COMMONWEALTH OF VIRGINIA

Information Technology Resource Management (ITRM)

GUIDANCE DOCUMENT
Authenticators and Lifecycle Management

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 14
6 Minimum Specifications 15

1 Publication Version Control

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

Publication Version	Date	Revision Description
1.0	07/20/2016	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 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.

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

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

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][2] and this document, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

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

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

Asymmetric Keys: Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

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

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

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

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

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

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

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

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

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

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

Authenticator Secret: The secret value contained within an authenticator.

Authenticity: The property that data originated from its purported source.

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

Bit: A binary digit: 0 or 1.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Entropy: A measure of the amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Public Key Certificate: A digital document issued and digitally signed by the private key of a Certificate authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. See also [RFC 5280].

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

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

Registration Authority (RA): A trusted entity that establishes and vouches for the identity or attributes of a subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Token: See Authenticator.

Token Authenticator: See Authenticator Output.

Token Secret: See Authenticator Secret.

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

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

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

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

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

Verified Name: A subscriber name that has been verified by identity proofing.

Verifier: An entity that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the verifier may also need to validate credentials that link the authenticator(s) and identity and check their status.

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

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

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

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

5 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.

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 authenticators and lifecycle management within an identity management system. The document assumes that the identity management system will be supported by a trust framework, compliant with Applicable Law.[6] The minimum specifications have been stated based on language in NIST SP 800-63B.

The document defines minimum requirements, assurance levels, and privacy and security provisions for authenticators and lifecycle management. The document assumes that specific business, legal and technical requirements for authenticators will be established in the trust framework for each distinct identity management system, and that these requirements will be designed based on the Identity Assurance Level (IAL) and Authenticator Assurance Level (AAL) requirements for the system.

The document limits its focus to authenticators and lifecycle management. 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.

[6] For the purpose of this guidance document, the term "Applicable Law" shall mean laws, statutes, regulations and rules of the jurisdiction in which each participant in the identity management system operates.

6 Minimum Specifications

National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3) defines "electronic authentication" as "the process of establishing confidence in the identity of users or information systems."[7] Information systems may use the authenticated identity to determine if that user is authorized to perform an electronic transaction.

This document establishes minimum specifications for authenticators and lifecycle management conformant with, and using language from, NIST SP 800-63B. However, the minimum specifications defined in this document have been developed to accommodate requirements for authenticators established under other national and international standards.[8] The minimum specifications in this document also assume that specific business, legal and technical requirements for an identity management system will be documented in the trust framework for that system. Minimum specifications for other components of an identity management system have been documented in separate guidance documents in the IMSAC series, pursuant to §2.2-436 and §2.2-437.

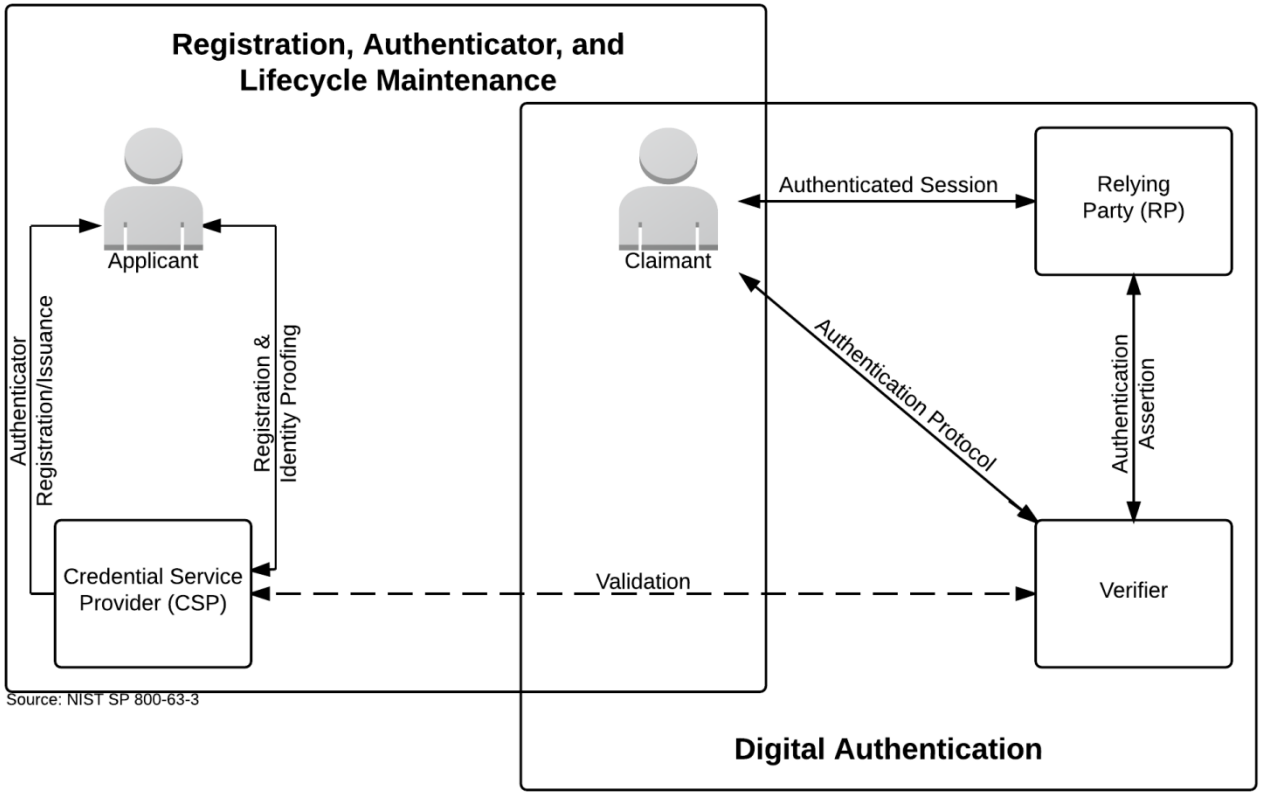
Electronic Authentication Model

Electronic authentication is the process of establishing confidence in individual identities presented to a digital system. The minimum specifications in this document assume that the authentication and transaction take place across a network. The electronic authentication model used for these minimum specifications has been shown in Figure 1. The minimum specifications for electronic authentication have been defined in *ITRM Guidance Document, Electronic Authentication*.

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

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

587 **Figure 1. Electronic Authentication Model**



588
589
590 Source: NIST SP 800-63-3, accessible at https://pages.nist.gov/800-63-3/sp800-63-3.html
591 Note: Figure 1 illustrates the model for electronic authentication in an identity management system, as documented in NIST SP 800-63-3
592 (Public Review), containing all components, requirements, and specifications recommended by IMSAC. However, the minimum
593 specifications defined in this document have been developed to accommodate requirements for authenticators and lifecycle management
594 established under other national and international standards.
595

Assurance Model

The minimum specifications defined in this document for authenticators and lifecycle management assume that the trust framework for an identity management system will define a specific assurance model for that system.[9] Therefore, the assurance model presented below, which is based on NIST SP 800-63-3, should be viewed as a recommended framework. Other assurance models have been established in OMB M-04-04 and the State Identity, Credential, and Access Management (SICAM) guidelines, published by the National Association of Chief Information Officers (NASCIO). A crosswalk showing disparities in the NIST SP 800-63-3, OMB M-04-04, and SICAM assurance models has been provided in **Figure 2**.

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

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

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

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

Authenticator Assurance Level 2 – AAL 2 provides higher assurance that the same claimant who participated in previous transactions is accessing the protected transaction or data. Two different authentication factors are required. Various types of authenticators, including multi-factor Software Cryptographic Authenticators, may be used as described in NIST 800-63B. AAL 2 also permits any of the authentication methods of AAL 3. AAL 2 authentication requires cryptographic mechanisms that protect the primary authenticator against compromise by the protocol threats for all threats at AAL 1 as well as verifier impersonation attacks. Approved cryptographic techniques are required for all assertion protocols used at AAL 2 and above.[10]

[9] Trust Frameworks for identity management systems also should set requirements for how the assurance for each credential will be documented in the medata for the credential to support audit and compliance.

[10] Approved cryptographic techniques shall be FIPS approved, NIST recommended, or otherwise compliant with Commonwealth IT Information Security Standard (SEC501): http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/HostedEnvironmentInformationSecurityStandardSEC52501.pdf

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

Figure 2. Assurance Model Crosswalk

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

Authenticator Assurance Levels

In order to satisfy the requirements of a given Authenticator Assurance Level (AAL), shown in Figure 2, a claimant must authenticate themselves with at least a given level of strength to be recognized as a subscriber. The result of an authentication process is an identifier, that may be pseudonymous, that must be used each time that subscriber authenticates to that relying party (RP). A summary of AAL requirements has been provided in **Figure 3**.

Authenticator Assurance Level 1

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

Permitted Authenticator Types – AAL 1

AAL 1 permits the use of any of the following authenticator types:

1. Memorized Secret
2. Look-up Secret
3. Out of Band (Partially deprecated)
4. Single Factor OTP Device
5. Multi-Factor OTP Device
6. Single Factor Cryptographic Device
7. Multi-Factor Software Cryptographic Authenticator
8. Multi-Factor Cryptographic Device

Authenticator and Verifier Requirements – AAL 1

Cryptographic authenticators used at AAL 1 must use approved cryptography.
Verifiers operated by government agencies at AAL 1 must be validated to meet the requirements of [FIPS 140] Level 1.

Assertion Requirements – AAL 1

In order to be valid at AAL 1, authentication assertions must meet the requirements defined in NIST SP 800-63C. Bearer assertions may be used.

Reauthentication – AAL 1

At AAL 1, reauthentication of the subscriber should be repeated at least once per 30 days, regardless of user activity.

Security Controls – AAL 1
The CSP should employ appropriately tailored security controls from the low baseline of security controls defined in [NIST SP 800-53] or equivalent industry standard and should ensure that the minimum assurance requirements associated with the *low* baseline are satisfied.

Records Retention – AAL 1
The CSP shall comply with their respective records retention policies in accordance with whatever laws and/or regulations apply. Otherwise, no retention period is required.

Authenticator Assurance Level 2
AAL 2 provides higher assurance that the same claimant who participated in previous transactions is accessing the protected transaction or data. At least two different authentication factors are required. Various types of authenticators, including multi-factor software cryptographic authenticators, may be used as described below. AAL 2 also permits any of the authentication methods of AAL 3. AAL 2 authentication requires cryptographic mechanisms that protect the primary authenticator against compromise by the protocol threats for all threats at AAL 1 as well as against verifier impersonation attacks. Approved cryptographic techniques are required at AAL 2 and above.

Permitted Authenticator Types – AAL 2
At AAL 2, it is required to have (a) a multi-factor authenticator, or (b) a combination of two single-factor authenticators.

When a multi-factor authenticator is used, any of the following may be used:

1. Multi-Factor OTP Device
2. Multi-Factor Software Cryptographic Authenticator
3. Multi-Factor Cryptographic Device

When a combination of two single-factor authenticators is used, it must include a Memorized Secret authenticator and one possession-based (“something you have”) authenticator from the following list:

- Look-up Secret
- Out of Band
- Single Factor OTP Device
- Single Factor Cryptographic Device

Note: The requirement for a memorized secret authenticator above derives from the need for two different types of authentication factors to be used. All biometric authenticators compliant with this specification are multi-factor, so something you know (a memorized secret) is the remaining possibility.

Authenticator and Verifier Requirements – AAL 2
Cryptographic authenticators used at AAL 2 must use approved cryptography. Authenticators developed by government agencies must be validated to meet the requirements of [FIPS 140] Level 1. Verifiers operated by government agencies at AAL 2 must be validated to meet the requirements of [FIPS 140] Level 1.

Assertion Requirements – AAL 2
In order to be valid at AAL 2, authentication assertions must meet the requirements defined in NIST SP 800-63C. Bearer assertions may be used.

Reauthentication – AAL 2
At AAL 2, authentication of the subscriber must be repeated at least once per 12 hours, regardless of user activity. Reauthentication of the subscriber must be repeated following no more than 30 minutes of user inactivity. The CSP may prompt the user to cause activity just before the inactivity timeout. Reauthentication may use a single authentication factor.

Security Controls – AAL 2
The CSP should employ appropriately tailored security controls from the moderate baseline of security controls defined in [NIST SP 800-53] or equivalent industry standard and should ensure that the minimum assurance requirements associated with the *moderate* baseline are satisfied.

Records Retention – AAL 2
CSPs shall comply with their respective records retention policies in accordance with whatever laws and/or regulations apply to those entities. Otherwise, retention of records is required for seven years and 6 months.

Authenticator Assurance Level 3
AAL 3 is intended to provide the highest practical remote network authentication assurance. Authentication at AAL 3 is based on proof of possession of a key through a cryptographic protocol. AAL 3 is similar to AAL 2 except that only “hard” cryptographic authenticators are allowed.

Permitted Authenticator Types – AAL 3
Authentication Assurance Level 3 requires the use of one of three kinds of hardware devices:

1. Multi-Factor OTP Device
2. Multi-Factor Cryptographic Device
3. Single-Factor Cryptographic Device used in conjunction with Memorized Secret

Authenticator and Verifier Requirements – AAL 3
Multi-factor authenticators used at AAL 3 must be hardware cryptographic modules validated at [FIPS 140] Level 2 or higher overall with at least [FIPS 140] Level 3 physical security. Single-factor cryptographic devices used at AAL 3 must be validated at [FIPS 140] Level 1 or higher overall with at least [FIPS 140] Level 3 physical security. These requirements may be met by

using the PIV authentication key of a [FIPS 201] compliant Personal Identity Verification (PIV) Card. Verifiers at AAL 3 must be validated at [FIPS 140] Level 1 or higher.

Assertion Requirements – AAL 3

In order to be valid at AAL 3, authentication assertions must meet the requirements of proof-of-possession assertions as defined in NIST SP 800-63C.

Reauthentication – AAL 3

At AAL 3, authentication of the subscriber must be repeated at least once per 12 hours, regardless of user activity. Reauthentication of the subscriber must be repeated following a period of no more than 15 minutes of user inactivity. It is permissible to prompt the user to cause activity just before the inactivity timeout.

Security Controls – AAL 3

The CSP should employ appropriately tailored security controls from the high baseline of security controls defined in [NIST SP 800-53] or an equivalent industry standard and should ensure that the minimum assurance requirements associated with the *high* baseline are satisfied.

Records Retention – AAL 3

The CSP shall comply with their respective records retention policies in accordance with whatever laws and/or regulations apply to those entities. Otherwise, retention of records is required for ten years and 6 months.

798 **Figure 3. Summary of AAL Requirements**

799

Requirement	AAL 1	AAL 2	AAL 3
Authenticator types	Memorized Secret Look-up Secret Out of Band SF OTP Device MF OTP Device SF Cryptographic Device MF Software Cryptographic Authenticator MF Cryptographic Device	MF OTP Device MF Software Cryptographic Authenticator MF Cryptographic Device or memorized secret plus: Look-up Secret Out of Band SF OTP Device SF Cryptographic Device	MF OTP Device MF Cryptographic Device SF Cryptographic Device plus Memorized Secret
FIPS 140 verification	Level 1 (Government agency verifiers)	Level 1 (Government agency authenticators and verifiers)	Level 2 overall (MF authenticators) Level 1 overall (Verifiers and SF Crypto Devices) Level 3 physical security (all authenticators)
Assertions	Bearer or proof of possession	Bearer or proof of possession	Proof of possession only
Reauthentication	30 days	12 hours or 30 minutes inactivity; may use one authentication factor	12 hours or 15 minutes inactivity; must use both authentication factors
Security Controls	[SP 800-53] Low Baseline (or equivalent)	[SP 800-53] Moderate Baseline (or equivalent)	[SP 800-53] High Baseline (or equivalent)
Records Retention	Not required	7 years, 6 months	10 years, 6 months

800

Authenticator and Verifier Requirements

The minimum specifications defined in this document for authenticators establish the following requirements for each authenticator type. The technical requirements for each authenticator type are the same regardless of the AAL.

Requirements by Authenticator Type

Memorized Secrets

A Memorized Secret authenticator (commonly referred to as a *password* or *PIN* if it is numeric) is a secret value that is intended to be chosen and memorizable by the user. Memorized secrets need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value.

Memorized Secret Authenticators

Memorized secrets must be at least 8 characters in length if chosen by the subscriber; memorized secrets chosen randomly by the CSP or verifier must be at least 6 characters in length and may be entirely numeric. Some values for user-chosen memorized secrets may be disallowed based on their appearance on a blacklist of compromised values. No other complexity requirements for memorized secrets are imposed.

Memorized Secret Verifiers

Verifiers must require subscriber-chosen memorized secrets to be at least 8 characters in length. Verifiers must permit user-chosen memorized secrets to be at least 64 characters in length. All printing ASCII [RFC 20] characters as well as the space character must be acceptable in memorized secrets; Unicode [ISO/ISC 10646:2014] characters should be accepted as well.

Verifiers may remove space characters prior to verification; all other characters must be considered significant. Truncation of the secret must not be performed. For purposes of the above length requirements, each Unicode code point must be counted as a single character. Memorized secrets that are randomly chosen by the CSP (e.g., at enrollment) or by the verifier (e.g., when a user requests a new PIN) must be at least 6 characters in length and must be generated using an approved random number generator.

Memorized secret verifiers must not permit the subscriber to store a “hint” that is accessible to an unauthenticated claimant. Verifiers also must not prompt subscribers to use specific types of information (e.g., “What was the name of your first pet?”) when choosing memorized secrets.

When processing requests to establish and change memorized secrets, verifiers should compare the prospective secrets against a dictionary of known commonly-used and/or compromised values. This list should include passwords from previous breach corpuses, as well as dictionary words and specific words (such as the name of the service itself) that users are likely to choose. If the chosen secret is found in the dictionary, the subscriber should be

required to choose a different value. The subscriber should be advised that they need to select a different secret because their previous choice was commonly used.

Verifiers must implement a throttling mechanism that effectively limits the number of failed authentication attempts an attacker can make on the subscriber's account.

Verifiers should not impose other composition rules (mixtures of different character types, for example) on memorized secrets. Verifiers should not require memorized secrets to be changed arbitrarily (e.g., periodically) unless there is evidence of compromise of the authenticator or a subscriber requests a change.

In order to assist the claimant in entering a memorized secret successfully, the verifier should offer an option to display the secret (rather than a series of dots or asterisks, typically) as it is typed. The verifier must hide the character after it is displayed for a time sufficient for the claimant to see the character. This allows the claimant to verify their entry if they are in a location where their screen is unlikely to be observed.

Verifiers must use approved encryption and must authenticate themselves to the claimant (e.g., through the use of a X.509 certificate using approved encryption that is acceptable to the claimant) when requesting memorized secrets in order to provide resistance to eavesdropping and phishing attacks.

Verifiers must store memorized secrets in a form that is resistant to offline attacks. Secrets must be hashed with a *salt* value using an approved hash function such as PBKDF2 as described in [SP800-132]. The salt value must be a 32 bit (or longer) random value generated by an approved random number generator and is stored along with the hash result. At least 10,000 iterations of the hash function should be performed. A keyed hash function (e.g., HMAC), with the key stored separately from the hashed authenticators (e.g., in a hardware security module) should be used to further resist dictionary attacks against the stored hashed authenticators.

Look-up Secrets

A look-up secret authenticator is a physical or electronic record that stores a set of secrets shared between the claimant and the CSP. The claimant uses the authenticator to look up the appropriate secret(s) needed to respond to a prompt from the verifier. For example, a claimant may be asked by the verifier to provide a specific subset of the numeric or character strings printed on a card in table format.

Look-up Secret Authenticators

CSPs creating look-up secret authenticators must use an approved random number generator to generate the list of secrets, and must deliver the authenticator securely to the subscriber. Look-up secrets must have at least 64 bits of entropy, or must have at least 20 bits of entropy if the number of failed authentication attempts is limited as described in Section 5.2.2.
If the authenticator uses look-up secrets sequentially from a list, the subscriber may dispose of used secrets, but only after a successful authentication.

Look-up Secret Verifiers

Verifiers of look-up secrets must prompt the claimant for the next secret from their authenticator or for a specific (i.e., numbered) secret. A given secret from an authenticator must be used successfully only once; therefore, a given authenticator can only be used for a finite number of successful authentications. If the look-up secret is derived from a grid card, each cell of the grid must be used only once.

Verifiers must store look-up secrets in a form that is resistant to offline attacks. Secrets must be hashed with a "salt" value using an approved hash function as described in [SP 800-132]. The "salt" value must be a 32 bit (or longer) random value generated by an approved random number generator that is stored along with the hash result. A keyed hash function (e.g., HMAC [FIPS198-1]), with the key stored separately from the hashed authenticators (e.g., in a hardware security module) should be used to further resist dictionary attacks against the stored hashed authenticators.

Look-up secrets must be generated using an approved random number generator and must have at least 20 bits of entropy. When look-up secrets have less than 64 bits of entropy, the verifier must implement a throttling mechanism that effectively limits the number of failed authentication attempts an attacker can make on the subscriber's account.

Verifiers must use approved encryption and must authenticate themselves to the claimant (e.g., through the use of a X.509 certificate using approved encryption that is acceptable to the claimant) when requesting look-up secrets in order to provide resistance to eavesdropping and phishing attacks.

Out of Band

An Out of Band authenticator is a physical device that is uniquely addressable and can receive a verifier-selected secret for one-time use. The device is possessed and controlled by the claimant and supports private communication over a secondary channel that is separate from the primary channel for e-authentication.

The out-of-band authenticator can operate in one of two ways:

- The claimant presents the secret that was received by the out-of-band authenticator to the verifier using the primary channel for e-authentication.
- The claimant sends a response to the verifier from the out-of-band authenticator via the secondary communications channel.

Two key requirements are that the device be uniquely addressable and that communication over the secondary channel be private. Some voice-over-IP telephone services can deliver text messages and voice calls without the need for possession of a physical device; these must not be used for out of band authentication. Mechanisms such as smartphone applications employing secure communications protocols are preferred for out-of-band authentication.

If the authenticator responds directly to the verifier via the secondary communications channel, the verifier must send and the authenticator must display information, such as a transaction ID or description, allowing the claimant to uniquely associate the authentication operation on the primary channel with the request on the secondary channel.

Ability to receive email messages or other types of instant message does not generally prove the possession of a specific device, so they must not be used as out of band authentication methods.

Out of Band Authenticators

The out of band authenticator must establish an authenticated protected channel in order to retrieve the out of band secret or authentication request. This channel is considered to be out of band with respect to the primary communication channel, even if it terminates on the same device, provided the device does not leak information from one to the other.

The out of band authenticator must uniquely authenticate itself in one of the following ways in order to receive the authentication secret:

- Authentication to the verifier using approved cryptography. The key should be stored in the most secure storage available on the device (e.g., keychain storage, trusted platform module, or trusted execution environment if available).
- Authentication to a public mobile telephone network using a SIM card or equivalent that uniquely identifies the device

Out of band authenticators should not display the authentication secret on a device that is locked by the owner (i.e., requires an entry of a PIN or passcode). However, authenticators may indicate the receipt of an authentication secret on a locked device.

If the out of band authenticator sends an approval message over the secondary communication channel (rather than by the claimant transferring a received secret to the primary communication channel):

- The authenticator must display identifying information about the authentication transaction to the claimant prior to their approval.
- The secondary communication channel must be an authenticated protected channel.

Out of Band Verifiers

Out of band verifiers must generate a random authentication secret with at least 20 bits of entropy using an approved random number generator. They then optionally signal the device containing the subscriber's authenticator to indicate readiness to authenticate.

If the out of band verification is to be made using a SMS message on a public mobile telephone network, the verifier must verify that the pre-registered telephone number being used is actually associated with a mobile network and not with a VoIP (or other software-based) service. It then sends the SMS message to the pre-registered telephone number.

Changing the pre-registered telephone number must not be possible without two-factor authentication at the time of the change.

If out of band verification is to be made using a secure application (e.g., on a smart phone), the verifier may send a push notification to that device. The verifier then waits for a establishment of an authenticated protected channel and verifies the authenticator's identifying key. The verifier must not store the identifying key itself, but must use a verification method such as hashing (using an approved hash function) or proof of possession of the identifying key to uniquely identify the authenticator. Once authenticated, the verifier transmits the authentication secret to the authenticator.

Depending on the type of out-of-band authenticator, either:

- The verifier waits for the secret to be returned on the primary communication channel.
- The verifier waits for the secret, or some type of approval message, to be returned over the secondary communication channel.

If approval is made over the secondary communication channel, the request to the verifier must include a transaction identifier, such as a transaction ID or description, for display by the verifier.

In collecting the authentication secret from the claimant, the verifier must use approved encryption and must authenticate itself to the claimant. The authentication secret must be considered invalid if not received within 5 minutes.

If the authentication secret has less than 64 bits of entropy, the verifier must implement a throttling mechanism that effectively limits the number of failed authentication attempts an attacker can make on the subscriber's account as described in Section 5.2.2.

Single Factor OTP Device

A single factor OTP device is a hardware device that supports the time-based generation of one-time passwords. This includes software-based OTP generators installed on devices such as mobile phones. This device has an embedded secret that is used as the seed for generation of one-time passwords and does not require activation through a second factor. Authentication is accomplished by using the authenticator output (i.e., the one-time password) in an authentication protocol, thereby proving possession and control of the device. A one-time password device may, for example, display 6 characters at a time.

Single factor OTP devices are similar to look-up secret authenticators with the exception that the secrets are cryptographically generated by the authenticator and verifier and compared by the verifier. The secret is computed based on a nonce that may be time-based or from a counter on the authenticator and verifier.

Single Factor OTP Authenticators

Single factor OTP authenticators contain two persistent values. The first is a symmetric key that persists for the lifetime of the device. The second is a nonce that is changed each time the authenticator is used or is based on a real-time clock.

The secret key must be of at least the minimum approved length as defined in the latest revision of [SP 800-131A] (currently 112 bits). The nonce must be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.

The authenticator output is obtained by using an approved block cipher or hash function to combine the key and nonce in a secure manner. The authenticator output may be truncated to as few as 6 decimal digits (approximately 20 bits of entropy).

If the nonce used to generate the authenticator output is based on a real-time clock, the nonce must be changed at least once every 2 minutes. The OTP value associated with a given nonce must be accepted only once.

If the authenticator supplies its output via an electronic interface such as USB, it should require a physical input (e.g., pressing a button on the device) to cause a one-time password to be generated.

Single Factor OTP Verifiers

Single factor OTP verifiers effectively duplicate the process of generating the OTP used by the authenticator. As such, the symmetric keys used by authenticators are also present in the verifier, and must be strongly protected against compromise.

In collecting the OTP from the claimant, the verifier must use approved encryption and must authenticate itself to the claimant.

If the authenticator output has less than 64 bits of entropy, the verifier must implement a throttling mechanism that effectively limits the number of failed authentication attempts an attacker can make on the subscriber's account as described in Section 5.2.2.

Multi-Factor OTP Devices

A multi-factor (MF) OTP device hardware device generates one-time passwords for use in authentication and requires activation through a second factor of authentication. The second factor of authentication may be achieved through some kind of integral entry pad, an integral biometric (e.g., fingerprint) reader or a direct computer interface (e.g., USB port). The one-time password is typically displayed on the device and manually input to the verifier, although direct electronic output from the device as input to a computer is also allowed. For example, a one-time password device may display 6 characters at a time. The MF OTP device is *something you have*, and it may be activated by either *something you know* or *something you are*.

Multi-Factor OTP Authenticators

Multi-factor OTP authenticators operate in a similar manner to single-factor OTP authenticators, except that they require the entry of either a memorized secret or use of a biometric to obtain a password from the authenticator. Each use of the authenticator must require the input of the additional factor.

The authenticator output must have at least 6 decimal digits (approximately 20 bits) of entropy. The output must be generated by using an approved block cipher or hash function to combine a symmetric key stored on a personal hardware device with a nonce to generate a one-time password. The nonce may be based on the date and time or on a counter generated on the device.

Any memorized secret used by the authenticator for activation must be at least 6 decimal digits (approximately 20 bits) in length or of equivalent complexity. A biometric activation factor must meet the requirements of Section 5.2.3, including limits on number of successive authentication failures.

The unencrypted key and activation secret or biometric sample (and any biometric data derived from the biometric sample such as a probe produced through signal processing) must be immediately erased from storage immediately after a password has been generated.

Multi-Factor OTP Verifiers

Multi-factor OTP verifiers effectively duplicate the process of generating the OTP used by the authenticator, but without the requirement that a second factor be provided. As such, the symmetric keys used by authenticators must be strongly protected against compromise. In collecting the OTP from the claimant, the verifier must use approved encryption and must authenticate itself to the claimant. Time-based one-time passwords must have a lifetime of less than 2 minutes.

If the authenticator output or activation secret has less than 64 bits of entropy, the verifier must implement a throttling mechanism that effectively limits the number of failed authentication attempts an attacker can make on the subscriber's account.

Single Factor Cryptographic Devices

A single-factor cryptographic device is a hardware device that performs cryptographic operations on input provided to the device. This device does not require activation through a second factor of authentication. This device uses embedded symmetric or asymmetric cryptographic keys. Authentication is accomplished by proving possession of the device. The authenticator output is highly dependent on the specific cryptographic device and protocol, but it is generally some type of signed message.

Single Factor Cryptographic Device Authenticators

Single-factor cryptographic device authenticators encapsulate a secret key that is unique to the device and must not be exportable (removed from the device). They operate by signing a challenge nonce, usually presented through a direct computer interface such as a USB port. The secret key must be of at least the minimum approved length as defined in the latest revision of [SP 800-131A] (currently 112 bits). The challenge nonce must be at least 64 bits in length. The authenticator output is normally provided via a computer interface (usually the same one from which the challenge value was received).

Single-factor cryptographic device authenticators should require a physical input such as the pressing of a button in order to operate. This provides defense against unintended operation of the device, which might occur if the device to which it is connected is compromised.

Single Factor Cryptographic Device Verifiers

Single-factor cryptographic device verifiers generate a challenge nonce, send it to the corresponding authenticator, and use the authenticator output to verify possession of the device. The authenticator output is highly dependent on the specific cryptographic device and protocol, but it is generally some type of signed message.

The verifier contains either symmetric or asymmetric public keys corresponding to each authenticator. While both types of keys must be protected against modification, symmetric keys must additionally be strongly protected against unauthorized disclosure.

The challenge nonce must be at least 64 bits in length, and must either be unique over the lifetime of the authenticator or statistically unique (generated using an approved random number generator).

Multi-Factor Cryptographic Software

A multi-factor software cryptographic authenticator is a cryptographic key is stored on disk or some other “soft” media that requires activation through a second factor of authentication. Authentication is accomplished by proving possession and control of the key. The authenticator output is highly dependent on the specific cryptographic protocol, but it is generally some type of signed message. The MF software cryptographic authenticator is *something you have*, and it may be activated by either *something you know* or *something you are*.

Multi-Factor Cryptographic Software Authenticators

Multi-factor software cryptographic authenticators encapsulate a secret key that is unique to the authenticator and is accessible only through the input of an additional factor, either a memorized secret or a biometric. The key should be stored in the most secure storage available on the device (e.g., keychain storage, trusted platform module, or trusted execution environment if available). Each authentication operation using the authenticator must require the input of the additional factor.

Any memorized secret used by the authenticator for activation must be at least 6 decimal digits (approximately 20 bits) in length or of equivalent complexity.

The unencrypted key and activation secret or biometric sample (and any biometric data derived from the biometric sample such as a probe produced through signal processing) must be immediately erased from storage immediately after an authentication transaction has taken place.

Multi-Factor Cryptographic Software Verifiers

The requirements for a multi-factor cryptographic software verifier are identical to those for a multi-factor cryptographic device verifier, described in Section 5.1.8.2.

Multi-Factor Cryptographic Devices

A multi-factor cryptographic device is a hardware device that contains a protected cryptographic key that requires activation through a second authentication factor. Authentication is accomplished by proving possession of the device and control of the key. The authenticator output is highly dependent on the specific cryptographic device and protocol, but it is generally some type of signed message. The MF Cryptographic device is *something you have*, and it may be activated by either *something you know* or *something you are*.

Multi-Factor Cryptographic Device Authenticators

Multi-factor cryptographic device authenticators use tamper-resistant hardware to encapsulate a secret key that is unique to the authenticator and is accessible only through the input of an additional factor, either a memorized secret or a biometric.

Each authentication operation using the authenticator should require the input of the additional factor. Input of the additional factor may be accomplished via either direct input on the device or via a hardware connection (e.g., USB or smartcard).

Any memorized secret used by the authenticator for activation must be at least 6 decimal digits (approximately 20 bits) in length or of equivalent complexity. A biometric activation factor must meet the requirements of Section 5.2.3, including limits on number of successive authentication failures.

The unencrypted key and activation secret or biometric sample (and any biometric data derived from the biometric sample such as a probe produced through signal processing) must be immediately erased from storage immediately after an authentication transaction has taken place.

Multi-Factor Cryptographic Device Verifiers

Multi-factor cryptographic device verifiers generate a challenge nonce, send it to the corresponding authenticator, and use the authenticator output to verify possession of the device and activation factor. The authenticator output is highly dependent on the specific cryptographic device and protocol, but it is generally some type of signed message.

The verifier contains either symmetric or asymmetric public keys corresponding to each authenticator. While both types of keys must be protected against modification, symmetric keys must additionally be strongly protected against unauthorized disclosure.
The challenge nonce must be at least 64 bits in length, and must either be unique over the lifetime of the authenticator or statistically unique (generated using an approved random number generator). The verification operation must use approved cryptography.

General Authenticator Requirements

Physical Authenticators
CSPs must provide subscriber instructions on how to appropriately protect the authenticator against theft or loss. The CSP must provide a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected.

Rate Limiting (Throttling)
When the authenticator output or activation secret does not have sufficient entropy, the verifier must implement controls to protect against online guessing attacks. Unless otherwise specified in the description of a given authenticator, the verifier must effectively limit online attackers to 100 consecutive failed attempts on a single account in any 30-day period.

Additional techniques may be used to prioritize authentication attempts that are likely to come from the subscriber over those that are more likely to come from an attacker:

- Requiring the claimant to complete a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) before attempting authentication
- Requiring the claimant to wait for a short period of time (anything from 30 seconds to an hour, depending on how close the system is to its maximum allowance for failed attempts) before attempting Authentication following a failed attempt
- Only accepting authentication requests from a white list of IP addresses at which the subscriber has been successfully authenticated before
- Leveraging other risk-based or adaptive authentication techniques to identify user behavior that falls within, or out of, typical norms.

Since these measures often create user inconvenience, the verifier should allow a certain number of failed authentication attempts before employing the above techniques.
When the subscriber successfully authenticates, the verifier should disregard any previous failed attempts from the same IP address.

Use of Biometrics
For a variety of reasons, this document supports only limited use of biometrics for authentication. These include:

- Biometric False Match Rates (FMR) and False Non-Match Rates (FNMR) do not provide confidence in the authentication of the subscriber by themselves. In addition, FMR and FNMR do not account for spoofing attacks.

- Biometric matching is probabilistic, whereas the other authentication factors are deterministic.
- Biometric template protection schemes provide a method for revoking biometric credentials that are comparable to other authentication factors (e.g., PKI certificates and passwords). However, the availability of such solutions is limited, and standards for testing these methods are under development.
- Biometric characteristics do not constitute secrets. They can be obtained online or by taking a picture of someone with a camera phone (e.g. facial images) with or without their knowledge, lifted from through objects someone touches (e.g., latent fingerprints), or captured with high resolution images (e.g., iris patterns for blue eyes). While presentation attack detection (PAD) technologies such as liveness detection can mitigate the risk of these types of attacks, additional trust in the sensor is required to ensure that PAD is operating properly in accordance with the needs of the CSP and the subscriber.

Therefore, the use of biometrics for authentication is supported, with the following requirements and guidelines:

- Biometrics must be used with another authentication factor (something you know or something you have).
- Testing of the biometric system to be deployed must demonstrate an equal error rate of **1 in 1000** or better with respect to matching performance. The biometric system must operate with a false match rate of **1 in 1000** or better.
- When the biometric sensor and subsequent processing are not part of an integral unit that resists replacement of the sensor, the sensor must demonstrate that it is a certified or qualified sensor meeting these requirements by authenticating itself to the processing element.
- Testing of the biometric system to be deployed must demonstrate at least 90% resistance to presentation attacks for each relevant attack type (aka species), where resistance is defined as the number of thwarted presentation attacks divided by the number of trial presentation attacks. The biometric system must implement presentation attack protection (PAD).
- The biometric system must allow no more than 10 consecutive failed authentication attempts. Once that limit has been reached, the claimant must be required to use a different authenticator or to activate their authenticator with a different factor such as a memorized secret.
- Biometric matching should be performed locally on claimant's device or may be performed at a central verifier.

If matching is performed centrally:

- Use of the biometric must be bound tightly to a single, specific device that is identified using approved cryptography.
- Biometric revocation must be implemented.

- An authenticated protected channel between sensor and central verifier must be established, and the sensor authenticated, **prior** to capturing the biometric sample from the claimant.
- All transmission of biometrics shall be over the authenticated protected channel.

Biometric samples collected in the authentication process may be used to train matching algorithms or, with user consent, for other research purposes. Biometric samples (and any biometric data derived from the biometric sample such as a probe produced through signal processing) must be immediately erased from storage immediately after a password has been generated.

Biometrics are also used in some cases to prevent repudiation of registration and to verify that the same individual participates in all phases of the registration process as described in NIST SP 800-63A.

Attestation

Authenticators that are directly connected to or embedded in endpoints may convey attestation information such as the provenance or health and integrity of the authenticator (and possibly the endpoint as well) to the verifier as part of the authentication protocol. If this attestation is signed, the verifier should validate its signature. This information may be used as part of a risk-based authentication decision.

When federated authentication is being performed as described in NIST SP 800-63C, the verifier should include any such attestation information in the assertion it provides to the relying party.

Authenticator Lifecycle Management

During the lifecycle of an authenticator bound to a subscriber's identity, a number of events may occur that affect the use of that authenticator. These events include binding, loss, theft, unauthorized duplication, expiration, and revocation. This section describes the actions that must be taken in response to those events.

Authenticator binding

Authenticators may be provided by a CSP as part of a process such as enrollment; in other cases, the subscriber may provide their own, such as software or hardware cryptographic modules. For this reason, we refer to the *binding* of an authenticator rather than the issuance, but this does not exclude the possibility that an authenticator is issued as well.

Throughout the online identity lifecycle, CSPs must maintain a record of all authenticators that are or have been associated with the identity. It must also maintain the information required for throttling authentication attempts when required.

The record created by the CSP must contain the date and time the authenticator was bound to the account and should include information about the binding, such as the IP address or other device identifier associated with the enrollment. It should also contain information about unsuccessful authentications attempted with the authenticator.

Registration

The following requirements apply when an authenticator is bound to an identity as a result of a successful identity proofing transaction, as described in NIST SP 800-63A.

At IAL 2, the CSP must bind at least one, and should bind at least two, authenticators to the subscriber's online identity. Binding of multiple authenticators is preferred in order to recover from loss or theft of their primary authenticator. While at IAL 1 all identifying information is self-asserted, creation of online material or an online reputation makes it undesirable to lose control of an account as result of the loss of an authenticator. The second authenticator makes it possible to securely recover from that situation.

At IAL 2 and above, identifying information is associated with the online identity and the subscriber has undergone an identity proofing process as described in NIST SP 800-63A. Authenticators at the same AAL as the desired IAL must be bound to the account. For example, if the subscriber has successfully completed proofing at IAL 2, AAL 2 or 3 authenticators are appropriate to bind to the IAL 2 identity. As above, the availability of additional authenticators provides backup methods of authentication if an authenticator is lost or stolen.

Registration and binding may be broken up into a number of separate physical encounters or electronic transactions. (Two electronic transactions are considered to be separate if they are not part of the same protected session.)

In these cases, the following methods must be used to ensure that the same party acts as applicant throughout the processes:

1. For remote transactions:
    a. The applicant must identify himself/herself in each new transaction by presenting a temporary secret which was established during a prior transaction or encounter, or sent to the Applicant's phone number, email address, or postal address of record.
    b. Permanent secrets shall only be issued to the Applicant within a protected session.
2. For physical transactions:
    a. The applicant must identify himself/herself in person by either using a secret as described above, or through the use of a biometric that was recorded during a prior encounter.
    b. Temporary secrets must not be reused.
    c. If the CSP issues permanent secrets during a physical transaction, then they must be loaded locally onto a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record.

Post-Registration Binding

Following registration, binding an additional authenticator to an account requires the use of an existing authenticator of the same type (or types). For example, binding a new single-factor OTP device requires the subscriber to authenticate with another *something you have* authentication factor. If the account has only one authentication factor bound to it (which is possible only at IAL 1/AAL 1), an additional authenticator of the same factor may be bound to it.

Binding an additional authenticator must require the use of two different authentication factors, except as provided below.

If the subscriber has only one of the two authentication factors, they must repeat the identity proofing process, using the remaining authentication and should verify knowledge of some information collected during the proofing process to bind to the existing identity. In order to reestablish authentication factors at IAL 3, they must verify the biometric collected during the proofing process.

Binding Identity to a Subscriber Provided Authenticator

In some instances, a claimant may already possess authenticators at a suitable AAL without having been proofed at the equivalent IAL. For example, a user may have a two-factor authenticator from a social network provider, considered AAL2 and IAL1, and would like to use those credentials at a relying party that requires IAL2.

The following requirements apply when a claimant choses to increase IAL in order to bind to a suitable authenticator they already have.

1. The CSP may accept an existing authenticator at or above the desired IAL
2. The CSP must require the user to authenticate using their existing authenticator

3. The CSP must execute all required identity proofing processes for the desired IAL
4. If the user successfully completes identity proofing, the CSP may issue an enrollment code (temporary secret) that confirms address of record as per 800-63-A, Section 5.3.1, Address Confirmation Requirements, **OR** may request the claimant to register their own authenticator by proving proof of possession (for example, activating a private key by physically touching the token)

Renewal

The CSP should bind an updated authenticator an appropriate amount of time in advance of an existing authenticator's expiration. The process for this should conform closely to the initial authenticator issuance process (e.g., confirming address of record, etc.). Following successful use of the new authenticator, the CSP may revoke the authenticator that it is replacing.

Loss, Theft, and Unauthorized Duplication

Loss, theft, and unauthorized duplication of an authenticator are handled similarly, because in most cases one must assume that a lost authenticator has potentially been stolen or recovered by someone that is not the legitimate claimant of the authenticator. One notable exception is when a memorized secret is forgotten without other indication of having been compromised (duplicated by an attacker).

To facilitate secure reporting of loss or theft of an authenticator, the CSP should provide the subscriber a method to authenticate to the CSP using a backup authenticator; either a memorized secret or a physical authenticator may be used for this purpose (only one authentication factor is required for this purpose). Alternatively, the subscriber may establish an authenticated protected channel to the CSP and verify information collected during the proofing process. Alternatively, the CSP may verify an address of record (email, telephone, or postal) and suspend authenticator(s) reported to have been compromised. The suspension must be reversible if the subscriber successfully authenticates to the CSP and requests reactivation of an authenticator suspended in this manner.

Expiration

CSP's should issue authenticators that expire. When an authenticator expires, it must not be usable for authentication. When an authentication is attempted, the CSP should give an indication to the subscriber that the authentication failure is due to expiration rather than some other cause.

The CSP must require subscribers to surrender any physical authenticator containing trustable attributes as soon as practical after expiration or after receipt of a renewed authenticator.

Revocation

CSPs must revoke the binding of authenticators promptly when an online identity ceases to exist or when requested by the subscriber.

Privacy and Security

The minimum specifications established in this document for privacy and security in the use of person information for electronic authentication apply the Fair Information Practice Principles (FIPPs).[11] The FIPPs have been endorsed by the National Strategy for Trusted Identities in Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.[12]

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

The minimum specifications for identity proofing 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.

[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.

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

PRIVACY-1. DATA MINIMIZATION
Entities MUST limit the collection, use, transmission and storage of personal information to the minimum necessary to fulfill that transaction's purpose and related legal requirements. Entities providing claims or attributes MUST not provide any more personal information than what is requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to accommodate information requests of variable granularity, to support data minimization.

PRIVACY-2. PURPOSE LIMITATION
Entities MUST limit the use of personal information that is collected, used, transmitted, or stored to the specified purposes of that transaction. Persistent records of contracts, assurances, consent, or legal authority MUST be established by entities collecting, generating, using, transmitting, or storing personal information, so that the information, consistently is used in the same manner originally specified and permitted.

PRIVACY-3. ATTRIBUTE MINIMIZATION
Entities requesting attributes MUST evaluate the need to collect specific attributes in a transaction, as opposed to claims regarding those attributes. Wherever feasible, entities MUST collect, generate, use, transmit, and store claims about USERS rather than attributes. Wherever feasible, attributes MUST be transmitted as claims, and transmitted credentials and identities MUST be bound to claims instead of actual attribute values.

PRIVACY-4. CREDENTIAL LIMITATION
Entities MUST not request USERS' credentials unless necessary for the transaction and then only as appropriate to the risk associated with the transaction or to the risks to the parties associated with the transaction.

PRIVACY-5. DATA AGGREGATION RISK
Entities MUST assess the privacy risk of aggregating personal information, in systems and processes where it is collected, generated, used, transmitted, or stored, and wherever feasible, MUST design and operate their systems and processes to minimize that risk. Entities MUST assess and limit linkages of personal information across multiple transactions without the USER's explicit consent.

PRIVACY-6. USAGE notICE
Entities MUST provide concise, meaningful, and timely communication to USERS describing how they collect, generate, use, transmit, and store personal information.

PRIVACY-7. USER DATA CONTROL
Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete personal information.

PRIVACY-8. THIRD-PARTY LIMITATIONS
Wherever USERS make choices regarding the treatment of their personal information, those choices MUST be communicated effectively by that entity to any THIRD-PARTIES to which it transmits the personal information.

PRIVACY-9. USER notICE OF CHANGES
Entities MUST, upon any material changes to a service or process that affects the prior or ongoing collection, generation, use, transmission, or storage of USERS' personal information, notify those USERS, and provide them with compensating controls designed to mitigate privacy risks that may arise from those changes, which may include seeking express affirmative consent of USERS in accordance with relevant law or regulation.

PRIVACY-10. USER OPTION TO DECLINE
USERS MUST have the opportunity to decline registration; decline credential provisioning; decline the presentation of their credentials; and decline release of their attributes or claims.

PRIVACY-11. OPTIONAL INFORMATION
Entities MUST clearly indicate to USERS what personal information is mandatory and what information is optional prior to the transaction.

PRIVACY-12. ANONYMITY
Wherever feasible, entities MUST utilize identity systems and processes that enable transactions that are anonymous, anonymous with validated attributes, pseudonymous, or where appropriate, uniquely identified. Where applicable to such transactions, entities employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES collecting USER personal information. Organizations MUST request individuals' credentials only when necessary for the transaction and then only as appropriate to the risk associated with the transaction or only as appropriate to the risks to the parties associated with the transaction.

PRIVACY-13. CONTROLS PROPORTIONATE TO RISK
Controls on the processing or use of USERS' personal information MUST be commensurate with the degree of risk of that processing or use. A privacy risk analysis MUST be conducted by entities who conduct digital identity management functions, to establish what risks those functions pose to USERS' privacy.

PRIVACY-14. DATA RETENTION AND DISPOSAL
Entities MUST limit the retention of personal information to the time necessary for providing and administering the functions and services to USERS for which the information was collected, except as otherwise required by law or regulation. When no longer needed, personal information MUST be securely disposed of in a manner aligning with appropriate industry standards and/or legal requirements.

PRIVACY-15. ATTRIBUTE SEGREGATION
Wherever feasible, identifier data MUST be segregated from attribute data.

SECURE-1. SECURITY PRACTICES
Entities MUST apply appropriate and industry-accepted information security STANDARDS, guidelines, and practices to the systems that support their identity functions and services.

SECURE-2. DATA INTEGRITY
Entities MUST implement industry-accepted practices to protect the confidentiality and integrity of identity data—including authentication data and attribute values—during the execution of all digital identity management functions, and across the entire data lifecycle (collection through destruction).

SECURE-3. CREDENTIAL REPRODUCTION
Entities that issue or manage credentials and tokens MUST implement industry-accepted processes to protect against their unauthorized disclosure and reproduction.

SECURE-4. CREDENTIAL PROTECTION
Entities that issue or manage credentials and tokens MUST implement industry-accepted data integrity practices to enable individuals and other entities to verify the source of credential and token data.

SECURE-5. CREDENTIAL ISSUANCE
Entities that issue or manage credentials and tokens MUST do so in a manner designed to assure that they are granted to the appropriate and intended USER(s) only. Where registration and credential issuance are executed by separate entities, procedures for ensuring accurate exchange of registration and issuance information that are commensurate with the stated assurance level MUST be included in business agreements and operating policies.

SECURE-6. CREDENTIAL UNIQUENESS
Entities that issue or manage credentials MUST ensure that each account to credential pairing is uniquely identifiable within its namespace for authentication purposes.

SECURE-7. TOKEN CONTROL
Entities that authenticate a USER MUST employ industry-accepted secure authentication protocols to demonstrate the USER's control of a valid token.

SECURE-8. MULTIFACTOR AUTHENTICATION
Entities that authenticate a USER MUST offer authentication mechanisms which augment or are alternatives to a password.

SECURE-9. AUTHENTICATION RISK ASSESSMENT
Entities MUST have a risk assessment process in place for the selection of authentication mechanisms and supporting processes.

SECURE-10. UPTIME
Entities that provide and conduct digital identity management functions MUST have established policies and processes in place to maintain their stated assurances for availability of their services.

SECURE-11. KEY MANAGEMENT
Entities that use cryptographic solutions as part of identity management MUST implement key management policies and processes that are consistent with industry-accepted practices.

SECURE-12. RECOVERY AND REISSUANCE
Entities that issue credentials and tokens MUST implement methods for reissuance, updating, and recovery of credentials and tokens that preserve the security and assurance of the original registration and credentialing operations.

SECURE-13. REVOCATION
Entities that issue credentials or tokens MUST have processes and procedures in place to invalidate credentials and tokens.

SECURE-14. SECURITY LOGS
Entities conducting digital identity management functions MUST log their transactions and security events, in a manner that supports system audits and, where necessary, security investigations and regulatory requirements. Timestamp synchronization and detail of logs MUST be appropriate to the level of risk associated with the environment and transactions.

SECURE-15. SECURITY AUDITS
Entities MUST conduct regular audits of their compliance with their own information security policies and procedures, and any additional requirements of law, including a review of their logs, incident reports and credential loss occurrences, and MUST periodically review the effectiveness of their policies and procedures in light of that data.