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 This Guidance Document shall be effective as of December 1, 2017 and shall remain in force and effect unless rescinded or amended by further action pursuant to Section 2.2-436 of the *Code of Virginia*.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

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, *Code of Virginia*
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:

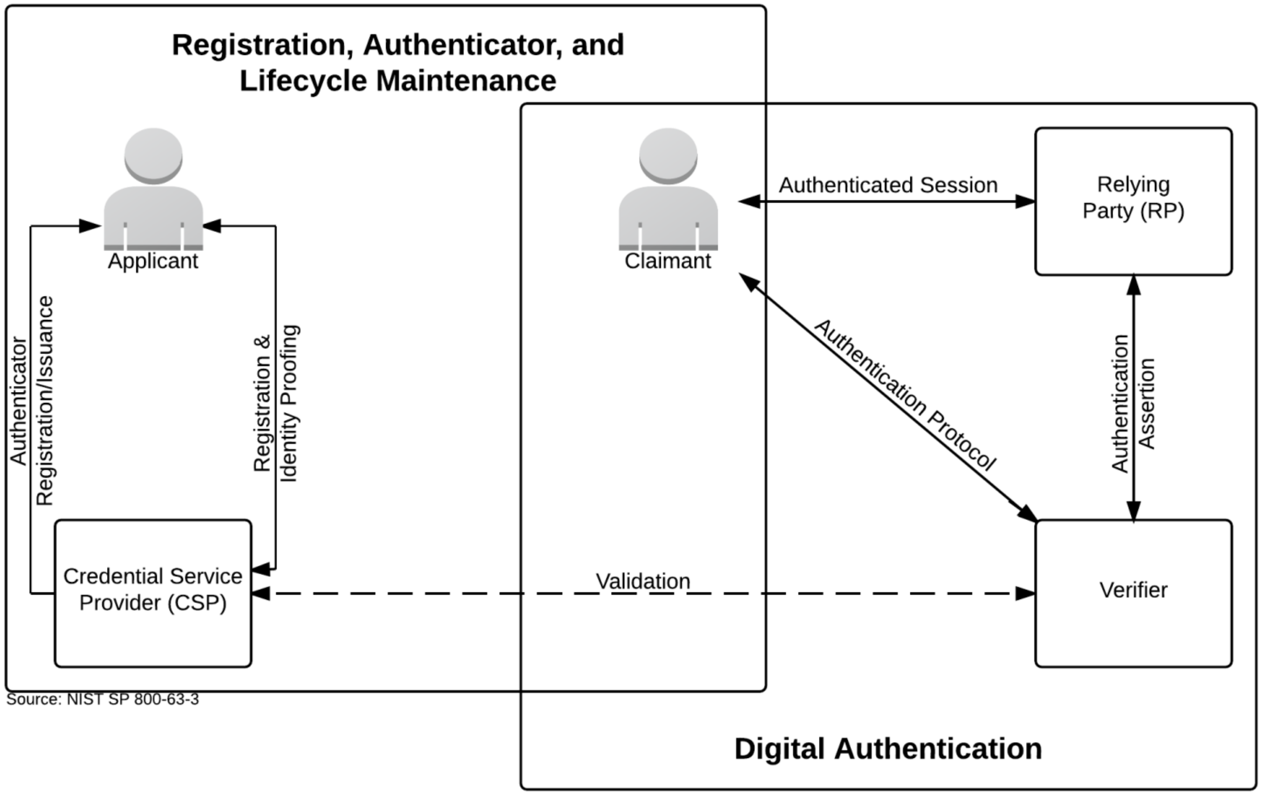
1. The claimant proves to the verifier that he or she possesses and controls the authenticator through an authentication protocol.
2. The verifier interacts with the CSP to validate the credential that binds the claimant's identity to his or her authenticator and to optionally obtain claimant attributes.
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