



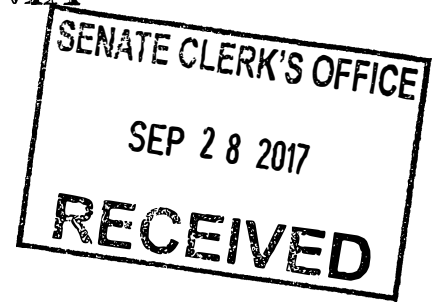
Document

COMMONWEALTH of VIRGINIA

Office of the Governor

Karen R. Jackson
Secretary of Technology

August 30, 2017



The Honorable Frank W. Wagner
Chairman, Joint Commission on Administrative Rules
P.O. Box 68008
Virginia Beach, VA 23471

Karen Perrine, Esquire
Joint Commission on Administrative Rules
Pocahontas Building
8th Floor
900 E. Main Street
Richmond, VA 23219

RE: Guidance Documents on Commonwealth Identity Management Standards

Dear Senator Wagner and Ms. Perrine:

I am writing to submit five guidance documents on Commonwealth identity management standards (enclosed), which were developed and recommended by the Identity Management Standards Advisory Council (Advisory Council) pursuant to section 2.2-437 of the *Code of Virginia*.

Section 2.2-436 of the *Code of Virginia* requires the Secretary of Technology, in consultation with the Secretary of Transportation, to review and approve or disapprove, upon the recommendation of the Advisory Council, guidance documents that (1) adopt nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions, and (2) the minimum specifications and standards that should be included in an identity trust framework so as to warrant liability protection pursuant to the Electronic Identity Management Act (§§ 59.1-550 to -555). Section 2.2-436 also requires the Secretary of Technology to provide you with a copy of final guidance documents at least 90 days prior to the effective date of such guidance documents.

Honorable Frank W. Wagner
Karen Perrine, Esquire
August 30, 2017
Page 2


Upon receipt of the Advisory Council's recommendation and in consultation with the Secretary of Transportation, I approved the enclosed five guidance documents on August 30, 2017. The effective date of these guidance documents is December 1, 2017.

For your ease of reference, the provision requiring submission of final guidance documents to the Joint Commission is paragraph (B) of section 2.2-436 of the *Code of Virginia*, which provides as follows:

- B. Final guidance documents approved pursuant to subsection A shall be posted on the Virginia Regulatory Town Hall and published in the Virginia Register of Regulations as a general notice. The Secretary of Technology shall send a copy of the final guidance documents to the Joint Commission on Administrative Rules established pursuant to § 30-73.1 at least 90 days prior to the effective date of such guidance documents. The Secretary of Technology shall also annually file a list of available guidance documents developed pursuant to this chapter pursuant to § 2.2-4008 of the Virginia Administrative Process Act (§ 2.2-4000 et seq.) and shall send a copy of such list to the Joint Commission on Administrative Rules.

If you have any comments or questions about this, please do not hesitate to contact me.

Sincerely,



Karen Jackson

Enclosures:

IMSAC Guidance Document 1: Digital Authentication
IMSAC Guidance Document 1.A: Identity Proofing and Verification
IMSAC Guidance Document 1.B: Authenticators and Lifecycle Management
IMSAC Guidance Document 1.C: Digital Identity Assertions
IMSAC Guidance Document 2: Identity Trust Frameworks

cc: The Honorable Susan C. Schaar, Clerk of the Senate ✓
The Honorable G. Paul Nardo, Clerk of the House

COMMONWEALTH OF VIRGINIA



IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

GUIDANCE DOCUMENT 1 Digital Authentication

In accordance with Section 2.2-436 of the *Code of Virginia*, the Secretary of Technology, after consultation with the Secretary of Transportation, approved this Guidance Document regarding digital authentication. This Guidance Document shall be effective as of December 1, 2017 and shall remain in force and effect unless rescinded or amended by further action pursuant to Section 2.2-436 of the *Code of Virginia*.

Table of Contents

1	Publication Version Control	1
2	Reviews	1
3	Purpose and Scope	2
4	Statutory Authority	3
5	Terminology and Definitions	4
6	Background	5
7	Minimum Specifications	6
8	Alignment Comparison	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
1.0	09/12/2016	Document revised by VITA staff based on public comment received pursuant to § 2.2-437.C, <i>Code of Virginia</i>
1.0	09/30/2016	Document revised by VITA staff based on comments from IMSAC during September 12, 2016, public meeting
1.0	12/05/2016	Document revised based on direction from VITA's Legal and Legislative Services Directorate and the Office of the Attorney General following September 12, 2016, public meeting
1.0	05/01/2017	Document revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by the Identity Management Standards Advisory Council (IMSAC)
1.0	06/05/2017	Document recommended by IMSAC for adoption by the Secretary of Technology

2 Reviews

- The initial version of the document was prepared by staff from the Virginia Information Technologies Agency (VITA) at the direction of the Identity Management Standards Advisory Council (IMSAC).
- The document was revised based on public comment received in written and verbal form during the 30-day comment period, pursuant to § 2.2-437.C.
- The document was revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by IMSAC.

3 Purpose and Scope

Pursuant to §§ 2.2-436 and 2.2-437, this guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to establish minimum specifications for digital identity systems so as to warrant liability protection pursuant to the Electronic Identity Management Act ("the Act"), §§ 59.1-550 to -555. This guidance document was prepared to provide information or guidance of general applicability to the public for interpreting or implementing the Act. This guidance document was not developed as a Commonwealth of Virginia Information Technology Resource Management (ITRM) Policy, Standard, and Guideline, pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive branch agencies of the Commonwealth of Virginia.

The minimum specifications in this guidance document conform with the digital identity guidelines found in the March 31, 2017, Public Review version of the National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3). IMSAC will continue to monitor modifications to NIST SP 800-63-3 and may recommend to the Secretary of Technology revisions to the minimum specifications in order to maintain consistency with the NIST guidance.

4 Statutory Authority

The following section documents the statutory authority established in the Code of Virginia for the development of minimum specifications and standards for the authentication process within a digital identity system. References to statutes below and throughout this document shall be to the Code of Virginia, unless otherwise specified.

Governing Statutes:

Secretary of Technology

§ 2.2-225. Position established; agencies for which responsible; additional powers

<http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225/>

Identity Management Standards Advisory Council

§ 2.2-437. Identity Management Standards Advisory Council

<http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/>

Commonwealth Identity Management Standards

§ 2.2-436. Approval of electronic identity standards

<http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/>

Electronic Identity Management Act

Chapter 50. Electronic Identity Management Act

<http://law.lis.virginia.gov/vacode/title59.1/chapter50/>

5 Terminology and Definitions

The core terms used within the digital identity management domain may be assigned a wide range of definitions, depending on the context or community of interest. For the purpose of the IMSAC guidance document series, the terminology has been defined in the IMSAC Reference Document: Terminology and Definitions, which may be accessed at <http://vita.virginia.gov/default.aspx?id=6442475952>

The IMSAC terminology aligns with the definitions published in the following documents:

- National Institute of Standards and Technology Special Publication 800-63-3 March 31, 2017 Public Review version, available at <https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3>
- Electronic Identity Management Act (§ 59.1-550), available at <http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550>
- International Telecommunication Union, Recommendation X. 1255, available at <http://www.itu.int/ITU-T/recommendations/rec.aspx?id=11951&lang=en>

6 Background

In 2015, the Virginia General Assembly passed the Electronic Identity Management Act (§§ 59.1-550 to -555) to address demand in the state's digital economy for secure, privacy enhancing digital authentication and identity management. Growing numbers of communities of interest have advocated for stronger, scalable and interoperable identity solutions to increase consumer protection and reduce liability for principal actors in the identity ecosystem – identity providers, credential service providers and relying parties.

To address the demand contemplated by the Electronic Identity Management Act, the General Assembly created the Identity Management Standards Advisory Council (IMSAC) to advise the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to §2.2-436. A copy of the IMSAC Charter has been provided in **Appendix 1**.

IMSAC 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 to -555); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

Purpose Statement

This guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to provide information or guidance of general applicability to the public for interpreting or implementing the Electronic Identity Management Act. Specifically, the document establishes minimum specifications for authentication within a digital identity system. The minimum specifications conform with NIST SP 800-63-3.

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

This guidance document focuses on digital authentication. Separate IMSAC guidance documents in this series define minimum specifications for other components of a digital identity system.

7 Minimum Specifications

National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3) defines digital authentication as the process of establishing confidence in user identities digitally presented to a system.⁷ Systems may use the authenticated identity to determine if that user is authorized to perform an electronic transaction.

This document establishes minimum specifications for digital authentication conformant with NIST SP 800-63-3. However, the minimum specifications defined in this document have been developed to accommodate requirements for digital authentication established under other national and international standards.⁸ The minimum specifications in this document also assume that specific business, legal, and technical requirements for a digital identity system will be documented in the identity trust framework for that system. Minimum specifications for other components of a digital identity system have been documented in separate guidance documents in the IMSAC series, pursuant to § 2.2-436 and § 2.2-437.

Digital Identity Model

Digital authentication is the process of establishing confidence in individual identities presented to a digital identity system. Digital identity systems can use the authenticated identity to determine if that individual is authorized to perform an online transaction. The minimum specifications in this document assume that the authentication and transaction take place across an open network, such as the internet.

The digital authentication model defined in these minimum specifications reflects current technologies and architectures used primarily by governmental entities. More complex models that separate functions among a broader range of parties are also available and may have advantages in some classes of applications. While a simpler model has been defined in these minimum specifications, it does not preclude members in digital identity systems from separating these functions.

In addition, certain enrollment, identity proofing, and issuance processes performed by the credential service provider (CSP) may be delegated to an entity known as the registration authority (RA) or identity manager (IM). A close relationship between the RA/IM and CSP is typical, and the nature of this relationship may differ among RAs, IMs, and CSPs. The minimum

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

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 State Chief Information Officers (NASCIO): <http://www.nascio.org/Portals/0/Publications/Documents/SICAM.pdf>; and the Identity Ecosystem Framework (IDEF), published by the Identity Ecosystem Steering Group (IDESG): <https://www.idesg.org/The-ID-Ecosystem/Identity-Ecosystem-Framework/IDEF-Core-Documents>.

specifications defined in this document assume that relationships between members and their requirements are established in the identity trust framework for the digital identity system.

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

The process used to verify an applicant's association with their real world identity is called identity proofing. The strength of identity proofing is described by a categorization called the identity assurance level (IAL, see *IMSAC Reference Document: NIST Assurance Model*). Minimum specifications for identity proofing and verification during the enrollment process have been established in *IMSAC Guidance Document 1.A: Identity Proofing and Verification*.

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

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

Authentication establishes confidence in the claimant's identity, and in some cases in the claimant's attributes. Authentication does not determine the claimant's authorizations or access privileges; this is a separate decision. RPs will use a subscriber's authenticated identity and attributes with other factors to make access control or authorization decisions. Nothing in this document precludes RPs from requesting additional information from a subscriber that has successfully authenticated.

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

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

Authentication Components and Process Flows

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

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

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

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

The verifier is a functional role, but is frequently implemented in combination with the CSP and/or the RP. If the verifier is a separate entity from the CSP, it is often desirable to ensure that the verifier does not learn the subscriber's authenticator secret in the process of authentication, or at least to ensure that the verifier does not have unrestricted access to secrets stored by the CSP.

The usual sequence of interactions in the enrollment, credential issuance, lifecycle management, and an identity proofing and verification process are as follows:

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

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

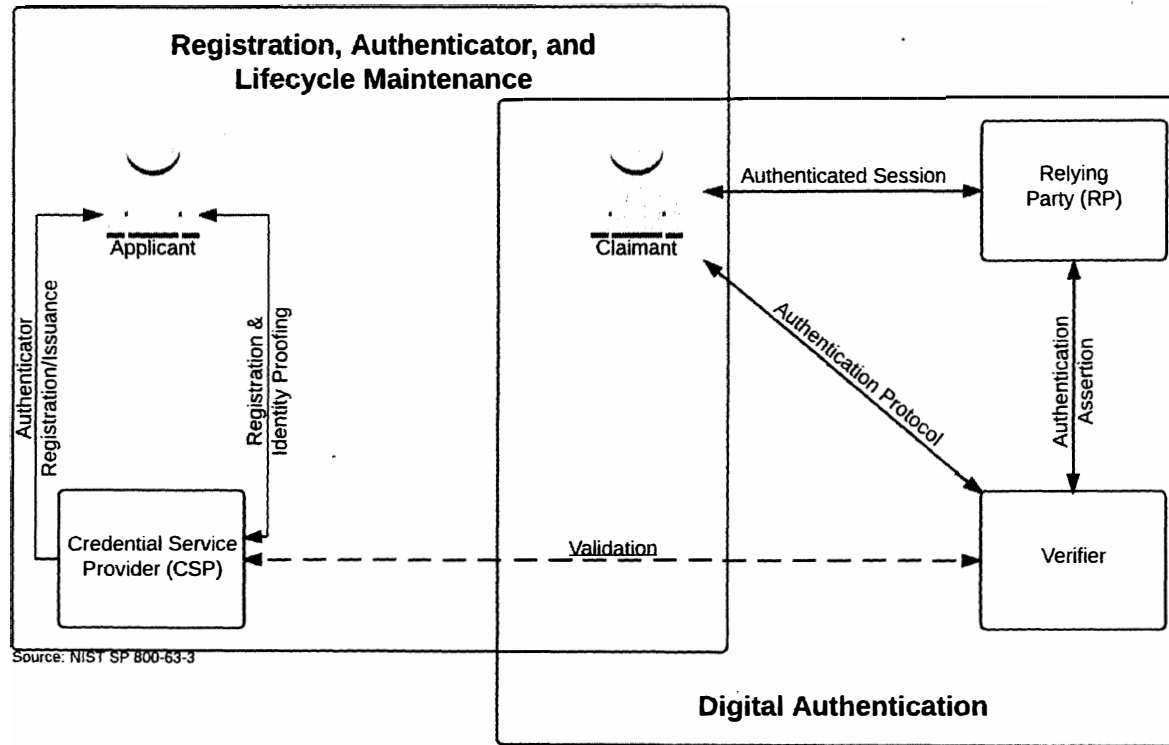
1. The claimant proves to the verifier that he or she possesses and controls the authenticator through an authentication protocol.
2. The verifier interacts with the CSP to validate the credential that binds the claimant's identity to his or her authenticator and to optionally obtain claimant attributes.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

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

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

As noted above, CSPs maintain status information about issued credentials. CSPs may assign a finite lifetime to a credential in order to limit the maintenance period. When the status changes, or when the credentials near expiration, credentials may be renewed or re-issued; or, the credential may be revoked or destroyed. Typically, the subscriber authenticates to the CSP using his or her existing, unexpired authenticator and credential in order to request issuance of a new authenticator and credential. If the subscriber fails to request authenticator and credential re-issuance prior to their expiration or revocation, he or she may be required to repeat the enrollment process to obtain a new authenticator and credential. Alternatively, the CSP may choose to accept a request during a grace period after expiration.

Figure 1. Digital Identity Model



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

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

Authentication Protocols and Lifecycle Management

Authenticators

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

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

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

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

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

Shared secrets stored on authenticators may be either symmetric keys or memorized secrets (e.g., passwords and PINs), as opposed to the asymmetric keys described above, which subscribers need not share with the verifier. While both keys and passwords can be used in similar protocols, one important difference between the two is how they relate to the subscriber. While symmetric keys are generally stored in hardware or software that the subscriber controls, passwords are intended to be memorized by the subscriber. Since most users choose short passwords to facilitate memorization and ease of entry, passwords typically have fewer characters than cryptographic keys. Furthermore, whereas systems choose keys at random, users attempting to choose memorable passwords will often select from a very small subset of the possible passwords of a given length, and many will choose very similar values. As such, whereas cryptographic keys are typically long enough to make network-based guessing attacks untenable, user-chosen passwords may be vulnerable, especially if no defenses are in place.

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

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

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

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

Credentials

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

Assertions

Upon completion of the digital authentication process, the verifier generates an assertion containing the result of the authentication and provides it to the RP. If the verifier is

implemented in combination with the RP, the assertion is implicit. If the verifier is a separate entity from the RP, as in typical federated identity models, the assertion is used to communicate the result of the authentication process, and optionally information about the subscriber, from the verifier to the RP. Minimum specifications for assertions have been defined in *IMSAC Guidance Document 1.C: Digital Identity Assertions*.

Assertions may be communicated directly to the RP, or can be forwarded through the subscriber, which has further implications for system design. An RP trusts an assertion based on the source, the time of creation, and the corresponding identity trust framework that governs the policies and process of CSPs and RPs. The verifier is responsible for providing a mechanism by which the integrity of the assertion can be confirmed.

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

Examples of Assertions include:

- SAML Assertions – SAML assertions are specified using a mark-up language intended for describing security assertions. They can be used by a verifier to make a statement to an RP about the identity of a claimant. SAML assertions may be digitally signed.
- Kerberos Tickets – Kerberos tickets allow a ticket granting authority to issue session keys to two authenticated parties using symmetric key based encapsulation schemes.
- OpenID Connect Claims - OpenID Connect are specified using JavaScript Object Notation (JSON) for describing security, and optionally, user claims. JSON user info claims may be digitally signed.

Relying Parties

An RP relies on results of an authentication protocol to establish confidence in the identity or attributes of a subscriber for the purpose of conducting an online transaction. RPs may use a subscriber's authenticated identity (pseudonymous or non-pseudonymous), the IAL, AAL, and other factors to make access control or authorization decisions. The verifier and the RP may be the same entity, or they may be separate entities. If they are separate entities, the RP normally receives an assertion from the verifier.

The RP ensures that the assertion came from a verifier trusted by the RP. The RP also processes any additional information in the assertion, such as personal attributes or expiration times. The RP is the final arbiter concerning whether a specific assertion presented by a verifier meets the RP's established criteria for system access, regardless of IAL and AAL.

Privacy and Security

The minimum specifications established in this document for privacy and security in the use of person information for digital authentication apply the Fair Information Practice Principles (FIPPs).⁹ The FIPPs have been endorsed by the National Strategy for Trusted Identities in Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.¹⁰

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 digital authentication 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 enrollment, 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 enrollment 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.

⁹ The term “person information” refers to protected data for person entities. 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 identity trust framework for the digital identity system.

¹⁰ 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>.

8 Alignment Comparison

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

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

NIST SP 800-63-3

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

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

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

IDESG Identity Ecosystem Framework (IDEF) Functional Model

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

Appendix 1. IMSAC Charter

COMMONWEALTH OF VIRGINIA IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL CHARTER

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

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

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

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

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

1. The Advisory Council consists of seven members, to be appointed by the Governor, with expertise in electronic identity management and information technology. Members include a representative of the Department of Motor Vehicles, a representative of the Virginia Information Technologies Agency, and five representatives of the business community with appropriate experience and expertise. In addition to the seven appointed members, the Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex officio member of the Advisory Council.
2. The Advisory Council designates one of its members as chairman.
3. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure of the Governor, and may be reappointed.
4. Members serve without compensation but may be reimbursed for all reasonable and necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.
5. Staff to the Advisory Council is provided by the Office of the Secretary of Technology.

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

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

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

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

Appendix 2. 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 enrollment; 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 enrollment and credential issuance are executed by separate entities, procedures for ensuring accurate exchange of enrollment 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 enrollment and credentialing operations.

SECURE-13. REVOCATION

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

SECURE-14. SECURITY LOGS

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

SECURE-15. SECURITY AUDITS

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

Appendix 3. Digital Authentication Standards Alignment Comparison Matrix

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

COMMONWEALTH OF VIRGINIA



IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

GUIDANCE DOCUMENT 1.A Identity Proofing and Verification

In accordance with Section 2.2-436 of the *Code of Virginia*, the Secretary of Technology, after consultation with the Secretary of Transportation, approved this Guidance Document regarding identity proofing and verification. This Guidance Document shall be effective as of December 1, 2017 and shall remain in force and effect unless rescinded or amended by further action pursuant to Section 2.2-436 of the *Code of Virginia*.

Table of Contents

1	Publication Version Control	1
2	Reviews	1
3	Purpose and Scope	2
4	Statutory Authority	3
5	Terminology and Definitions	4
6	Background	5
7	Minimum Specifications	6
8	Alignment Comparison	11

1 Publication Version Control

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

Publication Version	Date	Revision Description
1.0	05/02/2016	Initial Draft of Document
1.0	05/02/2016	Document revised by IMSAC at public workshop
1.0	06/23/2016	Document revised by VITA staff based on comments from IMSAC during May 2, 2016, public workshop
1.0	09/12/2016	Document revised by VITA staff based on public comment received pursuant to § 2.2-437.C, <i>Code of Virginia</i>
1.0	09/30/2016	Document revised by VITA staff based on comments from IMSAC during September 12, 2016, public meeting
1.0	05/01/2017	Document revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by the Identity Management Standards Advisory Council (IMSAC)
1.0	06/05/2017	Document recommended by IMSAC for adoption by the Secretary of Technology

2 Reviews

- The initial version of the document was prepared by staff from the Virginia Information Technologies Agency (VITA) at the direction of the Identity Management Standards Advisory Council (IMSAC).
- The document was reviewed by IMSAC during a council workshop, May 2, 2016.
- The document was revised based on public comment received in written and verbal form during the 30-day comment period, pursuant to § 2.2-437.C. IMSAC allowed at least 30 days for the submission of written comments following the posting and publication and held a meeting dedicated to the receipt of oral comment on June 30, more than 15 days after the posting and publication. The following comments were received on July 13, 2016, via the Virginia Regulatory Town Hall, with the response shown in brackets []:
 - For purposes of setting minimum standards for identity proofing and issuance of credentials/tokens/authenticators, continue to use levels of assurance as defined in the latest approved NIST 800-63 document series. This will be especially important to both identity providers and relying parties in the commercial sector. [Noted]

- On pages 21 and 22 under discussions of Level of Assurance 2, 3, and 4, add references to "virtual in-person proofing" as an approved method consistent with draft 800-63A. [The assurance model applied in the IMSAC guidance document series has been amended to be consistent with NIST SP 800-63-3. A definition for "virtual in-person proofing" based on NIST SP 800-63A has been added to this document.]
 - On page 15, add a definition of "virtual in-person proofing" perhaps based on section 5.4.3 of draft 800-63A. [A definition for "virtual in-person proofing" has been added to this document, consistent with NIST SP 800-63A.]
 - On page 12, add a definition of "remote network identity proofing." This could be modeled after language contained in NIST 800-63 series documents. [The term "remote network identity proofing" has not been defined in the NIST SP 800-63 document series. However, the term "remote" has been defined in the NIST SP 800-63 document series and in this document, and the definition covers remote transactions across a network in an identity proofing context.]
- The document was revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by IMSAC.

3 Purpose and Scope

Pursuant to §§ 2.2-436 and 2.2-437, this guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to establish minimum specifications for digital identity systems so as to warrant liability protection pursuant to the Electronic Identity Management Act ("the Act"), §§ 59.1-550 to -555. This guidance document was prepared to provide information or guidance of general applicability to the public for interpreting or implementing the Act. This guidance document was not developed as a Commonwealth of Virginia Information Technology Resource Management (ITRM) Policy, Standard, and Guideline, pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive branch agencies of the Commonwealth of Virginia.

The minimum specifications in this guidance document conform with the digital identity guidelines found in the March 31, 2017, Public Review version of the National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3). IMSAC will continue to monitor modifications to NIST SP 800-63-3 and may recommend to the Secretary of Technology revisions to the minimum specifications in order to maintain consistency with the NIST guidance.

4 Statutory Authority

The following section documents the statutory authority established in the Code of Virginia for the development of minimum specifications and standards for identity proofing and verification within a digital identity system. References to statutes below and throughout this document shall be to the Code of Virginia, unless otherwise specified.

Governing Statutes:

Secretary of Technology

§ 2.2-225. Position established; agencies for which responsible; additional powers

<http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225/>

Identity Management Standards Advisory Council

§ 2.2-437. Identity Management Standards Advisory Council

<http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/>

Commonwealth Identity Management Standards

§ 2.2-436. Approval of electronic identity standards

<http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/>

Electronic Identity Management Act

Chapter 50. Electronic Identity Management Act

<http://law.lis.virginia.gov/vacode/title59.1/chapter50/>

5 Terminology and Definitions

The core terms used within the digital identity management domain may be assigned a wide range of definitions, depending on the context or community of interest. For the purpose of the IMSAC guidance document series, the terminology has been defined in the IMSAC Reference Document: Terminology and Definitions, which may be accessed at <http://vita.virginia.gov/default.aspx?id=6442475952>

The IMSAC terminology aligns with the definitions published in the following documents:

- National Institute of Standards and Technology Special Publication 800-63-3 March 31, 2017 Public Review version, available at <https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3>
- Electronic Identity Management Act (§ 59.1-550), available at <http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550>
- International Telecommunication Union, Recommendation X. 1255, available at <http://www.itu.int/ITU-T/recommendations/rec.aspx?id=11951&lang=en>

6 Background

In 2015, the Virginia General Assembly passed the Electronic Identity Management Act (§§ 59.1-550 to -555) to address demand in the state's digital economy for secure, privacy enhancing digital authentication and identity management. Growing numbers of communities of interest have advocated for stronger, scalable and interoperable identity solutions to increase consumer protection and reduce liability for principal actors in the identity ecosystem – identity providers, credential service providers and relying parties.

To address the demand contemplated by the Electronic Identity Management Act, the General Assembly created the Identity Management Standards Advisory Council (IMSAC) to advise the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to §2.2-436. A copy of the IMSAC Charter has been provided in **Appendix 1**.

IMSAC 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 to -555); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

Purpose Statement

This guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to provide information or guidance of general applicability to the public for interpreting or implementing the Electronic Identity Management Act. Specifically, this guidance document establishes minimum specifications for identity proofing and verification to enable registration and authentication events within a digital identity system. The minimum specifications conform with NIST SP 800-63-3.

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

This guidance document focuses on identity proofing and verification. Separate IMSAC guidance documents in this series define minimum specifications for other components of a digital identity system.

7 Minimum Specifications

National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3) defines digital authentication as the process of establishing confidence in user identities digitally presented to a system.¹ Systems may use the authenticated identity to determine if that user is authorized to perform an electronic transaction.

Digital authentication begins with enrollment. The enrollment process involves an applicant applying to a CSP. If approved, the CSP creates a credential and binds it to one or more authenticators. The credential includes at least one identifier, which can be pseudonymous, and may include one or more attributes that the CSP has verified. The authenticators may be issued by the CSP, generated/provided directly by the subscriber, or provided by a third party. The authenticator and credential may be used in subsequent authentication events.

The process used to verify an applicant's association with their real world identity is called identity proofing. The strength of identity proofing is described by a categorization called the Identity Assurance Level (IAL, see *IMSAC Reference Document: NIST Assurance Model*).

This document establishes minimum specifications for the identity proofing and verification components of enrollment events in a digital identity system. Identity trust frameworks for digital identity systems should document the business, legal, and technical requirements for these components, as well as requirements for the remaining components of the system. Minimum specifications for identity trust frameworks have been defined in *IMSAC Guidance Document 2: Identity Trust Frameworks*.

Identity Proofing Requirements

Identity proofing and verification for enrollment should be designed to meet the specific requirements for the assurance model defined by the governing identity trust framework for the digital identity system. A trusted enrollment process ensures that (i) the RA and CSP have established the true identity of the applicant, (ii) the enrollment protocols satisfy the requirements for each assurance level, (iii) the RA and CSP maintain a record of the identity evidence and transaction flows to meet audit and compliance requirements, and (iv) the RA and CSP implement enforcement mechanisms to ensure compliance with all applicable provisions established in the identity trust framework.

¹ The Public Review version of National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3) may be accessed at <https://pages.nist.gov/800-63-3/sp800-63-3.html>. At the time of the publication of this document, NIST SP 800-63-3 was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3.

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

- A person with the applicant's claimed attributes exists, and those attributes are sufficient to uniquely identify a single person;
- The applicant whose authenticator is issued is in fact the person who is entitled to the identity;
- It is difficult for the claimant to later repudiate the enrollment and dispute an authentication using the subscriber's authenticator;
- Validate that all supplied evidence is correct and genuine (e.g., not counterfeit or misappropriated).

Enrollment, and the associated identity proofing and verification processes, may be completed through remote or in-person (physical or virtual) protocols. Provisions for remote versus in-person identity proofing and verification should be established in the identity trust framework for the digital identity system and satisfy requirements of the applicable assurance model.

Components and Process Flow

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

- The applicant's attestation of a claimed identity
- The applicant's presentation of evidence to prove the existence of the claimed identity
- The RA's review and validation of the applicant's claimed identity and supporting evidence
- The CSP's verification of the applicant's claimed identity
- The CSP's issuance or enrollment of a credential bound to the applicant's authenticator

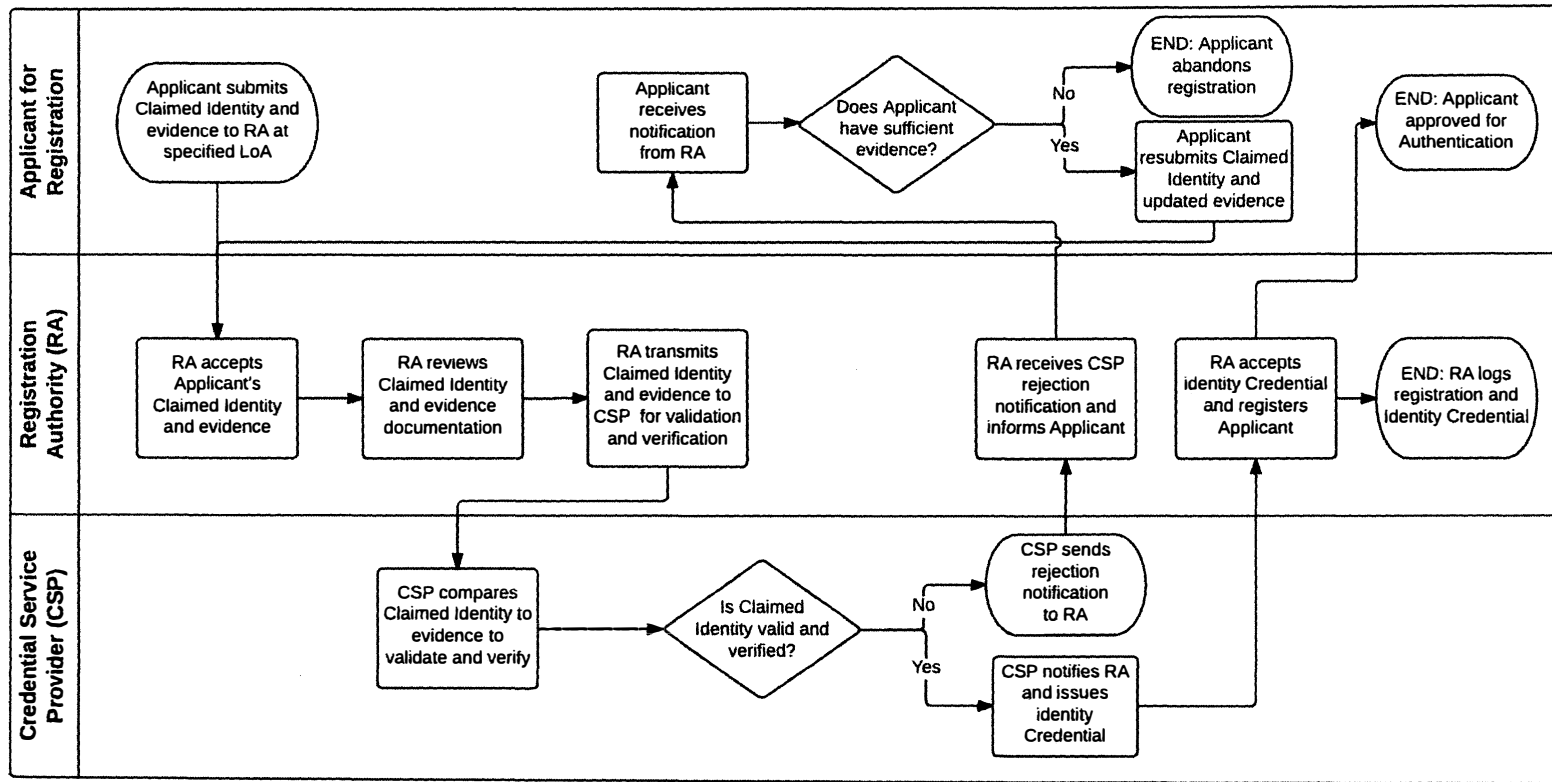
The process flow for implementing the components of the identity proofing and verification for enrollment generally consists of the following (**Figure 1**):

1. The applicant attests to the trusted RA a claimed identity at a specified assurance level
2. The applicant provides the RA either remotely or in person, depending on the assurance model requirements of the identity trust framework, evidence to prove the existence of the claimed identity (identity proofing) Note: Source of original identity document(s) must meet the assurance model and related compliance requirements set by the RA and defined in the identity trust framework
3. The RA transmits the identity proofing evidence to the CSP to verify whether the evidence may be considered valid (identity Validation)
4. The CSP compares the applicant's claimed identity to information associated with the claimed identity to determine whether it relates to the applicant (attribute verification)²

² The attribute verification process may consist of multiple steps and factors, including attribute information, knowledge-based tests, biometrics, activity history, counter-fraud checks, etc., depending on the assurance model requirements established in the identity trust framework. Specific attribute verification requirements should be defined in the governing identity trust framework for the digital identity system. Minimum specifications for attribute verification will be addressed in a forthcoming guidance document in the IMSAC series, pursuant to §2.2-436 and §2.2-437.

5. Upon successful completion of the attribute verification process, the CSP issues to the RA a credential bound to an authenticator for the applicant, confirming the applicant's claimed identity at the appropriate assurance level defined in the identity trust framework for the digital identity system
6. RA maintains a record of the evidence and transaction for the enrollment process.

Figure 1. Identity Proofing and Verification Process Flow



Privacy and Security

The minimum specifications established in this document for privacy and security in the use of person information for identity proofing and verification apply the Fair Information Practice Principles (FIPPs).³ The FIPPs have been endorsed by the National Strategy for Trusted Identities in Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.⁴

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 enrollment, 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 enrollment 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.

³ The term “person information” refers to protected data for person entities. 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 identity trust framework for the digital identity system.

⁴ 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>.

8 Alignment Comparison

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

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

NIST SP 800-63-3

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

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

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

IDESG Identity Ecosystem Framework (IDEF) Functional Model

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

Appendix 1. IMSAC Charter

COMMONWEALTH OF VIRGINIA IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL CHARTER

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

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

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

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

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

1. The Advisory Council consists of seven members, to be appointed by the Governor, with expertise in electronic identity management and information technology. Members include a representative of the Department of Motor Vehicles, a representative of the Virginia Information Technologies Agency, and five representatives of the business community with appropriate experience and expertise. In addition to the seven appointed members, the Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex officio member of the Advisory Council.
2. The Advisory Council designates one of its members as chairman.
3. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure of the Governor, and may be reappointed.
4. Members serve without compensation but may be reimbursed for all reasonable and necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.
5. Staff to the Advisory Council is provided by the Office of the Secretary of Technology.

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

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

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

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

Appendix 2. 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 enrollment; 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 enrollment and credential issuance are executed by separate entities, procedures for ensuring accurate exchange of enrollment 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 enrollment and credentialing operations.

SECURE-13. REVOCATION

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

SECURE-14. SECURITY LOGS

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

SECURE-15. SECURITY AUDITS

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

Appendix 3. Identity Proofing Standards Alignment Comparison Matrix

Component	NIST 800-63-3	SICAM	IDESG IDEF Functional Model
Applicant Claimed Identity	Alignment: Defines protocols and process flows for applicant assertion of claimed identity to federal agencies	Alignment: Defines protocols and process flows for applicant assertion of claimed identity to state agencies	Alignment: Identifies core operations within standard enrollment process flows for applicant claimed identity
	Misalignment: Federal protocols for applicant's claimed identity apply to federal agencies but may not be appropriate across sectors or private industry	Misalignment: Minor variations in terminology with Commonwealth's minimum specifications	Misalignment: Core operational definitions do not contain specific criteria for the process of applicant assertion of claimed identity
Applicant Identity Evidence	Alignment: Establishes rigorous requirements for what federal agencies may accept as identity evidence	Alignment: Establishes rigorous requirements for what state agencies may accept as identity evidence	Alignment: Defines core operations for attribute control and identity evidence, and for maintenance of records
	Misalignment: Federal requirements for acceptable identity evidence may not be appropriate across sectors or private industry	Misalignment: SICAM model provisions for acceptable identity evidence may not be appropriate across sectors or private industry	Misalignment: Core operational definitions do not contain specific criteria for acceptable identity evidence or maintenance of records
RA Validation of Applicant Claimed Identity	Alignment: Sets protocols and required flows for federal agencies to follow in RA Validation of claimed identity	Alignment: Sets protocols and required flows for state agencies to follow in RA Validation of claimed identity	Alignment: Documents core operations for Validation of claimed identity
	Misalignment: Federal protocols for RA Validation of claimed identity may not be appropriate across sectors or private industry	Misalignment: SICAM model for RA Validation of claimed identity may not be appropriate across sectors or private industry	Misalignment: Core operational definitions do not contain specific criteria for RA Validation of claimed identity
CSP Verification of Applicant Claimed Identity	Alignment: Provides clearly defined technical requirements for federal agencies to follow in CSP verification of claimed identity	Alignment: Provides clearly defined technical requirements for state agencies to follow in CSP verification of claimed identity	Alignment: Defines core operations for CSP verification of applicant claimed identity
	Misalignment: Federal verification protocols and requirements may not be appropriate across sectors or private industry	Misalignment: SICAM model for CSP verification of claimed identity may not be appropriate across sectors or private industry	Misalignment: Core operational definitions do not contain specific criteria or technical requirements for CSP verification
CSP Issuance/Registration of Applicant Credential	Alignment: Establishes protocols and technical requirements for issuance/ enrollment of identity credentials	Alignment: Establishes protocols and technical requirements for issuance/ enrollment of identity credentials	Alignment: Identifies core operational roles and responsibilities for Issuance/ enrollment of identity credentials
	Misalignment: Federal credential issuance/ enrollment protocols may not be appropriate across sectors or private industry	Misalignment: State government credential issuance/enrollment protocols may not be appropriate across sectors or private industry	Misalignment: Core operational roles and responsibilities do not contain specific criteria for audit and compliance purposes

COMMONWEALTH OF VIRGINIA



IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

GUIDANCE DOCUMENT 1.B Authenticators and Lifecycle Management

In accordance with Section 2.2-436 of the *Code of Virginia*, the Secretary of Technology, after consultation with the Secretary of Transportation, approved this Guidance Document regarding authenticators and lifecycle management. This Guidance Document shall be effective as of December 1, 2017 and shall remain in force and effect unless rescinded or amended by further action pursuant to Section 2.2-436 of the *Code of Virginia*.

Table of Contents

1	Publication Version Control	1
2	Reviews	1
3	Purpose and Scope	2
4	Statutory Authority	3
5	Terminology and Definitions	4
6	Background	5
7	Minimum Specifications	6

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
1.0	09/12/2016	Document revised by VITA staff based on public comment received pursuant to § 2.2-437.C, <i>Code of Virginia</i>
1.0	09/30/2016	Document revised by VITA staff based on comments from IMSAC during September 12, 2016, public meeting
1.0	12/05/2016	Document revised based on direction from VITA’s Legal and Legislative Services Directorate and the Office of the Attorney General following September 12, 2016, public meeting
1.0	05/01/2017	Document revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by the Identity Management Standards Advisory Council (IMSAC)
1.0	06/05/2017	Document recommended by IMSAC for adoption by the Secretary of Technology

2 Reviews

- The initial version of the document was prepared by staff from the Virginia Information Technologies Agency (VITA) at the direction of the Identity Management Standards Advisory Council (IMSAC).
- The document was revised based on public comment received in written and verbal form during the 30-day comment period, pursuant to § 2.2-437.C.
- The document was revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by IMSAC.

3 Purpose and Scope

Pursuant to §§ 2.2-436 and 2.2-437, this guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to establish minimum specifications for digital identity systems so as to warrant liability protection pursuant to the Electronic Identity Management Act ("the Act"), §§ 59.1-550 to -555. This guidance document was prepared to provide information or guidance of general applicability to the public for interpreting or implementing the Act. This guidance document was not developed as a Commonwealth of Virginia Information Technology Resource Management (ITRM) Policy, Standard, and Guideline, pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive branch agencies of the Commonwealth of Virginia.

The minimum specifications in this guidance document conform with the digital identity guidelines found in the March 31, 2017, Public Review version of the National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3). IMSAC will continue to monitor modifications to NIST SP 800-63-3 and may recommend to the Secretary of Technology revisions to the minimum specifications in order to maintain consistency with the NIST guidance.

4 Statutory Authority

The following section documents the statutory authority established in the Code of Virginia for the development of minimum specifications and standards for authenticators and lifecycle management within a digital identity system. References to statutes below and throughout this document shall be to the Code of Virginia, unless otherwise specified.

Governing Statutes:

Secretary of Technology

§ 2.2-225. Position established; agencies for which responsible; additional powers

<http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225/>

Identity Management Standards Advisory Council

§ 2.2-437. Identity Management Standards Advisory Council

<http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/>

Commonwealth Identity Management Standards

§ 2.2-436. Approval of electronic identity standards

<http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/>

Electronic Identity Management Act

Chapter 50. Electronic Identity Management Act

<http://law.lis.virginia.gov/vacode/title59.1/chapter50/>

5 Terminology and Definitions

The core terms used within the digital identity management domain may be assigned a wide range of definitions, depending on the context or community of interest. For the purpose of the IMSAC guidance document series, the terminology has been defined in the *IMSAC Reference Document: Terminology and Definitions*, which may be accessed at <http://vita.virginia.gov/default.aspx?id=6442475952>

The IMSAC terminology aligns with the definitions published in the following documents:

- National Institute of Standards and Technology Special Publication 800-63-3
March 31, 2017 Public Review version, available at
<https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3>
- Electronic Identity Management Act (§ 59.1-550), available at
<http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550>
- International Telecommunication Union, Recommendation X. 1255, available at
<http://www.itu.int/ITU-T/recommendations/rec.aspx?id=11951&lang=en>

6 Background

In 2015, the Virginia General Assembly passed the Electronic Identity Management Act (§§ 59.1-550 to -555) to address demand in the state’s digital economy for secure, privacy enhancing digital authentication and identity management. Growing numbers of communities of interest have advocated for stronger, scalable and interoperable identity solutions to increase consumer protection and reduce liability for principal actors in the identity ecosystem – identity providers, credential service providers and relying parties.

To address the demand contemplated by the Electronic Identity Management Act, the General Assembly created the Identity Management Standards Advisory Council (IMSAC) to advise the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to § 2.2-436. A copy of the IMSAC Charter has been provided in **Appendix 1**.

IMSAC 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 to -555); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

Purpose Statement

This guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to provide information or guidance of general applicability to the public for interpreting or implementing the Electronic Identity Management Act. Specifically, the document establishes minimum specifications for authenticators and lifecycle management within a digital identity system. The minimum specifications conform with NIST SP 800-63B.

The document defines minimum requirements, assurance levels, 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 identity trust framework for each distinct digital identity system, and that these requirements will be designed based on the Identity Assurance Level (IAL) and Authenticator Assurance Level (AAL) requirements for the system.

This guidance document focuses on authenticators and lifecycle management. Separate IMSAC guidance documents in this series define minimum specifications for other components of a digital identity system.

7 Minimum Specifications

National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3) defines digital authentication as the process of establishing confidence in user identities digitally presented to system. Systems may use the authenticated identity to determine if that user is authorized to perform an electronic transaction.

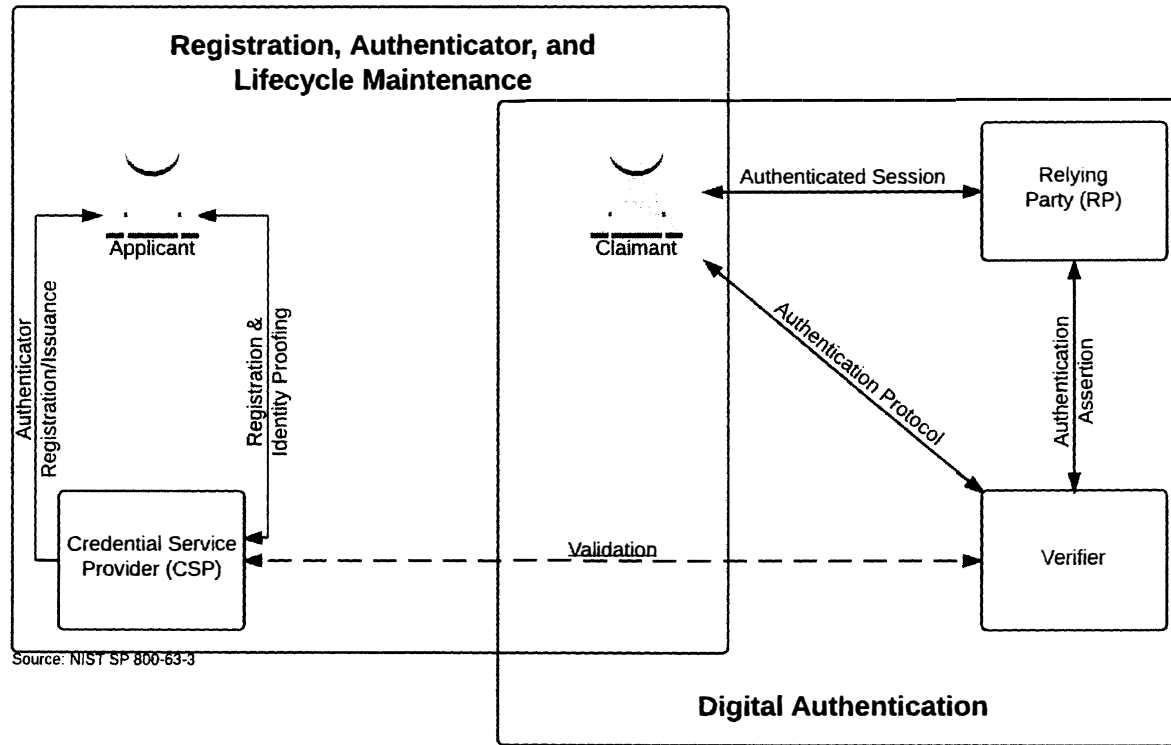
This document establishes minimum specifications for authenticators and lifecycle management conformant with NIST SP 800-63B. However, the minimum specifications defined in this document have been developed to accommodate requirements for authenticators established under other national and international standards.⁷ The minimum specifications in this document also assume that specific business, legal, and technical requirements for a digital identity system will be documented in the identity trust framework for that system. Minimum specifications for other components of a digital identity system have been documented in separate guidance documents in the IMSAC series, pursuant to §2.2-436 and §2.2-437.

Digital Identity Model

Digital authentication is the process of establishing confidence in individual identities presented to a digital identity system. The minimum specifications in this document assume that the authentication and transaction take place across an open network, such as the internet. The digital identity model used for these minimum specifications has been shown in Figure 1. Minimum specifications for the full digital identity model reflected in this document have been defined in *IMSAC Guidance Document 1: Digital Authentication*.

⁷ The minimum specifications defined in this document align with the State Identity Credential and Access Management (SICAM) Guidance and Roadmap, published by the National Association of State Chief Information Officers (NASCIO): <http://www.nascio.org/Portals/0/Publications/Documents/SICAM.pdf>; and the Identity Ecosystem Framework (IDEF), published by the Identity Ecosystem Steering Group (IDESG): <https://www.idesg.org/The-ID-Ecosystem/Identity-Ecosystem-Framework/IDEF-Core-Documents>.

Figure 1. Digital Identity Model



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

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

Authenticator Assurance Levels

The Authenticator Assurance Levels (AALs) described in this document have their foundation in the assurance model outlined in the *IMSAC Reference Document: NIST Assurance Model*. In order to satisfy the requirements of a given AAL, claimants must authenticate themselves with at least a given level of strength to be recognized as subscribers. 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). Optionally, other attributes that identify the subscriber as a unique subject may be provided. A summary of AAL requirements has been provided in **Figure 2**.

Authenticator Assurance Level 1

AAL1 provides some assurance that the claimant controls an authenticator registered to the subscriber. AAL1 requires single-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.

Permitted Authenticator Types – AAL 1

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

- Memorized Secret
- Look-up Secret
- Out-of-Band (Partially deprecated)
- Single-Factor OTP Device
- Multi-Factor OTP Device
- Single-Factor Cryptographic Software
- Single-Factor Cryptographic Device
- Multi-Factor Software Cryptographic Authenticator
- Multi-Factor Cryptographic Device

Authenticator and Verifier Requirements – AAL 1

Cryptographic authenticators used at AAL1 must use approved cryptography. Software-based authenticators that operate within the context of a general purpose operating system may, where practical, attempt to detect compromise of the platform in which they are running (e.g., by malware) and must decline to operate when such a compromise is detected. Communication between the claimant and channel (the primary channel in the case of an out-of-band authenticator) must be via an authenticated protected channel to provide confidentiality of the authenticator output and resistance to MitM attacks. Verifiers operated by government agencies at AAL1 must be validated to meet the requirements of [FIPS 140] Level 1.

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 applicable laws and regulations. If the CSP opts to retain records in the absence of any legal requirements, the CSP must conduct a privacy risk assessment to determine how long records should be retained.

Authenticator Assurance Level 2

AAL2 provides high confidence that the claimant controls authenticator(s) registered to the subscriber. Proof of possession and control of two different authentication factors is required through a secure authentication protocol. Approved cryptographic techniques are required at AAL2 and above.

Permitted Authenticator Types – AAL 2

At AAL 2, it is required to have a multi-factor authenticator, or a combination of two single-factor authenticator.

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

- Multi-Factor OTP Device
- Multi-Factor Software Cryptographic authenticator
- Multi-Factor Cryptographic Device

When a combination of two single-factor authenticator 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
- Single-Factor Cryptographic Software

Note: When biometric authentication implements the requirements in NIST SP 800-63B the device has to be authenticated. Therefore, it is unnecessary to implement another factor with biometrics as the device is “something you have”, which serves as a valid second factor of the authenticator.

Authenticator and Verifier Requirements – AAL 2

Cryptographic authenticators used at AAL2 must use approved cryptography. Authenticators procured by government agencies must be validated to meet the requirements of [FIPS 140] Level 1. Software-based authenticators that operate within the context of a general purpose

operating system may, where practical, attempt to detect compromise of the platform in which they are running (e.g., by malware) and should decline to operate when such a compromise is detected. At least one authenticator used at AAL2 must be replay resistant.

Authentication at AAL2 should demonstrate authentication intent from at least one authenticator. Communication between the claimant and verifier (the primary channel in the case of an out-of-band authenticator) must be via an authenticated protected channel to provide confidentiality of the authenticator output and resistance to MitM attacks.

Verifiers operated by government agencies at AAL2 must be validated to meet the requirements of [FIPS 140] Level 1. When a biometric factor is used in authentication at AAL2, the verifier should make a determination that the biometric sensor and subsequent processing meet the performance requirements stated in NIST SP 800-63B.

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 regulations apply to those entities. If the CSP opts to retain records in the absence of any legal requirements, the CSP must conduct a privacy risk assessment to determine how long records should be retained.

Authenticator Assurance Level 3

AAL3 provides very high confidence that the claimant controls authenticator(s) registered to the subscriber. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but also requires a “hard” cryptographic authenticator that provides verifier impersonation resistance.

Permitted Authenticator Types – AAL 3

Authentication Assurance Level 3 requires the use of one of two kinds of hardware devices:

- Multi-factor Cryptographic Device
- Single-factor Cryptographic Device used in conjunction with Memorized Secret

Authenticator and Verifier Requirements – AAL 3

Communication between the claimant and channel must be via an authenticated protected channel to provide confidentiality of the authenticator output and resistance to MitM attacks. All cryptographic device authenticators used at AAL3 must be verifier impersonation resistant and replay resistant. All authentication and reauthentication processes at AAL3 must demonstrate authentication intent from at least one authenticator as described in NIST SP 800-63-3. Multi-factor authenticators used at AAL3 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 AAL3 must be validated at [FIPS 140] Level 1 or higher overall with at least [FIPS 140] Level 3 physical security. Verifiers at AAL3 must be validated at [FIPS 140] Level 1 or higher. When a biometric factor is used in authentication at AAL3, the verifier must make a determination that the biometric sensor and subsequent processing meet the performance requirements stated in NIST SP 800-63B.

Reauthentication – AAL 3

At AAL3, 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. Reauthentication must use both authentication factors. The verifier may 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 [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 must comply with their respective records retention policies in accordance with whatever laws and regulations apply to those entities. If the CSP opts to retain records in the absence of any legal requirements, the CSP must conduct a privacy risk assessment to determine how long records should be retained.

Figure 2. Summary of AAL Requirements

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 authenticator and verifiers)	Level 2 overall (MF authenticator) 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

Authenticator and Verifier Requirements

The minimum specifications defined in this document establish the following requirements for each authenticator type. With the exception of reauthentication requirements and the requirement for verifier impersonation resistance at AAL3, the technical requirements for each authenticator type are the same regardless of the AAL at which the authenticator is used.

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 should permit user-chosen memorized secrets to be up to 64 characters or more in length. All printing ASCII [RFC 20] characters as well as the space character should be acceptable in memorized secrets; Unicode [ISO/ISC 10646:2014] characters should be accepted as well. Verifiers may remove multiple consecutive space characters, or all space characters, prior to verification provided that the result is at least 8 characters in length. 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.

If Unicode characters are accepted in memorized secrets, the verifier should apply the Normalization Process for Stabilized Strings defined in Section 12.1 of Unicode Standard Annex 15 [UAX 15] using either the NFKC or NFKD normalization. Subscribers choosing memorized secrets containing Unicode characters should be advised that some characters may be represented differently by some endpoints, which can affect their ability to authenticate successfully. This process is applied prior to hashing of the byte string representing the memorized secret.

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 bit 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 must compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised. For example, the list may include (but is not limited to):

- Passwords obtained from previous breach corpuses
- Dictionary words
- Repetitive or sequential characters (e.g. ‘aaaaa’, ‘1234abcd’)
- Context specific words, such as the name of the service, the username, and derivatives thereof

If the chosen secret is found in the list, the CSP or verifier must advise the subscriber that they need to select a different secret, provide the reason for rejection, and require the subscriber to choose a different value. 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 must not impose other composition rules (e.g., mixtures of different character types) on memorized secrets. Verifiers must not require memorized secrets to be changed arbitrarily (e.g., periodically) and should only require a change if the subscriber requests a change or there is evidence of compromise of the authenticator.

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) until it is entered. This allows the claimant to verify their entry if they are in a location where their screen is unlikely to be observed. The verifier may also permit the user’s device to display individual entered characters for a short time after each character is typed to verify correct entry, particularly on mobile devices. The verifier must use approved encryption and must utilize an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM 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 [SP 800-132]. The salt value must be a 32-bit or longer random value generated by an approved random bit generator and 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 [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

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. A common application of look-up secrets is the use of "recovery keys" stored by the subscriber for use in the event another authenticator is lost or malfunctions.

Look-up Secret Authenticators

CSPs creating look-up secret authenticator must use an approved random bit 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. 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 authenticator (e.g., in a hardware security module) should be used to further resist dictionary attacks against the stored hashed authenticator.

Look-up secrets must be generated using an approved random bit generator and must have at least 20 bits of entropy. When look-up secrets have less than 64 bits of entropy, 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 must use approved encryption and utilize an authenticated protected channel when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.

Out-of-Band

An out-of-band authenticator is a physical device that is uniquely addressable and can communicate securely with the verifier over a distinct communications channel, referred to as the secondary channel. The device is possessed and controlled by the claimant and supports private communication over this secondary channel that is separate from the primary channel for e-authentication. The out-of-band authenticator can operate in one of the following ways:

- The claimant transfers a secret received by the out-of-band device via the secondary channel to the verifier using the primary channel. For example, the claimant may receive the secret on their mobile device and type it (typically a 6-digit code) into their authentication session.

- The claimant transfers a secret received via the primary channel to the out-of-band device for transmission to the verifier via the secondary channel. For example, the claimant may view the secret on their authentication session and either type it into an app on their mobile device or use a technology such as a barcode or QR code to effect the transfer.
- The claimant compares secrets received from the primary channel and the secondary channel and confirms the authentication via the secondary channel.

The purpose of the secret is to securely bind the authentication operation on the primary and secondary channel. When the response is via the primary communication channel, the secret also establishes the claimant's control of the out-of-band device.

Out-of-Band Authenticators

The out-of-band authenticator must establish a separate channel with the verifier 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 without the authorization of the claimant.

The out-of-band device should be uniquely addressable and communication over the secondary channel shall be private. Methods that do not prove possession of a specific device, such as voice-over-IP (VOIP) or email, must not be used for out-of-band authentication.

The out-of-band authenticator must uniquely authenticate itself in one of the following ways in communicating with the verifier:

- Establish an authenticated protected channel to the verifier using approved cryptography. The key used must be stored in the most secure storage available on the device (e.g., keychain storage, trusted platform module, trusted execution environment).
- Authenticate to a public mobile telephone network using a SIM card or equivalent that uniquely identifies the device. This method must only be used if a secret is being sent from the verifier to the out-of-band device via the telephone network (SMS or voice).

If a secret is sent by the verifier to the out-of-band device, the device must not display the authentication secret on a device while it is locked by the owner (i.e., requires an entry of a PIN, passcode, or biometric). However, authenticators should 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), it must do one of the following:

- The authenticator must accept transfer of the secret from the primary channel which it must send to the verifier over the secondary channel to associate the approval with the

authentication transaction. The claimant may perform the transfer manually or use a technology such as a barcode or QR code to effect the transfer.

- The authenticator must present a secret received via the secondary channel from the verifier and prompt the claimant to verify the consistency of that secret with the primary channel, prior to accepting a yes/no response from the claimant. It must then send that response to the verifier.

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, such as on a smart phone, the verifier may send a push notification to that device. The verifier then waits for the 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 use of 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, one of the following must take place:

- Transfer of secret to primary channel - The verifier may signal the device containing the subscriber's authenticator to indicate readiness to authenticate. It must then transmit a random secret to the out-of-band authenticator. The verifier must then wait for the secret to be returned on the primary communication channel.
- Transfer of secret to secondary channel - The verifier must display a random authentication secret to the claimant via the primary channel. It must then wait for the secret to be returned on the secondary channel from the claimant's out-of-band authenticator.
- Verification of secrets by claimant - The verifier must display a random authentication secret to the claimant via the primary channel, and must send the same secret to the out-of-band authenticator via the secondary channel for presentation to the claimant. It must then wait for an approval (or disapproval) message via the secondary channel.

In all cases, the authentication must be considered invalid if not completed within 5 minutes. In order to provide replay resistance, verifiers must accept a given authentication secret only once during the validity period.

The verifier must generate random authentication secrets with at least 20 bits of entropy using an approved random bit generator. 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.

Single-Factor OTP Device

A single-factor OTP device generates OTPs. This includes hardware devices as well as 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 OTPs and does not require activation through a second factor. The OTP is displayed on the device and manually input to the verifier, thereby proving possession and control of the device. An OTP device may, for example, display 6 characters at a time. A single-factor OTP device is something you have.

Single-factor OTP devices are similar to look-up secret authenticators with the exception that the secrets are cryptographically and independently 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 and its algorithm must provide at least the minimum security strength specified in the latest revision of [SP 800-131A] (112 bits as of the date of this publication). 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.

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.

When a multi-factor OTP authenticator is being associated with a subscriber account, the verifier (or associated CSP) must obtain secrets required to duplicate the authenticator output from the authenticator source (typically its manufacturer) using approved cryptography.

The verifier must use approved encryption and an authenticated protected channel when collecting the OTP in order to provide resistance to eavesdropping and MitM attacks. Time-based OTPs must have a lifetime of less than 2 minutes. In order to provide replay resistance as described in Section 5.2.7, verifiers must accept a given time-based OTP only once during the validity period.

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 NIST SP 800-63B.

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 NIST requirements, 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.

When a multi-factor OTP authenticator is being associated with a subscriber account, the verifier (or associated CSP) must obtain secrets required to duplicate the authenticator output from the authenticator source (typically its manufacturer) using approved cryptography. The verifier or CSP must also establish, via the authenticator source, that the authenticator is a multi-factor device. In the absence of a trusted statement that it is a multi-factor device, the verifier must treat it the authenticator as single-factor.

The verifier must use approved encryption and utilize an authenticated protected channel when collecting the OTP in order to provide resistance to eavesdropping and MitM attacks. Time-based OTPs must have a lifetime of less than 2 minutes. In order to provide replay resistance, verifiers must accept a given time-based OTP only once during the validity period.

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. A biometric activation factor must meet the requirements in NIST SP 800-63B, including limits on the number of consecutive authentication failures.

Single-Factor Cryptographic Software

A single-factor software cryptographic authenticator is a cryptographic key stored on disk or some other "soft" media. 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 single-factor software cryptographic authenticator is something you have.

Single-factor Cryptographic Software Authenticators

Single-factor software cryptographic authenticators encapsulate a secret key that is unique to the authenticator. The key must be stored in the most secure storage available on the device (e.g., keychain storage, trusted platform module, or trusted execution environment if available). The key must be strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.

Single-factor Cryptographic Software Verifiers

The requirements for a single-factor cryptographic software verifier are identical to those for a single-factor cryptographic device verifier.

Single-Factor Cryptographic Devices

A single-factor cryptographic device is a hardware device that performs cryptographic operations using protected cryptographic key(s) and provides the authenticator output via direct connection to the user endpoint. The device uses embedded symmetric or asymmetric cryptographic keys, and does not require activation through a second factor of authentication. Authentication is accomplished by proving possession of the device via the authentication protocol. The authenticator output is provided by direct connection to the user endpoint and is highly dependent on the specific cryptographic device and protocol, but it is typically some type of signed message. A single-factor cryptographic device is something you have.

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 (i.e., it cannot be removed from the device). The authenticator operates by signing a challenge nonce presented through a direct computer interface such as a USB port. Although cryptographic devices contain software, they differ from cryptographic software authenticators by the fact that all embedded software is under control of the CSP (or other issuer), and that the entire authenticator is subject to any applicable FIPS 140 requirements at the AAL being authenticated.

The secret key and its algorithm must provide at least the minimum security length specified in the latest revision of [SP 800-131A] (112 bits as of the date of this publication). The challenge nonce must be at least 64 bits in length. Approved cryptography must be used.

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, trusted execution environment). Each authentication operation using the authenticator must require the input of both factors.

Any memorized secret used by the authenticator for activation must be at least 6 decimal digits in length or of equivalent complexity and must be rate limited. A biometric activation factor must meet the requirements of NIST SP 800-63B, and must include limits on the allowable number of consecutive 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 erased from memory 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.

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. The authenticator operates by signing a challenge nonce presented through a direct computer interface such as a USB port.

Although cryptographic devices contain software, they differ from cryptographic software authenticators by the fact that all embedded software is under control of the CSP (or manufacturer), and that the entire authenticator is subject to any applicable FIPS 140 requirements at the AAL being authenticated.

The secret key and its algorithm must provide at least the minimum security length specified in the latest revision of [SP 800-131A] (112 bits as of the date of this publication). The challenge nonce must be at least 64 bits in length. Approved cryptography must be used.

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, smartcard).

Any memorized secret used by the authenticator for activation must be at least 6 decimal digits in length or of equivalent complexity and must be rate limited. A biometric activation factor must meet the requirements NIST SP 800-63B, and must include limits on the number of consecutive 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 overwritten in memory 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 required in the authenticator type descriptions cited above, 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 no more than 100 consecutive failed attempts on a single account.

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 CAPTCHA before attempting authentication.
- Requiring the claimant to wait following a failed attempt for a period of time that is increasing in intervals from, say, 30 seconds to an hour, as the account approaches its maximum allowance for consecutive failed attempts.
- 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.

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). 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 have).
- An authenticated protected channel between sensor (or endpoint containing a sensor that resists sensor replacement) and verifier must be established and the sensor or endpoint authenticated prior to capturing the biometric sample from the claimant.
- Empirical testing of the biometric system to be deployed must demonstrate an EER of 1 in 1000 or better with respect to matching performance. The biometric system must operate with an FMR of 1 in 1000 or better.
- The biometric system should implement PAD. Testing of the biometric system to be deployed should 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.

Note: PAD is being considered as a mandatory requirement in future editions of this guideline.

The biometric system must allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD meeting the above requirements is implemented. Once that limit has been reached, the biometric authenticator must either:

- Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt, e.g., 1 minute before the following failed attempt, 2 minutes before the second following attempt, etc.

OR

- Disable the biometric user verification and offer another factor (a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already implemented.

Determination of sensor/endpoint performance, integrity, and authenticity can be accomplished in several different ways, any of which are acceptable under this guideline. These include but are not limited to: authentication of the sensor or endpoint, certification by an approved accreditation authority, or runtime interrogation of signed metadata (e.g., attestation).

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 limited to one or more specific devices that are identified using approved cryptography.
- Biometric revocation, referred to as biometric template protection in ISO/IEC 24745, must be implemented.
- 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 erased from memory immediately after any training or research data has been derived.

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 SP 800-63A.

Attestation

Attestation is information conveyed to the verifier regarding a directly connected authenticator or the endpoint involved in an authentication operation. Information conveyed by attestation MAY include, but is not limited to:

- The provenance (manufacturer or supplier certification), health, and integrity of the authenticator and/or endpoint.
- Security features of the authenticator.
- Security and performance characteristics of biometric sensor(s).
- Sensor modality.

If this attestation is signed, it must be signed using a digital signature that provides at least the minimum security strength specified in the latest revision of [SP 800-131A] (112 bits as of the date of this publication). Attestation information may be used as part of a risk-based authentication decision.

Verifier Impersonation Resistance

Verifier impersonation attacks, sometimes referred to as “phishing attacks”, refer to attempts by fraudulent verifiers and RPs to fool an unwary claimant into authenticating to an impostor website. In previous editions of SP 800-63, protocols that are resistant to verifier impersonation attacks were also referred to as “strongly MitM resistant”.

Authentication protocols that are verifier impersonation resistant must authenticate the verifier and either:

1. Strongly and irreversibly bind the authenticator output to the public key of the certificate presented by the verifier to which it is sent, or to that verifier’s authenticated hostname or domain name; or
2. Determine whether the verifier’s authenticated hostname or domain name is on a list of trusted verifiers, and release the authenticator output only to a verifier on that list.

One example of the former class of verifier impersonation resistant authentication protocols is client-authenticated TLS, because the client signs the authenticator output along with earlier messages from the protocol that are unique to the particular TLS connection being negotiated. Other protocols that may be used are techniques that irreversibly include the verifier’s hostname or domain in the generation of the authenticator output, making that authenticator

output unusable by a fraudulent verifier (the attacker) if proxied to the intended verifier. The latter class of verifier impersonation resistant protocols relies on access control to release the authenticator output only to trusted verifiers.

In contrast, authenticators that involve the manual entry of an authenticator output, such as out of band and OTP authenticators, must not be considered verifier impersonation resistant because they assume the vigilance of the claimant to determine that they are communicating with the intended verifier.

Verifier-CSP Communications

In situations where the verifier and CSP are separate entities, communications between the verifier and CSP must occur through a mutually-authenticated secure channel (such as a client-authenticated TLS connection) using approved cryptography.

Verifier Compromise Resistance

Use of some types of authenticators requires that the verifier store a copy of the authenticator secret. For example, an OTP authenticator requires that the verifier independently generate the authenticator output for comparison against the value sent by the claimant. Because of the potential for the verifier to be compromised and stored secrets stolen, authentication protocols that do not require the verifier to persistently store secrets that could be used for authentication are considered stronger, and are described herein as being verifier compromise resistant. Note that such verifiers are not resistant to all attacks; a verifier could be compromised in a different way, such as to always accept a particular authenticator output.

Verifier compromise resistance can be achieved in different ways, for example:

1. Use a cryptographic authenticator that requires that the verifier store a public key corresponding to a private key held by the authenticator.
2. Store the expected authenticator output in hashed form. This method can be used with some look-up secret authenticators, for example.

In order to be considered verifier compromise resistant, public keys stored by the verifier must use approved cryptography and must provide at least the minimum security strength specified in the latest revision of [SP 800-131A] (112 bits as of the date of this publication).

Other verifier compromise resistant secrets must use approved hash algorithms and the underlying secrets must have at least the minimum security strength specified in the latest revision of [SP 800-131A] (112 bits as of the date of this publication). Note that secrets (such as memorized secrets) having lower complexity must not be considered verifier compromise resistant when hashed because of the potential to defeat the hashing process through dictionary lookup or exhaustive search.

Replay Resistance

An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Replay resistance is in addition to the replay resistant nature of authenticated protected channel protocols, since the output could be stolen prior to entry into the protected channel. Protocols that use nonces or challenges to prove the “freshness” of the transaction are resistant to replay attacks since the verifier will easily detect that the old protocol messages replayed do not contain the appropriate nonces or timeliness data related to the current authentication session.

Examples of replay resistant authenticators are OTP devices, cryptographic authenticators, and look-up secrets. In contrast, memorized secrets are not considered replay resistant because the authenticator output (the secret itself) is provided for each authentication.

Authentication Intent

An authentication process requires intent if it requires the subject to explicitly respond to each authentication or reauthentication request. The goal of authentication intent is to make it more difficult for directly connected physical authenticators (cryptographic devices) to be used without the subject’s knowledge, such as by malware on the endpoint. Authentication intent must be established by the authenticator itself, although multi-factor cryptographic devices may establish intent by reentry of the other authentication factor on the endpoint with which the authenticator is used.

Authentication intent may be established in a number of ways. Authentication processes that require intervention of the subject, e.g., to enter an authenticator output on their endpoint from an OTP device, establish intent by their very nature. Cryptographic devices that require user action (e.g., pushing a button or reinsertion) for each authentication or reauthentication operation are also considered to establish intent.

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 issued 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.

Enrollment

The following requirements apply when an authenticator is bound to an identity as a result of a successful identity proofing transaction, as described in the *IMSAC Guidance Document 1.A: Identity Proofing and Verification*.

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 and thus a CSP should bind at least two authenticators to the subscriber's credential at IAL1 as well.

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 *IMSAC Guidance Document 1.A: Identity Proofing and Verification*. 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.

Enrollment 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 must 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 chooses 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 *IMSAC Guidance Document 1.A: Identity Proofing and Verification*, **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

CSPs may issue authenticators that expire. If and when an authenticator expires, it must not be usable for authentication. When an authentication is attempted using an expired authenticator, 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 or prove destruction of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator.

Revocation and Termination

Revocation of an authenticator (sometimes referred to as termination, especially in the context of PIV credentials) refers to removal of the binding between an authenticator and a credential the CSP maintains. CSPs must revoke the binding of authenticators promptly when an online identity ceases to exist (e.g., subscriber's death, discovery of a fraudulent subscriber), when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements.

The CSP must require subscribers to surrender or prove destruction of any physical authenticator containing certified attributes signed by the CSP as soon as practical after revocation or termination takes place.

Privacy and Security

The minimum specifications established in this document for privacy and security in the use of person information for digital authentication apply the Fair Information Practice Principles (FIPPs).⁸ The FIPPs have been endorsed by the National Strategy for Trusted Identities in Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.⁹

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 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.

⁸ The term “person information” refers to protected data for person entities. 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 identity trust framework for the digital identity system.

⁹ 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.

COMMONWEALTH OF VIRGINIA



IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

GUIDANCE DOCUMENT 1.C Digital Identity Assertions

In accordance with Section 2.2-436 of the *Code of Virginia*, the Secretary of Technology, after consultation with the Secretary of Transportation, approved this Guidance Document regarding digital identity assertions. This Guidance Document shall be effective as of December 1, 2017 and shall remain in force and effect unless rescinded or amended by further action pursuant to Section 2.2-436 of the *Code of Virginia*.

Table of Contents

1	Publication Version Control	1
2	Reviews	1
3	Purpose and Scope	1
4	Statutory Authority	2
5	Terminology and Definitions	3
6	Background	4
7	Minimum Specifications	5

1 Publication Version Control

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

Publication Version	Date	Revision Description
1.0	10/12/2016	Initial Draft of Document
1.0	05/01/2017	Document revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by the Identity Management Standards Advisory Council (IMSAC)
1.0	06/05/2017	Document recommended by IMSAC for adoption by the Secretary of Technology

2 Reviews

- The initial version of the document was prepared by staff from the Virginia Information Technologies Agency (VITA) at the direction of the Identity Management Standards Advisory Council (IMSAC).
- The document was revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by IMSAC.

3 Purpose and Scope

Pursuant to §§ 2.2-436 and 2.2-437, this guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to establish minimum specifications for digital identity systems so as to warrant liability protection pursuant to the Electronic Identity Management Act ("the Act"), §§ 59.1-550 to -555. This guidance document was prepared to provide information or guidance of general applicability to the public for interpreting or implementing the Act. This guidance document was not developed as a Commonwealth of Virginia Information Technology Resource Management (ITRM) Policy, Standard, and Guideline, pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive branch agencies of the Commonwealth of Virginia.

The minimum specifications in this guidance document conform with the digital identity guidelines found in the March 31, 2017, Public Review version of the National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3). IMSAC will continue to monitor modifications to NIST SP 800-63-3 and may recommend to the Secretary of Technology revisions to the minimum specifications in order to maintain consistency with the NIST guidance.

4 Statutory Authority

The following section documents the statutory authority established in the Code of Virginia for the development of minimum specifications and standards for identity assertions within a digital identity system. References to statutes below and throughout this document shall be to the Code of Virginia, unless otherwise specified.

Governing Statutes:

Secretary of Technology

§ 2.2-225. Position established; agencies for which responsible; additional powers

<http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225/>

Identity Management Standards Advisory Council

§ 2.2-437. Identity Management Standards Advisory Council

<http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/>

Commonwealth Identity Management Standards

§ 2.2-436. Approval of electronic identity standards

<http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/>

Electronic Identity Management Act

Chapter 50. Electronic Identity Management Act

<http://law.lis.virginia.gov/vacode/title59.1/chapter50/>

5 Terminology and Definitions

The core terms used within the digital identity management domain may be assigned a wide range of definitions, depending on the context or community of interest. For the purpose of the IMSAC guidance document series, the terminology has been defined in the IMSAC Reference Document: Terminology and Definitions, which may be accessed at <http://vita.virginia.gov/default.aspx?id=6442475952>

The IMSAC terminology aligns with the definitions published in the following documents:

- National Institute of Standards and Technology Special Publication 800-63-3 March 31, 2017 Public Review version, available at <https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3>
- Electronic Identity Management Act (§ 59.1-550), available at <http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550>
- International Telecommunication Union, Recommendation X. 1255, available at <http://www.itu.int/ITU-T/recommendations/rec.aspx?id=11951&lang=en>

6 Background

In 2015, the Virginia General Assembly passed the Electronic Identity Management Act (§§ 59.1-550 to -555) to address demand in the state's digital economy for secure, privacy enhancing digital authentication and identity management. Growing numbers of communities of interest have advocated for stronger, scalable and interoperable identity solutions to increase consumer protection and reduce liability for principal actors in the identity ecosystem – identity providers, credential service providers and relying parties.

To address the demand contemplated by the Electronic Identity Management Act, the General Assembly created the Identity Management Standards Advisory Council (IMSAC) to advise the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to §2.2-436. A copy of the IMSAC Charter has been provided in **Appendix 1**.

IMSAC 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 to -555); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

Purpose Statement

This guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to provide information or guidance of general applicability to the public for interpreting or implementing the Electronic Identity Management Act. Specifically, this guidance document establishes minimum specifications for assertions in a digital identity system. The minimum specifications conform with NIST SP 800-63C.

This guidance document defines assertion types, core components, presentation methods, security, and privacy provisions for assertions. The document assumes that specific business, legal, and technical requirements for assertions will be established in the identity trust framework for each distinct digital identity system, and that these requirements will be designed based on the digital authentication model, Identity Assurance Level (IAL), and Authenticator Assurance Level (AAL) requirements for the system.

This guidance document focuses on digital identity assertions. Separate IMSAC guidance documents in this series define minimum specifications for other components of a digital identity system.

7 Minimum Specifications

National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3) defines an assertion in a digital identity system as a statement from a verifier to a relying party (RP) that contains identity information about a subscriber. Assertions may also contain verified attributes.⁶ Systems may use the authenticated identity to determine if that user is authorized to perform an electronic transaction.

This document establishes minimum specifications for assertions within a digital identity system. The minimum specifications assume that specific business, legal, and technical requirements for a digital identity system will be documented in the identity trust framework for that system. Minimum specifications for other components of a digital identity system have been documented in separate guidance documents in the IMSAC series, pursuant to § 2.2-436 and § 2.2-437.

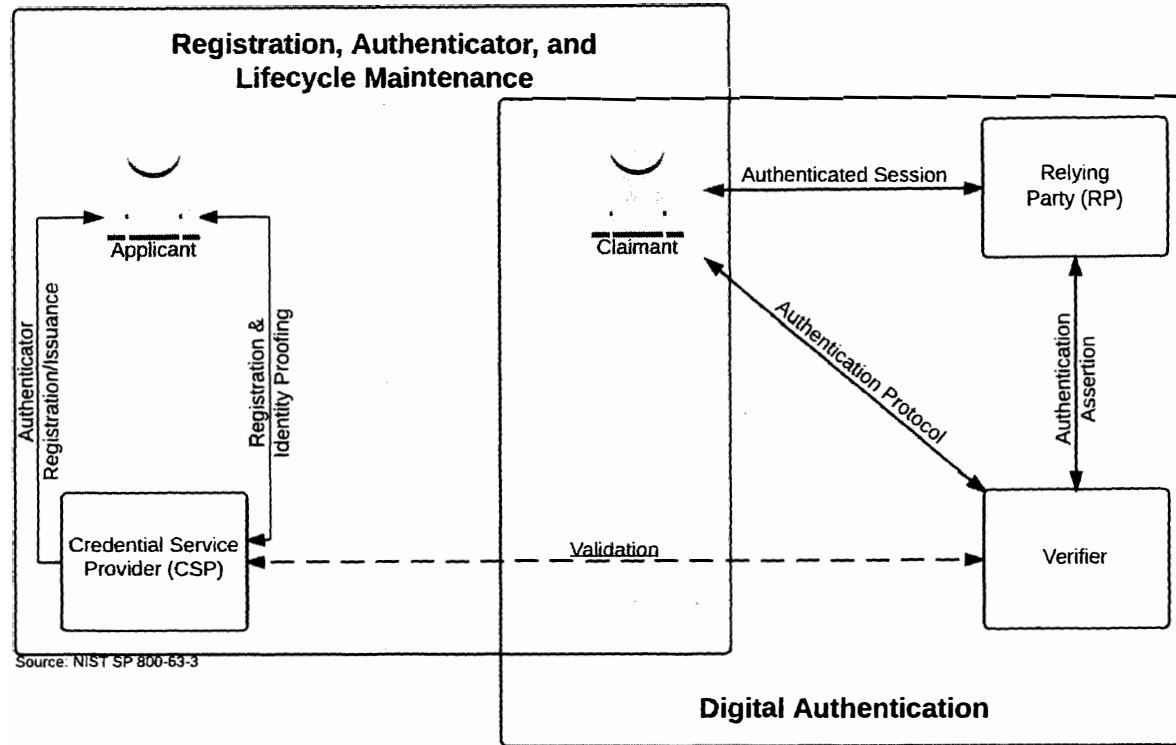
Digital Identity Model

Assertions play an integral role in digital authentication, the process of establishing confidence in individual identities presented to a digital identity system. Digital identity systems implement assertions as part of the process to authenticate a person's identity. In turn, the authenticated identity may be used to determine if that person is authorized to perform an online transaction. The minimum specifications in this document assume that the authentication and transaction take place across an open network, such as the internet.

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

⁶ The Public Review version of National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3) may be accessed at <https://pages.nist.gov/800-63-3/sp800-63-3.html>. At the time of the publication of this document, NIST SP 800-63-3 was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3.

Figure 1. Digital Identity Model



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

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

Assertions

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

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

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

These core claims, particularly the issuance and expiration claims, apply to the assertion about the authentication event itself, and not to any additional identity attributes associated with the subscriber, even when those claims are included within the assertion. A subscriber's attributes may expire or be invalidated independently of the expiration or invalidation of the assertion.

Assertions may include other additional identity attributes. Privacy requirements for presenting attributes in assertions have been provided below in this document. The RP may fetch additional identity attributes from the IdP in a separate transaction using an authorization credential issued alongside the assertion.

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

Assertion Binding

An assertion can be classified based on whether presentation by a claimant of an assertion reference or the assertion itself is sufficient for establishing the binding between the subscriber and the assertion, or if a stronger binding is required.

Holder-of-Key Assertions

A holder-of-key assertion contains a reference to a symmetric key or a public key (corresponding to a private key) possessed by and representing the subscriber. An RP may decide when to require the subscriber to prove possession of the key, depending on the policy of the RP. However, the RP must require the subscriber to prove possession of the key that is referenced in the assertion in parallel with presentation of the assertion itself in order for the assertion to be considered holder-of-key. Otherwise, an assertion containing reference to a key which the user has not proved possession of will be considered a bearer assertion.

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

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

Bearer Assertions

A bearer assertion can be presented by any party as proof of the bearer's identity. If an attacker is able to capture or manufacture a valid assertion representing a subscriber, and that attacker is able to successfully present that assertion to the RP, then the attacker will be able to impersonate the subscriber at that RP.

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

Assertion Protection

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

Assertion Identifier

Assertions must be sufficiently unique to permit unique identification by the target RP. Assertions may accomplish this by use of an embedded nonce, timestamp, assertion identifier, or a combination of these or other techniques.

Signed Assertion

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

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

Encrypted Assertion

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

Audience Restriction

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

Pairwise Pseudonymous Identifiers

In some circumstances, it is desirable to prevent the subscriber's account at the IdP from being linked through one or more RPs through use of a common identifier. In these circumstances, pairwise pseudonymous identifiers must be used within the assertions generated by the IdP for the RP, and the IdP must generate a different identifier for each RP.

When unique pseudonymous identifiers are used with RPs alongside attributes, it may still be possible for multiple colluding RPs to fully identify and correlate a subscriber across digital identity systems using these attributes. For example, given that two independent RPs will each see the same subscriber identified with a different pairwise pseudonymous identifier, the RPs could still determine that the subscriber is the same person by comparing their name, email address, physical address, or other identifying attributes carried alongside the pairwise pseudonymous identifier. Privacy policies may prohibit such correlation, but pairwise pseudonymous identifiers can increase effectiveness of these policies by increasing the administrative effort in managing the attribute correlation.

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

Pairwise Pseudonymous Identifier Generation

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

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

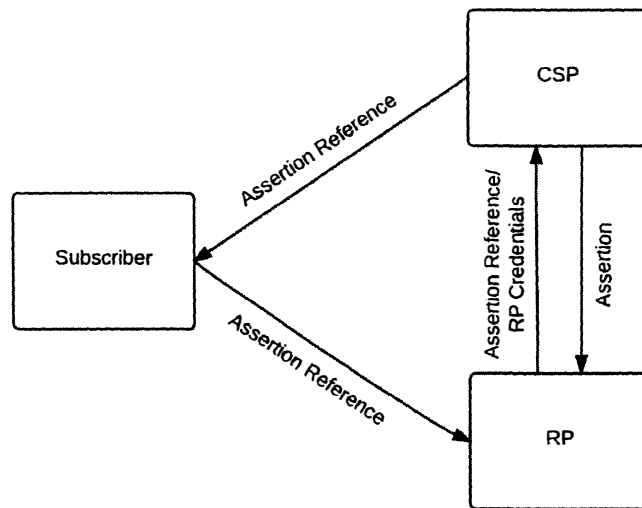
The RPs must conduct a privacy risk assessment to consider the privacy risks associated with requesting a common identifier. The IdP must ensure that only intended RPs are correlated; otherwise, a rogue RP could learn of the Pseudonymous Identifier for a correlation by fraudulently posing as part of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

Assertion Presentation

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

Back-Channel Presentation

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

Figure 2. Back-Channel Assertion Presentation

Source: NIST SP 800-63C

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

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

The Assertion Reference:

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

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

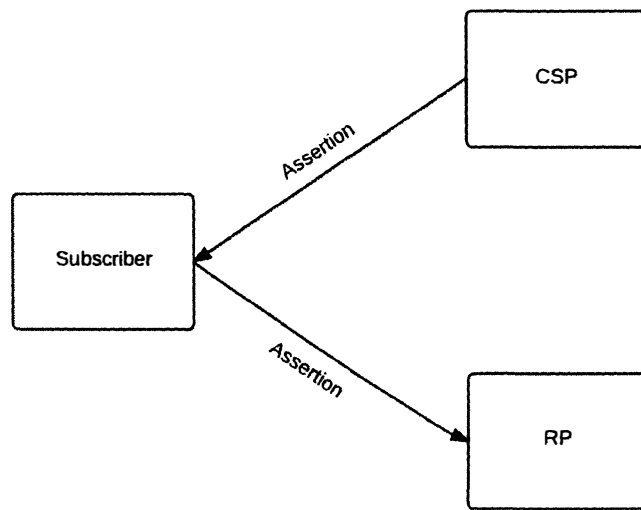
Conveyance of the assertion reference from the IdP to the subscriber as well as from the subscriber to the RP must be made over an authenticated protected channel. Conveyance of

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

Front-Channel Presentation

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

Figure 3: Front-Channel Assertion Presentation



Source: NIST SP 800-63C

In the front-channel model, an assertion is visible to the subscriber, which could potentially cause leakage of system information included in the assertion. In this model, it is more difficult for the RP to query the IdP for additional attributes. Since the assertion is under the control of the subscriber, the front-channel presentation method allows the subscriber to submit a single assertion to unintended parties, perhaps by a browser replaying an assertion at multiple RPs. Even if the assertion is audience restricted and rejected by RPs, its presentation at unintended RPs could lead to leaking information about the subscriber and their online activities.

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

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

Conveyance of the assertion from the IdP to the subscriber as well as from the subscriber to the RP must be made over an authenticated protected channel.

Security

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

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

Common attacks against assertion transmission transactions include the following:

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

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

In other cases, the IdP will generate a temporary secret and transmit it to the authenticated subscriber for this purpose. When this secret is used to authenticate to the RP, this temporary

secret will be referred to as a secondary authenticator. Secondary authenticators include assertions in the direct model, session keys in Kerberos, assertion references in the indirect model, and cookies used for authentication.

Threats to the secondary authenticator include the following:

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

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

Threat Mitigation Strategies

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

- **Assertion Manufacture/Modification:** To mitigate this threat, the following mechanisms are used:
 - The assertion is digitally signed by the IdP. The RP checks the digital signature to verify that it was issued by a legitimate IdP.
 - The assertion is sent over a protected session such as TLS. In order to protect the integrity of assertions from malicious attack, the IdP is authenticated.
 - The assertion contains a non-guessable random identifier.
- **Assertion Disclosure:** To mitigate this threat, one of the following mechanisms are used:
 - The assertion is sent over a protected session to an authenticated RP. Note that, in order to protect assertions against both disclosure and manufacture/modification using a protected session, both the RP and the IdP need to be validated.
 - Assertions are signed by the IdP and encrypted for a specific RP. It should be noted that this provides all the same guarantees as a mutually authenticated protected session, and may therefore be considered equivalent. The general requirement for protecting against both assertion disclosure and assertion manufacture/modification may therefore be described as a mutually authenticated protected session or equivalent between the IdP and the RP.

- **Assertion Repudiation by the IdP:** To mitigate this threat, the assertion is digitally signed by the IdP using a key that supports non-repudiation. The RP checks the digital signature to verify that it was issued by a legitimate IdP.
- **Assertion Repudiation by the subscriber:** To mitigate this threat, the IdP issues holder-of-key assertions, rather than bearer assertions. The subscriber can then prove possession of the asserted key to the RP. If the asserted key matches the subscriber's presented key, it will be proof to all parties involved that it was the subscriber who authenticated to the RP rather than a compromised IdP impersonating the subscriber.
- **Assertion Redirect:** To mitigate this threat, the assertion includes the identity of the RP for which it was generated. The RP verifies that incoming assertions include its identity as the recipient of the assertion.
- **Assertion Reuse:** To mitigate this threat, the following mechanisms are used:
 - The assertion includes a timestamp and has a short lifetime of validity. The RP checks the timestamp and lifetime values to ensure the assertion is currently valid.
 - The RP keeps track of assertions that were consumed within a (configurable) time window to ensure that an assertion is not used more than once within that time window.
- **Secondary Authenticator Manufacture:** To mitigate this threat, one of the following mechanisms is used:
 - The secondary authenticator may contain sufficient entropy that an attacker without direct access to the IdP's random number generator cannot guess the value of a valid secondary authenticator.
 - The secondary authenticator may contain timely assertion data that is signed by the IdP or integrity protected using a key shared between the IdP and the RP.
- **Secondary Authenticator Capture:** To mitigate this threat, adequate protections are in place throughout the lifetime of any secondary authenticators used in the assertion protocol:
 - In order to protect the secondary authenticator while it is in transit between the IdP and the subscriber, the secondary authenticator is sent via a protected session established during the primary authentication of the subscriber.
 - In order to protect the secondary authenticator from capture as it is submitted to the RP, the secondary authenticator is used in an authentication protocol which protects against eavesdropping and man-in-the-middle attacks.
 - In order to protect the secondary authenticator after it has been used, it is never transmitted over an unprotected session or to an unauthenticated party while it is still valid.
- **Assertion Substitution:** To mitigate this threat, one of the following mechanisms is used:
 - Responses to assertion requests contain the value of the assertion reference used in the request or some other nonce that was cryptographically bound to the request by the RP.
 - Responses to assertion requests are bound to the corresponding requests by message order, as in HTTP, provided that assertions and requests are protected by a protocol such as TLS that can detect and disallow malicious reordering of packets.

Assertion Examples

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

Security Assertion Markup Language (SAML)

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

The building blocks of SAML include:

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

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

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

Kerberos Tickets

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

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

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

To authenticate using the session key, the subscriber sends the ticket to the RP along with encrypted data that proves that the subscriber possesses the session key embedded within the Kerberos ticket. Session keys are either used to generate new tickets, or to encrypt and authenticate communications between the subscriber and the RP.

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

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

OpenID Connect

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

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

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

- `iss` : HTTPS URL identifying the IdP that issued the assertion
- `sub` : IdP-specific subject identifier representing the subscriber

- `aud` : IdP-specific audience identifier, equal to the OAuth 2.0 client identifier of the client at the IdP
- `exp` : Timestamp at which the identity token expires and after which must not be accepted the client
- `iat` : Timestamp at which the identity token was issued and before which must not be accepted by the client

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

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

Privacy and Security

The minimum specifications established in this document for privacy and security in the use of person information for digital authentication apply the Fair Information Practice Principles (FIPPs).⁹ The FIPPs have been endorsed by the National Strategy for Trusted Identities in Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.¹⁰

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 assertions 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.

⁹ The term “person information” refers to protected data for person entities. 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 identity trust framework for the digital identity system.

¹⁰ 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.

COMMONWEALTH OF VIRGINIA



IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

GUIDANCE DOCUMENT 2 Identity Trust Frameworks

In accordance with Section 2.2-436 of the *Code of Virginia*, the Secretary of Technology, after consultation with the Secretary of Transportation, approved this Guidance Document regarding identity trust frameworks. This Guidance Document shall be effective as of December 1, 2017 and shall remain in force and effect unless rescinded or amended by further action pursuant to Section 2.2-436 of the *Code of Virginia*.

Table of Contents

1	Publication Version Control	1
2	Reviews	1
3	Purpose and Scope	2
4	Statutory Authority	2
5	Terminology and Definitions	3
6	Background	4
7	Minimum Specifications	5
8	Alignment Comparison	9

1 Publication Version Control

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

Publication Version	Date	Revision Description
1.0	05/02/2016	Initial Draft of Document
1.0	05/02/2016	Document revised by IMSAC at public workshop
1.0	06/23/2016	Document revised by VITA staff based on comments from IMSAC during May 2, 2016, public workshop
1.0	09/12/2016	Document revised by VITA staff based on public comment received pursuant to § 2.2-437.C, <i>Code of Virginia</i>
1.0	09/30/2016	Document revised by VITA staff based on comments from IMSAC during September 12, 2016, public meeting
1.0	05/01/2017	Document revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by the Identity Management Standards Advisory Council (IMSAC)
1.0	06/05/2017	Document recommended by IMSAC for adoption by the Secretary of Technology

2 Reviews

- The initial version of the document was prepared by staff from the Virginia Information Technologies Agency (VITA) at the direction of the Identity Management Standards Advisory Council (IMSAC).
- The document was reviewed by IMSAC during a council workshop, May 2, 2016.
- The document was revised based on public comment received in written and verbal form during the 30-day comment period, pursuant to § 2.2-437.C.
- The document was revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by IMSAC.

3 Purpose and Scope

Pursuant to §§ 2.2-436 and 2.2-437, this guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to establish minimum specifications for digital identity systems so as to warrant liability protection pursuant to the Electronic Identity Management Act ("the Act"), §§ 59.1-550 to -555. This guidance document was prepared to provide information or guidance of general applicability to the public for interpreting or implementing the Act. This guidance document was not developed as a Commonwealth of Virginia Information Technology Resource Management (ITRM) Policy, Standard, and Guideline, pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive branch agencies of the Commonwealth of Virginia.

4 Statutory Authority

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

Governing Statutes:

Secretary of Technology

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

Identity Management Standards Advisory Council

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

Commonwealth Identity Management Standards

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

Electronic Identity Management Act

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

5 Terminology and Definitions

The core terms used within the digital identity management domain may be assigned a wide range of definitions, depending on the context or community of interest. For the purpose of the IMSAC guidance document series, the terminology has been defined in the *IMSAC Reference Document: Terminology and Definitions*, which may be accessed at <http://vita.virginia.gov/default.aspx?id=6442475952>.

The IMSAC terminology aligns with the definitions published in the following documents:

- National Institute of Standards and Technology Special Publication 800-63-3 March 31, 2017 Public Review version, available at <https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3>
- Electronic Identity Management Act (§ 59.1-550), available at <http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550>
- International Telecommunication Union, Recommendation X. 1255, available at <http://www.itu.int/ITU-T/recommendations/rec.aspx?id=11951&lang=en>

6 Background

In 2015, the Virginia General Assembly passed the Electronic Identity Management Act (§§ 59.1-550 to -555) to address demand in the state's digital economy for secure, privacy enhancing digital authentication and identity management. Growing numbers of communities of interest have advocated for stronger, scalable and interoperable identity solutions to increase consumer protection and reduce liability for principal actors in the identity ecosystem – identity providers, credential service providers and relying parties.

To address the demand contemplated by the Electronic Identity Management Act, the General Assembly created the Identity Management Standards Advisory Council (IMSAC) to advise the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to §2.2-436. A copy of the IMSAC Charter has been provided in **Appendix 1**.

IMSAC 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 to -555); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

Purpose Statement

This guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to provide information or guidance of general applicability to the public for interpreting or implementing the Electronic Identity Management Act. Specifically, this guidance document establishes minimum specifications for identity trust frameworks supporting digital identity systems.

The document defines minimum requirements, components, and related provisions for identity trust frameworks. The document assumes a specific identity trust framework will address the business, legal, and technical requirements for each distinct digital identity system; these requirements will be designed based on the specific assurance model supported by the system; and the identity trust framework will be compliant with applicable laws, regulations, and statutes.

The document limits its focus to identity trust frameworks. Separate IMSAC guidance documents in this series define minimum specifications for other components of a digital identity system.

7 Minimum Specifications

The Commonwealth of Virginia's Electronic Identity Management Act defines identity trust framework as a digital identity system with established identity, security, privacy, technology, and enforcement rules and policies adhered to by certified identity providers that are members of the identity trust framework (§ 59.1-550). Identity trust frameworks consist of multiparty agreements among members, which enforce requirements and ensure trust in the acceptance of identity credentials.

This document establishes minimum specifications for identity trust frameworks. Identity trust frameworks should be designed to document the business, legal, and technical components for enterprise architecture, business processes, governance models, operational policies and practices, and member obligations within the system. Identity trust frameworks also should contain the requirements for meeting the assurance model supported by the system. Subsequent guidance documents in the IMSAC series have addressed other components of digital identity systems, pursuant to § 2.2-436 and § 2.2-437.

Trust Framework Components

The following section outlines the minimum specifications for the business, legal and technical components of a standard identity trust framework. These components have been identified through a rigorous assessment of existing identity trust frameworks in the identity ecosystem and other domains, as outlined in Section 8 of this report. The components also align with the Identity Ecosystem Framework (IDEF), adopted by the Identity Ecosystem Steering Group in October 2015.¹

Business Components

- **Limitations on Use of Data:** Collection, maintenance, and use of a person's identity information solely for the purpose for which it was collected.
- **Governance Authority & Change Processes:** Governance model for the identity trust framework built on a transparent, clearly defined structure and change-management process.
- **Operating Policies & Procedures:** Policies and procedures for the operations, maintenance, and business continuity of the identity trust framework's operational authority, and across the digital identity system.
- **Security, Privacy & Confidentiality (Business):** Compliant business processes and documentation for notifying a person of the security, privacy, and confidentiality provisions

¹ Identity Ecosystem Framework (IDEF) Baseline Functional Requirements (v.1.0), Identity Ecosystem Steering Group (IDESG), may be accessed at: https://workspace.idesg.org/kws/public/download/83/IDEF-Baseline-Requirements-v1.0-FINAL-10152015.pdf&wg_abbrev=idesg_document.

in the identity trust framework and for gaining consent from the person for using identity information.

- **Suspension & Termination (Voluntary & Involuntary):** Provisions for suspending or terminating a member due to failure to meet the obligations in the agreement, or the member's self-suspension or termination of participation in the identity trust framework.
- **Data Elements & Data Classification:** Attribute-level documentation, classification, and labeling of the person identity information used within the identity trust framework to support compliant handling of the data through the entire data lifecycle.
- **Expectations of Performance:** Provisions in the identity trust framework that set the performance and service criteria for all members – IdPs, CSPs, and RPs – including requirements for breach response and resolution, system(s) interruption or failure, and other risk situations.
- **Use Cases (Exchange & Member Types):** Documented examples for roles and responsibilities of members of the identity trust framework and data flows across the digital identity system.

Legal Components

- **Definition/Identification of Applicable Law:** Provisions requiring members of the identity trust framework to comply with all governing laws, statutes, rules, and regulations of the jurisdiction in which each member operates.
- **Legal Agreements for Exchange Structure:** Statement of requirements for the architecture, performance, and service specifications, and member obligations for the operation and maintenance of the exchange of person identity information within the identity trust framework.
- **Security, Privacy & Consent Provisions (Legal):** Terms and conditions establishing member obligations for the collection, labeling, operational use, and maintenance of person identity information and for gaining consent from the person for using identity information.
- **Assignment of Liability & Risk for Members:** Articles that define how liability and risk within the identity trust framework will be distributed among members, with indemnification provisions for violation of the agreement.
- **Representations & Warranties:** Statements of factual principles in the identity trust framework upon which members may rely, and assurances of the implied indemnification obligation in the event the principles are violated or proven false.
- **Grant of Authority:** Provisions requiring members of the identity trust framework to assign to the Governance Authority decision-making authority over the identity trust framework.
- **Dispute Resolution:** Statement of requirements and processes for mediation and the resolution of disputes among members in the identity trust framework in a manner that avoids adjudicative procedures.
- **Authorizations for Data Requests by Members:** Articles defining role-based rules, requirements, and processes for members of the identity trust framework to access person identity information.

- **Open Disclosure & Anti-Circumvention:** Provisions requiring transparency in the rules, policies, and practices for operations and governance of the identity trust framework, and prohibiting the circumvention of technical protections within the digital identity system for the handling of person identity information.
- **Confidential Person Information:** Statements documenting the business, legal and technical requirements for the classification, labeling and handling of confidential person identity information.
- **Audit, Accountability & Compliance:** Terms of conditions documenting and requiring members of the identity trust framework to comply with audit procedures, and the consequences of members failing to comply with the audit findings and corrective action plan to address deficiencies.

Technical Components

- **Performance & Service Specifications:** Architecture and infrastructure specifications, protocols, and requirements for all members – IdPs, CSPs, and RPs – covering full end-to-end integration for the digital identity system supported by the identity trust framework, including technical, solutions, and information architecture.
- **Security, Privacy & Confidentiality:** Architecture and infrastructure specifications, protocols, and requirements within the digital identity system supported by the identity trust framework designed for the collection, labeling, operational use, and maintenance of person identity information and for gaining consent from the person for using identity information.
- **Breach Notification:** Processes, protocols, and requirements compliant with applicable law for notifying the appropriate authorities in the event of a breach of person identity information, and related risk situations, within the identity trust framework.
- **System Access:** Standards-based, open architecture processes, protocols, and requirements for member authentication and access to the digital identity system supported by the identity trust framework.
- **Provisions for Future Use of Data:** Terms and conditions defining limitations on, and permitted purposes for, the use of person identity information after the information has been used for the Registration event and the issuance of a credential by a credential service provider.
- **Duty of Response by Members:** Terms and conditions requiring identity trust framework member systems to respond to and process messaging requests – inbound and outbound – within the digital identity system, normally establishing the time in which the member system must respond and process the request.
- **Onboarding, Testing & Certification Requirements:** Documented processes, protocols, specifications, and requirements for onboarding, testing, and certifying prospective member systems in the identity trust framework.
- **Handling of Test Data v. Production Data:** Terms and conditions compliant with applicable law preventing the use of production data in a test environment.

- **Compliance with Governing Standards:** Terms and conditions identifying and stating requirements for member compliance with governing external standards for the identity trust framework, including standards for information processing, Electronic Authentication, and Authorization.

8 Alignment Comparison

The minimum specifications for identity trust frameworks established in this document have been developed based on a detailed comparison analysis of identity trust frameworks and related governance models currently operational in the identity management ecosystem. Specifically, the minimum specifications build upon core components of existing identity trust frameworks while adapting or extending them to meet the requirements of IMSAC, pursuant to §2.2-436-§2.2-437. The analysis covered identity trust frameworks on a global scale, including a detailed review of the Open Identity Exchange (OIX) Trust Framework Model (OIX/OITF) and the European Union (EU) standards.

The following identity trust frameworks were evaluated by IMSAC. Results from the alignment comparison analysis have been compiled into matrix form in **Appendix 2**.

- State Identity, Credential and Access Management (SICAM) Guidance and Roadmap – Strategic framework published by the National Association of State Chief Information Officers (NASCIO) to promote alignment with FICAM within state government.²
- AAMVA DL/ID Security Framework – Set of requirements, recommendations and standards maintained by the American Association of Motor Vehicle Administrators (AAMVA) for use by Motor Vehicle Administrations to ensure driver’s license and identification security.
- eHealth Exchange Data Use & Reciprocal Support Agreement (DURSA) – Trust framework established to support the exchange health information and messaging within eHealth Exchange, the Nationwide Health Information Network.
- InCommon Trust Framework – Trust framework designed to facilitate authentication and identity management for students, faculty, staff and other service providers for institutions of higher education.
- Kantara Initiative Trust Framework – Trust framework developed on a for-profit, subscription basis to enable secure, identity-based, online interactions in a secure environment.
- Open Identity Exchange (OIX)/OITF Model – Set of guidelines and recommended mechanisms (assurance model and level of protection) for developing and implementing an identity trust framework for secure, confidence-based exchange of information (global).

² The Federal Identity, Credential, and Access Management (FICAM) program was created 2008 to address challenges, implementation issues, and design requirements for digital Identity, credential, and access management for federal agencies. For more information, visit:
https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000XNYG

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. Trust Framework Alignment Comparison Matrix

	Trust Framework (TF) Components for IMSAC			
	Business	Legal	Technical	Other
Trust Framework (TF) Comparison Matrix	<ul style="list-style-type: none"> • Limitations on Use of Data (“Permitted Purpose”) • Governance Authority & Change Processes • Operating Policies & Procedures • Security, Privacy & Confidentiality-Business: Consent/Auth.) • Suspension & Termination (Voluntary & Involuntary) • Data Elements & Data Classification (Attribute Level/Person Identity Information) • Expectations of Performance • Use Cases (Exchange & Member Types) 	<ul style="list-style-type: none"> • Definition/Identification of “Applicable Law” • Legal Agreements for Exchange Structure • Security, Privacy & Consent Provisions • Assignment of Liability & Risk for Members • Representations & Warranties • Grant of Authority • Dispute Resolution • Authorizations for Data Requests by Member • Open Disclosure & Anti-Circumvention • Confidential Person Information • Audit, Accountability & Compliance 	<ul style="list-style-type: none"> • Performance & Service Specifications • Security, Privacy & Confidentiality (Technical: Infrastructure/Architecture) • Breach Notification • System Access (ID/Authentication) • Provisions for Future Use of Data • Duty of Response by Members • Onboarding, Testing & Certification Requirements • Handling of Test Data v. Production Data • Compliance Governing Standards 	<ul style="list-style-type: none"> • Openness & Transparency • TF Lifecycle Management (“Living Agreement”) • Support & Capacity Building (IGs) • Scalability to Support Array of Members (Horizontal/Vertical) • Glossary of TF Terms/Definitions • Component-based Approach for TF Elements

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	Legal	Technical	Other
<p>State Identity, Credential and Access Management (SICAM) Guidance and Roadmap</p>	<ul style="list-style-type: none"> + Limitations on Use of Data (§6.6) + Governance Authority & change processes (§6.6) + Operating policies & procedures (§6.6) + Security, privacy & confidentiality (§6.6) + Suspension & termination (§6.6) + Data elements & data classification (attribute level/PII) (§5.5, §6.5, §6.6) + Expectations of performance (§6.6) 	<ul style="list-style-type: none"> + Compliance w/ applicable law (§6.6) + Legal agreements for exchange structure (§6.6) + Security, privacy & consent (§6.6) + Liability (§6.6) + Representations & warranties (§6.6) + Grant of authority (§6.6) + Dispute resolution (§6.6) + Authorizations for data exchange (§6.6) + Non-exclusivity (§6.6) + Confidential Person Information (§6.6, §6.3) + Audit (§6.6) + Accountability & compliance (§6.9) 	<ul style="list-style-type: none"> + Performance & service specifications (§5, §6.4) + Security, privacy & confidentiality (§5, §6.4) + Breach notification (§5, §6.4; §6.6) + System access (§6.6) + Provisions for future use of data/services (§6) + Expectations of Members (§6.6) + Duty of response by Members (§6.6) + Onboarding, testing & certification (§6.6) + Compliance with governing standards (§5, §6.6) 	<ul style="list-style-type: none"> + Openness & transparency (§6.6) + TF lifecycle management (§6.6) + Scalability to support array of Members (§6.8) + Glossary of TF terms/definitions (§1.4) + Component-based approach for different Member types (§6.6)

NASCIO, State Identity, Credential and Access Management (SICAM) Guidance and Roadmap, Sept. 2012.

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	Legal	Technical	Other
AAMVA DL/ID Security Framework	<ul style="list-style-type: none"> + Data element-level verification and validation (§1.3 #9, §1.4 #10, §1.4 #13, §3.3.4, §7.4, Appdx.) + Data (Name) collection, use and maintenance (§3.3.4, § 7.1, Appdx.) + AAMVA DL/ID Personal ID Card Design Specification (§1.4 #12, §3.3.4, 7.3, Appdx.) + Procedures for initial customer ID and validation (§3.3.3, §6.0) + Record & document use, permitted purpose (§3.3.5, §4.6, §7.1, §8.0) + Benefits/ business drivers (§2.0, §3.1) + Business-driven agreement among MVAs (§3.1, §3.3, §4.5) + Business requirements for P&Ps, document issuing systems, and internal controls, Driver License Agreement (DLA) (§3.3.1, §4.2, §4.5, Appdx.) 	<ul style="list-style-type: none"> + Assumes MVA compliance with applicable law, document use, data sharing (§1.5 All Recs., §3.1, §3.2, §3.3.5, §4.5, §8.3, Appdx.) + Enforcement thru business requirements (§2.0, §3.1, §4.5) + Audit plan (§1.1 #2, §1.2 #5, §3.3.2, §5.1, Appdx.) + Compliance and oversight, internal controls (§3.3.2, §4.4, §5.2) + Risk assessment & management (§1.1 #3, §3.3.5, § 4.2, §4.4, §8.0) + Privacy (§1.1 #4, §4.2, Appdx., §3.3.4, §3.3.5, §4.5, §4.6, §7.1, §7.4, §8.3) + Common set of verifiable resources (§1.3 #8, §3.3.3, §6.2, Appdx.) + Machine-Readable Technology (MRT) (§3.3.5, §8.2, Appdx.) + Restrictions, minimum penalties and sanctions (§3.3.5, §8.1, Appdx.) 	<ul style="list-style-type: none"> + Electronic verification (w/issuing entity) of DL/ID data elements (§1.3 #9, §3.3.3, §6.3) + Standards for MVA system integrity, interoperability & reciprocity (§2.0, §3.1, §3.3.2, §4.2, §4.5) + Compliance with governing standards (§3.3.2, §4.5, §5.2) + System integrity, security & privacy (§4.6) 	<ul style="list-style-type: none"> + Compliance and implementation support thru FDR employee training (§1.1 #1, §3.3.1, §4.1) + Common definition of “residency” (§1.3 #6, §3.3.3) tied to DL/ID verification (§1.3 #7, §3.3.3, §6.1) + “End of stay” on immigration doc. as expiration date for DL/ID - data element derivation (§1.4 #11, §3.3.4, §7.2, Appdx.) + Horizontal scalability thru reciprocity (§3.1) + Openness enforced thru privacy provisions (§4.6, §7.1) + Limits on disclosure enforced thru privacy provisions (§4.6, 7.1) + Glossary of abbreviations/ acronyms (§9.0) + LE Use Case (§1.5 Rec. #8, data sharing §3.3.5, §8.3, Appdx.)

AAMVA. DL/ID Security Framework, Feb. 2004.

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	Legal	Technical	Other
<p>eHealth Exchange Data Use & Reciprocal Support Agreement (DURSA)</p>	<ul style="list-style-type: none"> + Limitations on use of data (§1.jj; §3; §5.01-5.03) + Governance Authority (§4) & change processes (§10.03; §11.03) + Operating policies & procedures (§11; Appdx.; change process in §11.03) + Security, privacy & confidentiality (§7; §8; §14) + Suspension & termination (§19) + Data elements & data classification (attribute level/PII) (§1.v; §1.w; §1.kk) + Expectations of performance (§12) 	<ul style="list-style-type: none"> + Definition/compliance w/ applicable law (§1.a; §15.11; §23.01; Appdx.) + Legal agreements for exchange structure (recitals; §1.ee; §3.01; §23.07) + Security, privacy & consent (§14) + Liability (§18) + Representations & warranties (§15; disclaimers in §17) + Grant of authority (§4.03) + Dispute resolution (§21; Appdx.) + Authorizations for data exchange (§12; §13) + Open disclosure & anti-circumvention (§15; §23.04; §23.07) + Confidential Person information (§16) + Audit (§9) + Accountability & compliance (§10.01; 11.01; §15.03; §15.06) 	<ul style="list-style-type: none"> + Performance & service specifications (§10; Appdx.; change process in §10.03) + Security, privacy & confidentiality (§7; §8; §14) + Breach notification (§14.03) + System access (§6) + Provisions for future use of data (§5.02) + Expectations of Members (§12) + Duty of response by Members (§13) + Onboarding, testing & certification (§10.01) + Handling of test data v. production data (§15.07) 	<ul style="list-style-type: none"> + Openness & transparency (overview; recitals) + TF lifecycle management (“living agreement”) (overview; §4; §10.03; §11.03) + Scalability to support array of Members (horizontal/vertical) (Member types defined in §1; expectations in §12.02; duties in §13) + Glossary of TF terms/definitions (§1) + Component-based approach for different Member types (types defined in §1; expectations in §12.02; duties in §13; warranties in §15)

eHealth Exchange, Data Use and Reciprocal Support Agreement, Sept. 2014.

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	Legal	Technical	Other
InCommon Trust Framework	<ul style="list-style-type: none"> + Limitations on use of data (ICPOP; IAS; limits on use of ID information in PA §9) + Governance Authority & change processes (ICPOP; PA §17) + Operating policies & procedures (ICPOP) + Security, privacy & confidentiality (PA §6, §9; ICPOP) + Suspension & termination (PA §5.b, §5.c) + Data elements & data classification (attribute level/PII) (IAS; PA §6.b) + Expectations of performance (PA §6, §7) + Use cases and examples (InCommon Website; ICBP; Members) 	<ul style="list-style-type: none"> + Definition/compliance w/ applicable law (PA §15) + Legal agreements for exchange structure (ICPP; PA §6, §7.b) + Security, privacy & consent (PA §6, §9) + Liability (PA §11, includes disclaimer & limitations) + Representations & warranties (addressed in PA §7.b) + Grant of authority to executive (PA §18) + Dispute resolution process (PA §10; ICBL §5) + Authorizations for data exchange (PA §18) + Open disclosure & anti-circumvention (PA §14, §16) + Confidential Person information (PA §8, §9) + Audit (ICPOP) + Accountability & compliance (PA §15) 	<ul style="list-style-type: none"> + Performance & service specifications (PA §6, §7) + Security, privacy & confidentiality (ICPOP) + Breach notification (PA and addenda; ICPOP) + System access (ICPOP) + Provisions for future use of data (ICPOP) + Expectations of Members (PA §6, §7) + Duty of response by Members (PA §6, §7) + Onboarding, testing & certification (ICPOP) + Handling of test data v. production data (ICPOP) 	<ul style="list-style-type: none"> + Openness & transparency (ICBP) + TF lifecycle management (“living agreement”) (ICBL; PA §17) + Implementation support (ICPOP) + Scalability to support array of Members (horizontal/vertical) (Member types defined in Join §1, Members) + Glossary of TF terms/definitions (InCommon Website) + Component-based approach for different Member types (Members)

ICPOP=InCommon Member Operational Practices
 PA=InCommon Participation Agreement
 IAS=InCommon Attribute Summary

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	Legal	Technical	Other
Kantara Initiative Trust Framework	<ul style="list-style-type: none"> + Limitations on use of data (KTR MTAU) + Governance Authority (BL §4; OP §2) & change/ amendment processes (BL §12; OP §9; MA §3) + Operating policies & procedures (OP) + Security, privacy & confidentiality (AP; MA) + Suspension & termination (MA §2; BL §8.11; KTR MTAU) + Data elements & data classification (KTR; KIC) + Expectations of performance (AP; KTR MTAU; KIC) + Use cases (Working groups for business cases-trusted federations) 	<ul style="list-style-type: none"> + Definition/identification of applicable law (KTR MTAU; see also “Governing law and jurisdiction” provision in KTR MTAU) + Legal agreement for exchange structure (MA) + Security, privacy & consent provisions + Liability (KTR MTAU) + Warranty (KTR MTAU) + Grant of authority (MA) + Authorizations for data requests by Member + Open disclosure & anti-circumvention (Other agreements in KTR MTAU) + Confidential Person information (Options set in IPRP; IPRP Art. 3) + Accountability & compliance (w/ antitrust laws in BL §17; MA) 	<ul style="list-style-type: none"> + Performance & service specifications (AP; KTR/KTV; KTR MTAU; KIC; Member protection & treatment in IPRP) + Security, privacy & confidentiality (AP; MA) + Technical certification & testing (AP; KIC) + Standards for technical & operational interoperability (KTR; MA goal #3; #7; KIC) 	<ul style="list-style-type: none"> + Open & transparent governance model (MA goals #3, #4; op; BL §3) + TF lifecycle management (MA goals #4, #6) + Support & capacity building (IGs) + Scalability to support array of Members (horizontal/vertical) (member types BL §8) + TF definitions (BL §1; OP §1; IPRP Art. 2)

BL=Bylaws; IPRP=Intellectual Property Rights Policies; MA=Member Agreement; OP=Operating Procedures
 KTR=Kantara Trust Registry; KTV=KTR Trust Validation; KTR MTAU=Metadata Terms of Access & Use; KIC=Kantara Interoperability Cert.-SAML, OATH, etc.
 AP= Assurance Programs; Identity Assurance Accreditation & Approval and Interoperability Certification Programs

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	Legal	Technical	Other
Open Identity Exchange (OIX)/OITF Model	<ul style="list-style-type: none"> + Limitations on use of data (OITF §III.B, §III.C, §V) + Governance Authority & change processes (OIX; OITF §III.C) + Operating policies & procedures (OIX; OITF §II, §III.B, §III.C) + Security, privacy & confidentiality (OIX; OITF §III.A, §V) + Suspension & termination (OITF §III.C) + Data elements & data classification (attribute level/PII) (OIX; OITF §III.A, §III.B) + Expectations of performance (OIX; OITF §II, §III.C) + Use cases for agreement, transaction & Member types (OITF §I, §III; OIX) 	<ul style="list-style-type: none"> + Compliance w/ applicable law (OIX; OITF §V) + Legal agreements for exchange structure (OIX; OITF §II, §III.C) + Security, privacy & consent (OIX; OITF §III.A) + Liability, representations & warranties (OITF §III.C) + Grant of authority (OIX; OITF §III.C) + Dispute resolution (OITF §II, §III.C, §V) + Authorizations for data exchange (OIX; OITF §III.A) + Anti-circumvention & open disclosure (OITF §V) + Audit (OIX; OITF §II, §III.B, §V) + Accountability & compliance (OIX; OITF §II, §V) 	<ul style="list-style-type: none"> + Performance & service specifications (OIX; OITF §II, §III.A, §III.B) + Security, privacy & confidentiality (OIX; OITF §III.A; §V) + Expectations of Members (OIX; OITF §III.A, §III.B, §III.C) + Onboarding, testing & certification (OIX; OITF §II, §III.B) 	<ul style="list-style-type: none"> + Openness & transparency (OIX; OITF §I; statement in OITF §V, §VI) + TF lifecycle management (OIX; OITF §II) + Scalability to support array of Members (horizontal/vertical) (OITF §II, §III.C, §IV) + High-level definitions (OITF §I) + Component-based approach for different Member types (OIX; OITF §II, §III.C) + Use cases & examples of TFs (OITF §IV)

OITF=The Open Identity Trust Framework (OITF) Model, March 2010
OIX=Open Identity Exchange Trust Framework Requirements and Guidelines v. 1 (Draft 2)