two Attribute Verification factors is required. While tokens may evolve, there are currently three kinds of tokens that may be used: “soft” cryptographic tokens, “hard” cryptographic tokens and “one-time password” device tokens.

LoA 3 requires that the Applicant prove through secure identity proofing and verification protocols that he or she controls the token, and must first unlock the token with a password or biometric, or must also use a password in a secure protocol, to establish two factor authentication. Long-term shared authentication secrets, if used, are never revealed to any party except the Applicant and verifiers operated directly by the CSP; however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are used for all operations. Assertions issued about Applicants as a result of a successful identity proofing and verification are either cryptographically authenticated by Relying Parties (using approved methods), or are obtained directly from a trusted party via secure registration protocols.

Level of Assurance 4

Highest practical remote network identity proofing and verification provided at this level. LoA 4 protocols are based on proof of possession of a key through a cryptographic protocol. LoA 4 is similar to LoA 3 except that only “hard” cryptographic tokens are required, Federal Information Processing Standard (FIPS) 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token must be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security.¹⁰ By requiring a physical token, which cannot readily be copied and because FIPS 140-2 requires operator authentication at LoA 2 and higher, LoA 4 ensures strong, two factor authentication.

LoA 4 requires strong cryptographic identity proofing and verification among all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used, as are biometrics. Registration requires that the Applicant prove through a secure authentication protocol that he or she controls the token. Long-term shared authentication secrets, if used, are never revealed to any party except the Applicant and verifiers operated directly by the CSP; however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Compliant cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the registration process.

¹⁰ Federal Information Processing Standard (FIPS) 140-2 may be accessed at <http://csrc.nist.gov/groups/STM/cmvp/standards.html>

79
80

Figure 2. SICAM Level of Assurance (LoA) Model

Comment [JG14]: Add “for example” language and table showing examples for each LOA. (T. Moran)

	Trust	Interoperability	Security	Process Improvement	
LoA 1	Issuing LoA 1 Identity	Single Entity Issuing LoA 1 Identity	Minimal to No Verification of Identity, Basic Credential	Minimal Identity Proofing, Verification, Attributes Collected	Identity/Credential
	Accepting LoA 1 Identity	Single Entity Use of LoA 1 Identity for Access	Access Control with Self-Asserted Credential	Minimal Access Efficiency Gains	Access Management
LoA 2	Issuing LoA 2 Identity	Single Entity Issuing LoA 2 Identity	Strong Verification of Identity and Basic Credential	Minimal Identity Proofing, Verification, Attributes Collected	Identity/Credential
	Accepting LoA 2 Credential	Multiple Entity Use of LoA 2 Credential for Physical Access	Access Control with LoA 2 Credential	Standardized Access Controls	Access Management
LoA 3	Issuing LoA 2/3 Credential and Digital Identity	Multiple Internal Points of Issuance	Strong Verification and Binding of Identity	Reduced Emphasis on Central Issuance	Identity/Credential
	Accepting LoA 2/3 Credential and Digital Identity	Multiple Entity Use of LoA 2/3 Credential and Digital Identity	Physical and Logical Access Control	Standardized Physical and Logical Access Controls	Access Management
LoA 4	Issuing LoA 4 Credential	Multiple Internal and External Points of Issuance	Highest Level of Verification and Binding	Widespread Issuance Reduces Internal Issuance Needs	Identity/Credential
	Accepting LoA 4 Credentials	Multiple Cross-Entity and Market Use of Credentials	Risk-Based Physical and Logical Access Controls	Achieving Business Process Improvements	Access Management

Source: NASCIO SICAM Guidance and Roadmap: <http://www.nascio.org/Portals/0/Publications/Documents/SICAM.pdf>

81
82
83

84 Privacy and Security

85

86 The minimum specifications established in this document for privacy and security in the use of
87 person information for identity proofing and verification apply the Fair Information Practice
88 Principles (FIPPs).¹¹ The FIPPs have been endorsed by the National Strategy for Trusted
89 Identities in Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.¹²

90

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

94

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

- 96 • Transparency: RAs and CSPs should be transparent and provide notice to Applicants
97 regarding collection, use, dissemination, and maintenance of person information required
98 during the registration, identity proofing and verification processes.
- 99 • Individual Participation: RAs and CSPs should involve the Applicant in the process of using
100 person information and, to the extent practicable, seek consent for the collection, use,
101 dissemination, and maintenance of that information. RAs and CSPs also should provide
102 mechanisms for appropriate access, correction, and redress of person information.
- 103 • Purpose Specification: RAs and CSPs should specifically articulate the authority that permits
104 the collection of person information and specifically articulate the purpose or purposes for
105 which the information is intended to be used.
- 106 • Data Minimization: RAs and CSPs should collect only the person information directly
107 relevant and necessary to accomplish the registration and related processes, and only retain
108 that information for as long as necessary to fulfill the specified purpose.
- 109 • Use Limitation/Minimal Disclosure: RAs and CSPs should use person information solely for
110 the purpose specified in the notice. Disclosure or sharing that information should be limited
111 to the specific purpose for which the information was collected.
- 112 • Data Quality and Integrity: RAs and CSPs should, to the extent practicable, ensure that
113 person information is accurate, relevant, timely, and complete.
- 114 • Security: RAs and CSPs should protect personal information through appropriate security
115 safeguards against risks such as loss, unauthorized access or use, destruction, modification,
116 or unintended or inappropriate disclosure.
- 117 • Accountability and Auditing: RAs and CSPs should be accountable for complying with these
118 principles, providing training to all employees and contractors who use person information,
119 and auditing the actual use of person information to demonstrate compliance with these
120 principles and all applicable privacy protection requirements.

Comment [JG15]: Should language for FIPPs be changed from "should" to "shall" or "must?" (L. Kimball)
Should IDESG IDEF Privacy and Security Requirements be included here? (J. Grant)
Keep FIPPs but incorporate IDEF requirements, as directed by IMSAC members (J. Grubbs)

Comment [JG16R15]: FIPPs kept, as published. IDESG IDEF Requirements added as Appendix 2.

¹¹ 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](#) for the identity management system.

¹² 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>.

121 7 Alignment Comparison

122
123 The minimum specifications for identity proofing and verification established in this document
124 have been developed to align with existing national and international standards for e-
125 authentication and identity management. Specifically, the minimum specifications reflect basic
126 requirements set forth in national standards at the federal and state level, ensuring compliance
127 while accommodating other identity management standards and protocols. This document
128 assumes that each [Federated Identity Management](#) system will comply with those governing
129 standards and protocols required by Applicable Law.

130
131 The following section outlines the alignment and disparities between the minimum
132 specifications in this document and core national standards. A crosswalk documenting the
133 alignment [and areas of misalignment](#) has been provided in **Appendix 3**.

134 135 NIST SP 800-63-2

136
137 The minimum specifications in this document conform with the basic requirements for identity
138 proofing and verification set forth in NIST SP 800-63-2. However, as the NIST guidance defines
139 specific requirements for federal agencies, the minimum specifications in this document
140 provide flexibility for [Federated Identity Management](#) systems across industries in the private
141 sector and levels of governance. This flexibility enables identity management systems to
142 adhere to the specifications but do so in a manner appropriate and compliant with their
143 governing [Trust Frameworks](#).

144 145 State Identity and Access Management Credential (SICAM) Guidance and Roadmap

146
147 The minimum specifications in this document conform with the basic requirements for identity
148 proofing and verification set forth by NASCIO in the SICAM Guidance and Roadmap. The
149 NASCIO guidance defines specific requirements for state agencies. Similar to the contrast with
150 the NIST guidance for federal agencies, the minimum specifications in this document provide
151 flexibility for [Federated Identity Management](#) systems across industries in the private sector
152 and levels of governance.

153 154 IDESG Identity Ecosystem Framework (IDEF) [Functional Model](#)

155
156 The minimum specifications in this document conform with the [core operations and](#) basic
157 requirements for privacy and security set forth by IDESG in the IDEF [Functional Model and](#)
158 Baseline Functional Requirements. The IDESG/IDEF requirements apply the FIPPs but extend
159 them to cover the Guiding Principles of the National Strategy for Trusted Identities in
160 Cyberspace (NSTIC). The minimum specifications in this document encourage adherence to the
161 IDEF [Functional Model](#), Baseline Functional Requirements and the NSTIC Guiding Principles.

162

163 Appendix 1. IMSAC Charter

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

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 [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.

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

207
208 The statutory authority and requirements for public notice and comment periods for guidance
209 documents have been established pursuant to § 2.2-437.C, as follows:

210
211 C. Proposed guidance documents and general opportunity for oral or written submittals as to
212 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published
213 in the Virginia Register of Regulations as a general notice following the processes and
214 procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§
215 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written
216 comments following the posting and publication and shall hold at least one meeting dedicated
217 to the receipt of oral comment no less than 15 days after the posting and publication. The
218 Advisory Council shall also develop methods for the identification and notification of interested
219 parties and specific means of seeking input from interested persons and groups. The Advisory
220 Council shall send a copy of such notices, comments, and other background material relative to
221 the development of the recommended guidance documents to the Joint Commission on
222 Administrative Rules.

223
224
225 This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the
226 minutes of the meeting and related IMSAC documents, visit:
227 <https://vita.virginia.gov/About/default.aspx?id=6442474173>

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

230

231 PRIVACY-1. DATA MINIMIZATION

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

237

238 PRIVACY-2. PURPOSE LIMITATION

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

244

245 PRIVACY-3. ATTRIBUTE MINIMIZATION

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

251

252 PRIVACY-4. CREDENTIAL LIMITATION

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

256

257 PRIVACY-5. DATA AGGREGATION RISK

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

263

264 PRIVACY-6. USAGE NOTICE

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

267

268 PRIVACY-7. USER DATA CONTROL

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

271 PRIVACY-8. THIRD-PARTY LIMITATIONS

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

276 PRIVACY-9. USER NOTICE OF CHANGES

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

283 PRIVACY-10. USER OPTION TO DECLINE

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

287 PRIVACY-11. OPTIONAL INFORMATION

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

291 PRIVACY-12. ANONYMITY

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

300 PRIVACY-13. CONTROLS PROPORTIONATE TO RISK

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

306 PRIVACY-14. DATA RETENTION AND DISPOSAL

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

313 PRIVACY-15. ATTRIBUTE SEGREGATION

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

315 SECURE-1. SECURITY PRACTICES

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

318
319 SECURE-2. DATA INTEGRITY

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

324
325 SECURE-3. CREDENTIAL REPRODUCTION

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

328
329 SECURE-4. CREDENTIAL PROTECTION

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

333
334 SECURE-5. CREDENTIAL ISSUANCE

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

340
341 SECURE-6. CREDENTIAL UNIQUENESS

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

344
345 SECURE-7. TOKEN CONTROL

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

348
349 SECURE-8. MULTIFACTOR AUTHENTICATION

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

352
353 SECURE-9. AUTHENTICATION RISK ASSESSMENT

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

356
357
358

359 SECURE-10. UPTIME
360 Entities that provide and conduct digital identity management functions MUST have established
361 policies and processes in place to maintain their stated assurances for availability of their
362 services.
363
364 SECURE-11. KEY MANAGEMENT
365 Entities that use cryptographic solutions as part of identity management MUST implement key
366 management policies and processes that are consistent with industry-accepted practices.
367
368 SECURE-12. RECOVERY AND REISSUANCE
369 Entities that issue credentials and tokens MUST implement methods for reissuance, updating,
370 and recovery of credentials and tokens that preserve the security and assurance of the original
371 registration and credentialing operations.
372
373 SECURE-13. REVOCATION
374 Entities that issue credentials or tokens MUST have processes and procedures in place to
375 invalidate credentials and tokens.
376
377 SECURE-14. SECURITY LOGS
378 Entities conducting digital identity management functions MUST log their transactions and
379 security events, in a manner that supports system audits and, where necessary, security
380 investigations and regulatory requirements. Timestamp synchronization and detail of logs
381 MUST be appropriate to the level of risk associated with the environment and transactions.
382
383 SECURE-15. SECURITY AUDITS
384 Entities MUST conduct regular audits of their compliance with their own information security
385 policies and procedures, and any additional requirements of law, including a review of their
386 logs, incident reports and credential loss occurrences, and MUST periodically review the
387 effectiveness of their policies and procedures in light of that data.
388

Appendix 3. Identity Proofing Standards Alignment Comparison Matrix

Comment [JG17]: Document alignment and lack of alignment; single table. (M. Watson, K. Crepps)

Component	NIST 800-63-2	SICAM	IDESG IDEF Functional Model
Applicant Identity Claim	<u>Alignment: Defines protocols and process flows for Applicant assertion of Identity Claim to federal agencies</u>	<u>Alignment: Defines protocols and process flows for Applicant assertion of Identity Claim to state agencies</u>	<u>Alignment: Identifies core operations within standard registration process flows for Applicant Identity Claim</u>
	<u>Misalignment: Federal protocols for Applicant's Identity Claim apply to federal agencies but may not be appropriate across sectors or private industry</u>	<u>Misalignment: Minor variations in terminology with Commonwealth's minimum specifications</u>	<u>Misalignment: Core operational definitions do not contain specific criteria for the process of Applicant assertion of Identity Claim</u>
Applicant Identity Evidence	<u>Alignment: Establishes rigorous requirements for what federal agencies may accept as Identity Evidence</u>	<u>Alignment: Establishes rigorous requirements for what state agencies may accept as Identity Evidence</u>	<u>Alignment: Defines core operations for Attribute Control and Identity Evidence, and for maintenance of records</u>
	<u>Misalignment: Federal requirements for acceptable Identity Evidence may not be appropriate across sectors or private industry</u>	<u>Misalignment: SICAM model provisions for acceptable Identity Evidence may not be appropriate across sectors or private industry</u>	<u>Misalignment: Core operational definitions do not contain specific criteria for acceptable Identity Evidence or maintenance of records</u>
RA Validation of Applicant Identity Claim	<u>Alignment: Sets protocols and required flows for federal agencies to follow in RA Validation of Identity Claim</u>	<u>Alignment: Sets protocols and required flows for state agencies to follow in RA Validation of Identity Claim</u>	<u>Alignment: Documents core operations for Validation of Identity Claim</u>
	<u>Misalignment: Federal protocols for RA Validation of Identity Claim may not be appropriate across sectors or private industry</u>	<u>Misalignment: SICAM model for RA Validation of Identity Claim may not be appropriate across sectors or private industry</u>	<u>Misalignment: Core operational definitions do not contain specific criteria for RA Validation of Identity Claim</u>
CSP Verification of Applicant Identity Claim	<u>Alignment: Provides clearly defined technical requirements for federal agencies to follow in CSP Verification of Identity Claim</u>	<u>Alignment: Provides clearly defined technical requirements for state agencies to follow in CSP Verification of Identity Claim</u>	<u>Alignment: Defines core operations for CSP Verification of Applicant Identity Claim</u>
	<u>Misalignment: Federal verification protocols and requirements may not be appropriate across sectors or private industry</u>	<u>Misalignment: SICAM model for CSP Verification of Identity Claim may not be appropriate across sectors or private industry</u>	<u>Misalignment: Core operational definitions do not contain specific criteria or technical requirements for CSP Verification</u>
CSP Issuance/Registration of Applicant Credential	<u>Alignment: Establishes protocols and technical requirements for issuance/ registration of Identity Credentials</u>	<u>Alignment: Establishes protocols and technical requirements for issuance/ registration of Identity Credentials</u>	<u>Alignment: Identifies core operational roles and responsibilities for Issuance/ Registration of Identity Credentials</u>
	<u>Misalignment: Federal Credential issuance/registration protocols may not be appropriate across sectors or private industry</u>	<u>Misalignment: State government Credential issuance/registration protocols may not be appropriate across sectors or private industry</u>	<u>Misalignment: Core operational roles and responsibilities do not contain specific criteria for audit and compliance purposes</u>