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

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

Version	Date	Revision Description
1.0	05/02/2016	Initial Draft of Document

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 will be reviewed by IMSAC during a council workshop, May 2, 2016.

- The document will be reviewed in a manner compliant with §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.

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 align with adopted definitions in the National Institute of Standards and Technology Special Publication 800-63-2 (NIST SP 800-63-2), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf. Terms used in this document not published in NIST SP 800-63-2 align with industry standard definitions.

Active Attack	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.
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 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. (See term in [ICAM] for more information.)
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 token 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 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 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.
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 authentication tokens 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. See [RFC 5280].
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."
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. Cookies are used for many purposes and may be assertions or may contain pointers to assertions. See Section 9.1.1 for more information.
Credential	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 between the Subscriber's token and identity.
Credential Service Provider (CSP)	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.
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 Token	A token 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 a token 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 (E-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. See Appendix A.
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	Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to

Management Act (FISMA)	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. See background information for more details. FIPS documents are available online through the FIPS home page: http://www.nist.gov/itl/fips.cfm
Federated Identity	The means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems.
Guessing Entropy	A measure of the difficulty that an Attacker has to guess the average password used in a system. In this document, 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 random quantity. The Attacker is assumed to know the actual password frequency distribution. See Appendix A.
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: 1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and 2. (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.
HTTPS	Protocol for secure communication over a computer network or the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or Secure Sockets Layer.
Identity	A set of attributes that uniquely describe a person within a given context.
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.

In-Person Identity Proofing	Method of identity proofing in which Applicants are required to present themselves and identity evidence documentation directly, at a physical location, to a representative of the Registration Authority. (Required for Level of Assurance 4 authentication.)
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 (KBA)	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.
Level of Assurance (LoA)	The continuum for the degree of certainty in the user's identity established by the Registration Authority during the registration process. 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) but provides for a more general framework to accommodate other identity management standards and protocols.
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.
Min-entropy	A measure of the difficulty that an Attacker has to guess the most commonly chosen password used in a system. In this document, 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).

	See Appendix A.
Multi-Factor	A characteristic of an authentication system or a token 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 token authenticator.
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)	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."
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 a token	The ability to activate and use the token 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 token. (For more discussion, see Section 7.1.1.)
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 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.
Pseudonym	A false name. In this document, all unverified names are assumed to be pseudonyms.
Public Credentials	Credentials that describe the binding in a way that does not compromise the token. (For more discussion, see Section 7.1.1.)
Public Key	The public part of an asymmetric key pair that is used to verify signatures or encrypt data.
Public Key	A digital document issued and digitally signed by the private key of a

Certificate	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 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.
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. See [SAML].
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 ability to collect publically available information on individuals and engineering it in a way that enables discovery of passwords, PINs, and other identity secrets. Also, 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 token in a tamper-evident fashion. (For more discussion, see Section 7.1.1.)
Subscriber	A party who has received a credential or token 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	Something that the Claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the Claimant’s identity.
Token Authenticator	The output value generated by a token. The ability to generate valid token authenticators on demand proves that the Claimant possesses 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.
Token Secret	The secret value, contained within a token, which is used to derive token authenticators.
Transport Layer Security (TLS)	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.
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 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.
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 token in a manner than can be modified without invalidating the credential. (For more discussion, see Section 7.1.1.)
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 Background

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 the Identity Management Standards Advisory Council (IMSAC). IMSAC was created by the General Assembly of the Commonwealth of Virginia in 2015 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 trust-based identity management system. The document assumes that the identity management system will be supported by a trust agreement, compliant with Applicable Law.[1]

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

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 agreement 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.

[1] For the purpose of this guidance document, the term "Applicable Law" shall mean laws, statutes, regulations and rules of the jurisdiction in which each participants of a trust-based identity management system operates.

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."[2] 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 agreement for the identity management system.

This document establishes minimum specifications for the identity proofing and verification components of a trust-based registration process. Trust agreements 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 agreement for the identity management system.[3] A trusted registration process ensures that (i) the RA and CSP have established the true identity of the Applicant and (ii) the registration protocols satisfy the requirements for each level of assurance.

At a minimum, identity proofing and verification requirements should establish that:

- A person with the Applicant's claimed attributes exists, and those attributes are sufficient to uniquely identify a single person;
- The Applicant whose token is registered is in fact the person who is entitled to the identity;
- It is difficult for the Claimant to later repudiate the registration and dispute an authentication using the Subscriber's token.

[2] 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

[3] 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.

Registration, and the associated identity proofing and verification processes, may be completed through remote or in-person protocols. Provisions for remote versus in-person identity proofing and verification should be established in the trust agreement for the identity management system and satisfy applicable level of assurance requirements.

Components and Process Flow

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

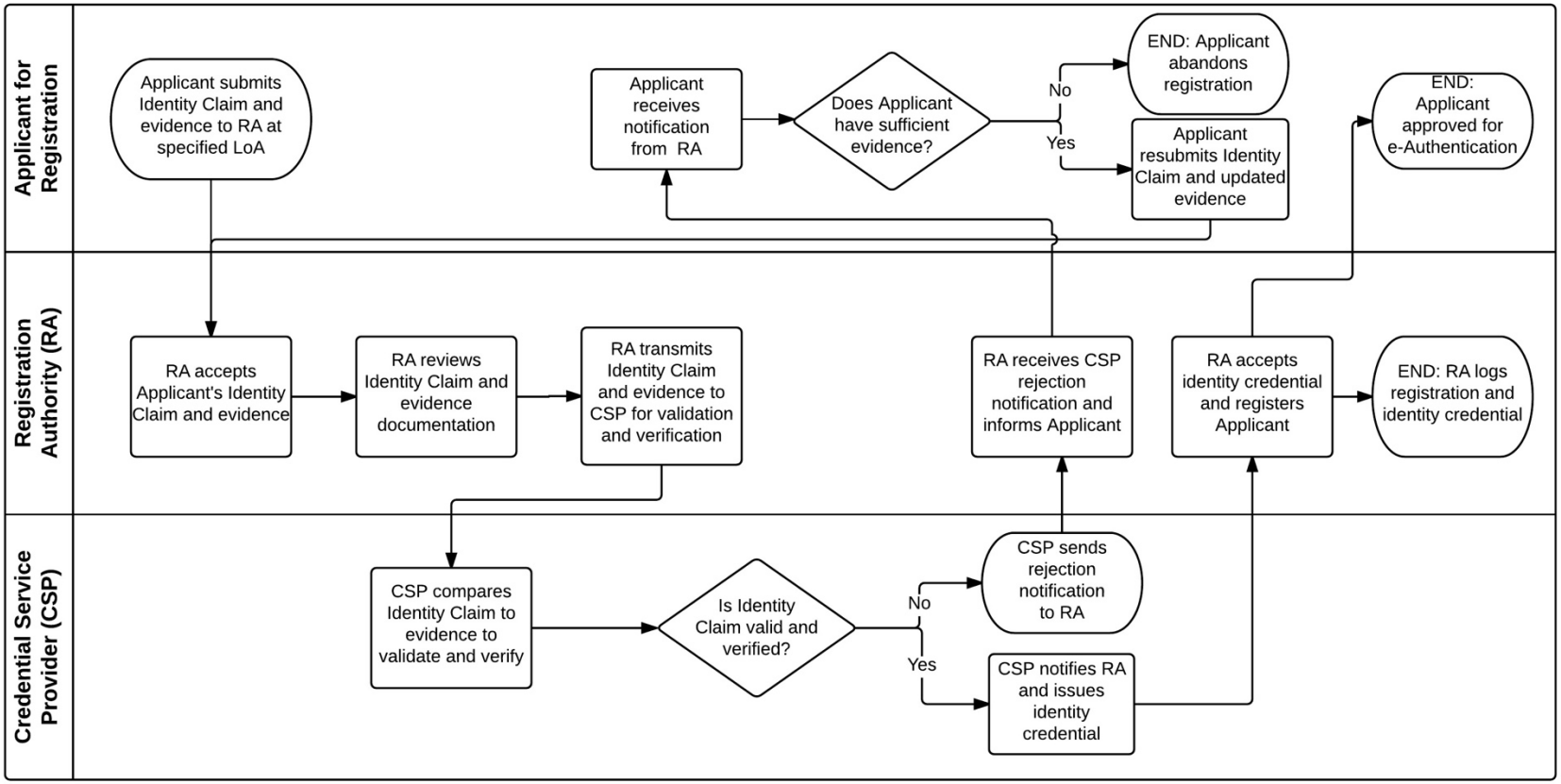
- The Applicant's assertion of an Identity Claim
- The Applicant's presentation of evidence to prove the existence of the claimed identity
- The RA's review and validation of the Applicant's Identity Claim and supporting evidence
- The CSP's verification of the Applicant's Identity Claim
- The CSP's issuance or registration of a credential bound to the Applicant's identity token

The process flow for implementing the components of the identity proofing and verification for registration generally consists of the following (see the process flow diagram in **Figure 1**):

1. The Applicant asserts to the trusted RA an Identity Claim at a specified level of assurance (Identity Claim)
2. The Applicant provides the RA either remotely or in person, depending on level of assurance requirements, evidence to prove the existence of the claimed identity (Identity Proofing)
3. The RA transmits the Identity Proofing evidence to the CSP to verify whether the evidence may be considered valid (Identity Validation)
4. The CSP compares the Applicant's Identity Claim to information associated with the Identity Claim to determine whether it relates to the Applicant (Attribute Verification)[4]
5. Upon successful completion of the Attribute Verification process, the CSP issues to the RA a credential bound to a token for the Applicant, confirming the Applicant's Identity Claim at the appropriate level of assurance (Credential Issuance or Registration)

[4] 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 agreement 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



Levels of Assurance

The minimum specifications established in this document for identity proofing and verification assume that trust agreements for identity management systems will define a specific level of assurance model. Therefore, the Level of Assurance (LoA) Model presented below should be viewed as a recommended framework for building identity proofing and verification protocols in a trust-based registration process. The LoA Model aligns with the Assurance Level Model published by the National Association of State Chief Information Officers (NASCIO) in its State Identity Credential and Access Management (SICAM) Guidance, as well as with OMB M04-04 and NIST SP 800-63.[5]

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

Plaintext passwords or secrets are not transmitted across a network at LoA 1. However, this level does not require cryptographic methods that block offline attacks by an eavesdropper. For example, simple password challenge-response protocols are allowed. At LoA 1, long-term shared authentication secrets may be revealed to verifiers. 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 a secure registration protocol.

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

Long-term shared authentication secrets, if used, are never revealed to any party except the Applicant and verifiers operated by the CSP; however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are required. 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 a secure registration protocol.

[5] The Assurance Level Model published by the National Association of State Chief Information Officers in its SICAM Guidance may be accessed at http://www.nascio.org/Portals/0/Publications/Documents/SICAM.pdf.

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.[6] By requiring a physical token, which cannot readily be copied and since 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. Strong approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the registration process.

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

Privacy and Security

The minimum specifications established in this document for privacy and security in the use of person information for identity proofing and verification apply the Fair Information Practice Principles (FIPPs).[7] The FIPPs have been endorsed by the National Strategy for Trusted Identities in Cyberspace (NSTIC) and the NASCIO in its SICAM Guidance.[8] The NSTIC FIPPs have been provided in **Appendix 2**.

The minimum specifications for identity proofing 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, 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 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.
- 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] 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 agreement for the identity management system.

[8] The minimum specifications established in this document 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, accessible at: https://workspace.idesg.org/kws/public/download/83/IDEF-Baseline-Requirements-v1.0-FINAL-10152015.pdf&wg_abbrev=idesg_document. 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.

7 Alignment Comparison

The minimum specifications for identity proofing and verification established in this document have been developed to align with existing national and international standards for e-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 trust-based 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 with national and internal standards has been provided in **Appendix 3**.

NIST SP 800-63-2

The minimum specifications in this document conform with the basic requirements for identity proofing and verification set forth in NIST SP 800-63-2. However, as the NIST guidance defines specific requirements for federal agencies, the minimum specifications in this document provide flexibility for trust-based 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 agreements.

State Identity and Access Management Credential (SICAM) Guidance

The minimum specifications in this document conform with the basic requirements for identity proofing and verification 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 trust-based identity management systems across industries in the private sector and levels of governance.

IDESG Identity Ecosystem Framework (IDEF) Core

The minimum specifications in this document conform with the basic requirements for privacy and security set forth by IDESG in the IDEF 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 provide encourage adherence to the IDEF Baseline Functional Requirements and the NSTIC Guiding Principles.

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 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. Fair Information Practice Principles (FIPPs)

To truly enhance privacy in the conduct of online transactions, Fair Information Practice Principles (FIPPs) must be universally and consistently adopted and applied in the Identity Ecosystem. FIPPs are the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy.[9]

In brief, the Fair Information Practice Principles are:

- Transparency: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
- Individual Participation: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
- Purpose Specification: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- Data Minimization: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- Use Limitation: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
- Data Quality and Integrity: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- Security: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- Accountability and Auditing: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Universal application of FIPPs provides the basis for confidence and trust in online transactions.

[9] National Institute of Standards and Technology, NSTIC FIPPs accessible at http://www.nist.gov/nstic/NSTIC-FIPPs.pdf

Appendix 3. Identity Proofing Standards Alignment Comparison Matrix