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 This Guidance Document shall be effective as of December 1, 2017 and shall remain in force and effect unless rescinded or amended by further action pursuant to Section 2.2-436 of the *Code of Virginia*.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

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 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.

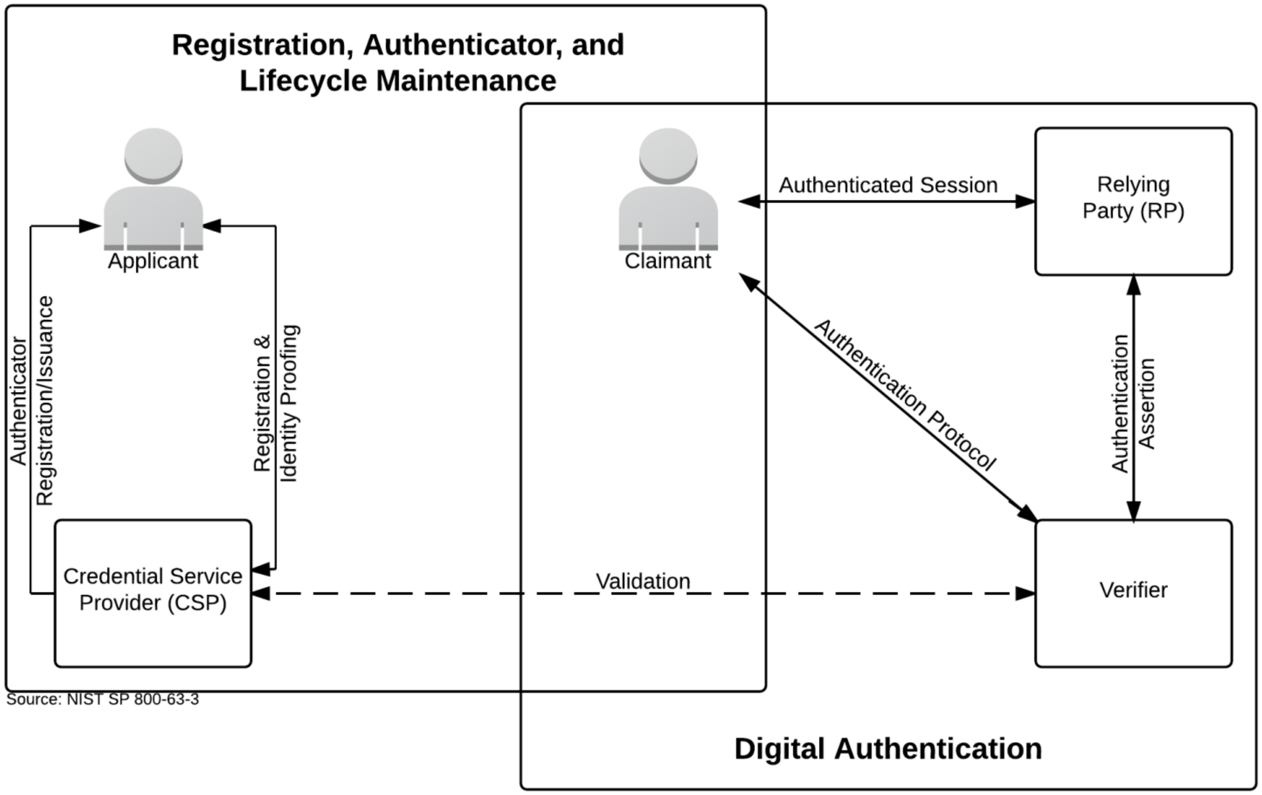
This document establishes minimum specifications for authenticators and lifecycle management conformant with NIST SP 800-63B. However, the minimum specifications defined in this document have been developed to accommodate requirements for authenticators established under other national and international 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. ‘aaaaaa’, ‘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 shoud 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 choses to increase IAL in order to bind to a suitable authenticator they already have.

1. The CSP may accept an existing authenticator at or above the desired IAL
2. The CSP must require the user to authenticate using their existing authenticator
3. The CSP must execute all required identity proofing processes for the desired IAL
4. If the user successfully completes identity proofing, the CSP may issue an enrollment code (temporary secret) that confirms address of record as per *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.