

# COMMONWEALTH OF VIRGINIA



## IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

### GUIDANCE DOCUMENT Authenticators and Lifecycle Management

**Table of Contents**

1 Publication Version Control ..... 1  
2 Reviews ..... 1  
3 Purpose and Scope ..... 2  
4 Statutory Authority ..... 3  
5 Definitions ..... 4  
6 Background ..... 16  
7 Minimum Specifications ..... 17

DRAFT

## 1 Publication Version Control

---

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

Publication Version	Date	Revision Description
1.0	07/20/2016	Initial Draft of Document
1.0	09/12/2016	Document revised by VITA staff based on public comment received pursuant to § 2.2-437.C, <i>Code of Virginia</i>
1.0	09/30/2016	Document revised by VITA staff based on comments from IMSAC during September 12, 2016, public meeting
1.0	12/05/2016	Document revised based on direction from VITA's Legal and Legislative Services Directorate and the Office of the Attorney General following September 12, 2016, public meeting

## 2 Reviews

---

- The initial version of the document was prepared by staff from the Virginia Information Technologies Agency (VITA) for the Secretary of Technology, under the direction from 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, *Code of Virginia*. The document was 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.). IMSAC allowed at least 30 days for the submission of written comments following the posting and publication and held a meeting dedicated to the receipt of oral comment on September 12, 2016, more than 15 days after the posting and publication.
- The document will be reviewed in a manner compliant with the Commonwealth of Virginia's Administrative Process Act, § 2.2-4000 et seq.

### 25 3 Purpose and Scope

---

26

27 Pursuant to § 2.2-436 and § 2.2-437, *Code of Virginia*, this guidance document was developed  
28 by the Identity Management Standards Advisory Council (IMSAC), on behalf of the Secretary of  
29 Technology, to establish minimum specifications for Digital Identity Systems so as to warrant  
30 liability protection pursuant to the Electronic Identity Management Act ("the Act"), Chapter 50  
31 of Title 59.1. The guidance document, as defined in § 2.2-4001, was prepared to provide  
32 information or guidance of general applicability to the public for interpreting or implementing  
33 the Act. The guidance document was not developed as a Commonwealth of Virginia  
34 Information Technology Resource Management (ITRM) Policy, Standard, and Guideline,  
35 pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive  
36 branch agencies of the Commonwealth of Virginia.

DRAFT

## 37 4 Statutory Authority

---

38

39 The following section documents the statutory authority established in the *Code of Virginia* for  
40 the development of minimum specifications and standards for Assertions within a Digital  
41 Identity System. References to statutes below and throughout this document shall be to the  
42 *Code of Virginia*, unless otherwise specified.

43

### 44 Governing Statutes:

45

#### 46 Secretary of Technology

47 § 2.2-225. Position established; agencies for which responsible; additional powers

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

49

#### 50 Identity Management Standards Advisory Council

51 § 2.2-437. Identity Management Standards Advisory Council

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

53

#### 54 Commonwealth Identity Management Standards

55 § 2.2-436. Approval of electronic identity standards

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

57

#### 58 Electronic Identity Management Act

59 Chapter 50. Electronic Identity Management Act

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

61

62

63

64

65

66

## 67 5 Definitions

---

68  
69 Terms used in this document comply with definitions in the Public Review version of the  
70 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3),  
71 and align with adopted definitions in § 59.1-550, *Code of Virginia* (COV), and the  
72 Commonwealth of Virginia's ITRM Glossary (ITRM Glossary).<sup>1</sup>

73  
74 Active Attack: An online attack where the attacker transmits data to the claimant, credential  
75 service provider, verifier, or relying Participant. Examples of active attacks include man-in-the-  
76 middle, impersonation, and session hijacking.

77  
78 Address of Record: The official location where an individual can be found. The address of record  
79 always includes the residential street address of an individual and may also include the mailing  
80 address of the individual. In very limited circumstances, an Army Post Office box number, Fleet  
81 Post Office box number or the street address of next of kin or of another contact individual can  
82 be used when a residential street address for the individual is not available.

83  
84 Approved: Federal Information Processing Standard (FIPS) approved or NIST recommended. An  
85 algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2)  
86 adopted in a FIPS or NIST Recommendation.

87  
88 Applicable Law: Laws, statutes, regulations, and rules of the jurisdiction in which the members  
89 of an Identity Trust Framework operates.

90  
91 Applicant: A Participant undergoing the processes of Registration and Identity Proofing.

92  
93 Assertion: A statement from a verifier to a relying Participant (RP) that contains identity  
94 information about a Subscriber. Assertions may also contain verified attributes.

95  
96 Assertion Reference: A data object, created in conjunction with an Assertion, which identifies  
97 the verifier and includes a pointer to the full Assertion held by the verifier.

98  
99 Assurance: In the context of [OMB M-04-04]<sup>2</sup> and this document, assurance is defined as 1) the  
100 degree of confidence in the vetting process used to establish the identity of an individual to  
101 whom the credential was issued, and 2) the degree of confidence that the individual who uses  
102 the credential is the individual to whom the credential was issued.

---

<sup>1</sup> NIST SP 800-63-3 may be accessed at <https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3>. At the time of the publication of this document, NIST SP 800-63-3 was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3.

§ 59.1-550, *Code of Virginia*, may be accessed at <http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550/>. The Commonwealth's ITRM Glossary may be accessed at [http://www.vita.virginia.gov/uploadedFiles/VITA\\_Main\\_Public/Library/PSGs/PSG\\_Sections/COV\\_ITRM\\_Glossary.pdf](http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/PSG_Sections/COV_ITRM_Glossary.pdf)

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

- 103 Assurance Model: Policies, processes, and protocols that define how Assurance will be  
104 established in an Identity Trust Framework.  
105
- 106 Asymmetric Keys: Two related keys, a public key and a private key that are used to perform  
107 complementary operations, such as encryption and decryption or signature generation and  
108 signature verification.  
109
- 110 Attack: An attempt by an unauthorized individual to fool a verifier or a relying Participant into  
111 believing that the unauthorized individual in question is the Subscriber.  
112
- 113 Attacker: A Participant who acts with malicious intent to compromise an Information System.  
114
- 115 Attribute: A claim of a named quality or characteristic inherent in or ascribed to someone or  
116 something.  
117
- 118 Authentication: The process of establishing confidence in the identity of users or Information  
119 Systems.  
120
- 121 Authentication Protocol: A defined sequence of messages between a claimant and a verifier  
122 that demonstrates that the claimant has possession and control of a valid authenticator to  
123 establish his/her identity, and optionally, demonstrates to the claimant that he or she is  
124 communicating with the intended verifier.  
125
- 126 Authentication Protocol Run: An exchange of messages between a claimant and a verifier that  
127 results in authentication (or authentication failure) between the two Participants.  
128
- 129 Authentication Secret: A generic term for any secret value that could be used by an attacker to  
130 impersonate the Subscriber in an authentication protocol. These are further divided into short-  
131 term authentication secrets, which are only useful to an attacker for a limited period of time,  
132 and long-term authentication secrets, which allow an attacker to impersonate the Subscriber  
133 until they are manually reset. The authenticator secret is the canonical example of a long term  
134 authentication secret, while the authenticator output, if it is different from the authenticator  
135 secret, is usually a short term authentication secret.  
136
- 137 Authenticator: Something that the claimant possesses and controls (typically a cryptographic  
138 module or password) that is used to authenticate the claimant's identity. In previous versions of  
139 this guideline, this was referred to as a token.  
140
- 141 Authenticator Assurance Level (AAL): A metric describing robustness of the authentication  
142 process proving that the claimant is in control of a given Subscriber's authenticator(s).  
143
- 144 Authenticator Output: The output value generated by an authenticator. The ability to generate  
145 valid authenticator outputs on demand proves that the claimant possesses and controls the

146 authenticator. Protocol messages sent to the verifier are dependent upon the authenticator  
147 output, but they may or may not explicitly contain it.

148

149 Authenticator Secret: The secret value contained within an authenticator.

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

151

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

156

157 Bit: A binary digit: 0 or 1.

158

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

162

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

164

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

167

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

176

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

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

183

184 Claimed Identity: A declaration by the applicant of their current Personal Name, date of birth  
185 and address. [GPG45]<sup>4</sup>

---

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

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

190

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

193

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

199

200 Credential Service Provider (CSP): A trusted entity that issues or registers Subscriber  
201 authenticators and issues electronic credentials to Subscribers. The CSP may encompass  
202 Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third  
203 Participant, or may issue credentials for its own use.

204

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

211

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

217

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

222

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

224

---

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

225 Data Integrity: The property that data has not been altered by an unauthorized entity.  
226

227 Derived Credential: A credential issued based on proof of possession and control of an  
228 authenticator associated with a previously issued credential, so as not to duplicate the Identity  
229 Proofing process.  
230

231 Digital Identity System: An Information System that supports Electronic Authentication and the  
232 management of a person's Identity in a digital environment. [Referenced in § 59.1-550, COV]  
233

234 Digital Signature: An asymmetric key operation where the private key is used to digitally sign  
235 data and the public key is used to verify the signature. Digital signatures provide authenticity  
236 protection, integrity protection, and non-repudiation.  
237

238 Eavesdropping Attack: An attack in which an attacker listens passively to the authentication  
239 protocol to capture information which can be used in a subsequent active attack to  
240 masquerade as the claimant.  
241

242 Electronic Authentication: The process of establishing confidence in user identities  
243 electronically presented to an Information System.  
244

245 Entropy: A measure of the amount of uncertainty that an attacker faces to determine the value  
246 of a secret. Entropy is usually stated in bits.  
247

248 Extensible Mark-up Language (XML): Extensible Markup Language, abbreviated XML, describes  
249 a class of data objects called XML documents and partially describes the behavior of computer  
250 programs which process them.  
251

252 Federal Bridge Certification Authority (FBCA): The FBCA is the entity operated by the Federal  
253 Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI  
254 Policy Authority to create, sign, and issue public key certificates to Principal CAs.  
255

256 Federal Information Security Management Act (FISMA): Title III of the E-Government Act  
257 requiring each federal agency to develop, document, and implement an agency-wide program  
258 to provide information security for the information and Information Systems that support the  
259 operations and assets of the agency, including those provided or managed by another agency,  
260 contractor, or other source.  
261

262 Federal Information Processing Standard (FIPS): Under the Information Technology  
263 Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards  
264 and guidelines that are developed by the National Institute of Standards and Technology (NIST)  
265 for Federal computer systems. These standards and guidelines are issued by NIST as Federal  
266 Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when

267 there are compelling Federal government requirements such as for security and interoperability  
268 and there are no acceptable industry standards or solutions.<sup>5</sup>

269

270 Federation: A process that allows for the conveyance of identity and authentication information  
271 across a set of networked systems. These systems are often run and controlled by disparate  
272 Participants in different network and security domains. [NIST SP 800-63C]

273

274 Governance Authority: Entity responsible for providing policy level leadership, oversight,  
275 strategic direction, and related governance activities within an Identity Trust Framework.

276

277 Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string.

278 Approved hash functions satisfy the following properties:

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

283

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

288

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

290

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

293

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

296

297 Identity Provider (IdP): The party that manages the subscriber's primary authentication  
298 credentials and issues Assertions derived from those credentials generally to the credential  
299 service provider (CSP).

300

301 Identity Trust Framework: A Digital Identity System with established identity, security, privacy,  
302 technology, and enforcement rules and policies adhered to by certified identity providers that  
303 are members of the Identity Trust Framework. Members of an Identity Trust Framework  
304 include Identity Trust Framework operators and identity providers. Relying Participants may be,  
305 but are not required to be, a member of an Identity Trust Framework in order to accept an  
306 identity credential issued by a certified identity provider to verify an identity credential holder's  
307 identity. [§ 59.1-550, COV]

308

---

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

309 Information System: A discrete set of information resources organized for the collection,  
310 processing, maintenance, use, sharing, dissemination, or disposition of information. [NIST  
311 Interagency/Internal Report (IR) 7298 r. 2]  
312

313 Kerberos: A widely used authentication protocol developed at MIT. In “classic” Kerberos, users  
314 share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to  
315 communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by  
316 the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords,  
317 the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who  
318 capture the initial user-to- KDC exchange. Longer password length and complexity provide  
319 some mitigation to this vulnerability, although sufficiently long passwords tend to be  
320 cumbersome for users.  
321

322 Knowledge Based Authentication: Authentication of an individual based on knowledge of  
323 information associated with his or her Claimed Identity in public databases. Knowledge of such  
324 information is considered to be private rather than secret, because it may be used in contexts  
325 other than authentication to a verifier, thereby reducing the overall assurance associated with  
326 the authentication process.  
327

328 Man-in-the-Middle Attack (MitM): An attack on the authentication protocol run in which the  
329 attacker positions himself or herself in between the claimant and verifier so that he can  
330 intercept and alter data traveling between them.  
331

332 Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric  
333 key to detect both accidental and intentional modifications of the data. MACs provide  
334 authenticity and integrity protection, but not non-repudiation protection.  
335

336 Multi-Factor: A characteristic of an authentication system or an authenticator that uses more  
337 than one authentication factor. The three types of authentication factors are something you  
338 know, something you have, and something you are.  
339

340 Network: An open communications medium, typically the Internet, that is used to transport  
341 messages between the claimant and other Participants. Unless otherwise stated, no  
342 assumptions are made about the security of the network; it is assumed to be open and subject  
343 to active (i.e., impersonation, man-in-the-middle, session hijacking) and passive (i.e.,  
344 eavesdropping) attack at any point between the Participants (e.g., claimant, verifier, CSP or RP).  
345

346 Nonce: A value used in security protocols that is never repeated with the same key. For  
347 example, nonces used as challenges in challenge-response authentication protocols must not  
348 be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay  
349 attack. Using a nonce as a challenge is a different requirement than a random challenge,  
350 because a nonce is not necessarily unpredictable.  
351

352 Off-line Attack: An attack where the attacker obtains some data (typically by eavesdropping on  
353 an authentication protocol run or by penetrating a system and stealing security files) that  
354 he/she is able to analyze in a system of his/her own choosing.  
355

356 Online Attack: An attack against an authentication protocol where the attacker either assumes  
357 the role of a claimant with a genuine verifier or actively alters the authentication channel.  
358

359 Online Guessing Attack: An attack in which an attacker performs repeated logon trials by  
360 guessing possible values of the authenticator output.  
361

362 Operational Authority: Entity responsible for operations, maintenance, management, and  
363 related functions of an Identity Trust Framework.  
364

365 Participant Requirements: A set of rules and policies in an Identity Trust Framework addressing  
366 identity, security, privacy, technology, and enforcement, which are assigned to each member  
367 type in a Digital Identity System. Member types include Registration Authorities (RAs), Identity  
368 Providers (IdPs), Credential Service Providers (CSPs), Verifiers, and Relying Parties (RPs).  
369 [§ 59.1-550, COV]  
370

371 Passive Attack: An attack against an authentication protocol where the attacker intercepts data  
372 traveling along the network between the claimant and verifier, but does not alter the data (i.e.,  
373 eavesdropping).  
374

375 Password: A secret that a claimant memorizes and uses to authenticate his or her identity.  
376 Passwords are typically character strings.  
377

378 Personal Identification Number (PIN): A password consisting only of decimal digits.  
379

380 Personal Identity Verification (PIV) Card: Defined by [FIPS 201] as a physical artifact (e.g.,  
381 identity card, smart card) issued to federal employees and contractors that contains stored  
382 credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that  
383 the Claimed Identity of the cardholder can be verified against the stored credentials by another  
384 person (human readable and verifiable) or an automated process (computer readable and  
385 verifiable).  
386

387 Personally Identifiable Information (PII): As defined by OMB Circular A-130, Personally  
388 Identifiable Information means information that can be used to distinguish or trace an  
389 individual's identity, either alone or when combined with other information that is linked or  
390 linkable to a specific individual.  
391

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

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

399

400 Physical In-Person: Method of Identity Proofing in which Applicants are required to physically  
401 present themselves and identity evidence to a representative of the Registration Authority or  
402 Identity Trust Framework. [NIST SP 800-63-2]

403

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

406

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

410

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

413

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

416

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

423

424 Pseudonymous Identifier: A meaningless, but unique number that does not allow the RP to  
425 infer the Subscriber but which does permit the RP to associate multiple interactions with the  
426 Subscriber's Claimed Identity.

427

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

430

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

433

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

438

439 Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software and  
440 workstations used for the purpose of administering certificates and public-private key pairs,  
441 including the ability to issue, maintain, and revoke public key certificates.  
442

443 Registration: The process through which an applicant applies to become a Subscriber of a CSP  
444 and an RA validates the identity of the applicant on behalf of the CSP.  
445

446 Registration Authority (RA): A trusted entity that establishes and vouches for the identity or  
447 attributes of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be  
448 independent of a CSP, but it has a relationship to the CSP(s).  
449

450 Relying Party (RP): An entity that relies upon the Subscriber's authenticator(s) and credentials  
451 or a verifier's Assertion of a claimant's identity, typically to process a transaction or grant access  
452 to information or a system.  
453

454 Remote: (As in remote authentication or remote transaction) An information exchange  
455 between network-connected devices where the information cannot be reliably protected end-  
456 to-end by a single organization's security controls. Note: Any information exchange across the  
457 Internet is considered remote.  
458

459 Replay Attack: An attack in which the attacker is able to replay previously captured messages  
460 (between a legitimate claimant and a verifier) to masquerade as that claimant to the verifier or  
461 vice versa.  
462

463 Risk Assessment: The process of identifying the risks to system security and determining the  
464 probability of occurrence, the resulting impact, and additional safeguards that would mitigate  
465 this impact. Part of Risk Management and synonymous with Risk Analysis.  
466

467 Salt: A non-secret value that is used in a cryptographic process, usually to ensure that the  
468 results of computations for one instance cannot be reused by an attacker.  
469

470 Secondary Authenticator: A temporary secret, issued by the verifier to a successfully  
471 authenticated Subscriber as part of an Assertion protocol. This secret is subsequently used, by  
472 the Subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer  
473 Assertions, Assertion references, and Kerberos session keys.  
474

475 Secure Sockets Layer (SSL): An authentication and security protocol widely implemented in  
476 browsers and web servers. SSL has been superseded by the newer Transport Layer Security  
477 (TLS) protocol; TLS 1.0 is effectively SSL version 3.1.  
478

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

483 SAML Authentication Assertion: A SAML Assertion that conveys information from a verifier to  
484 an RP about a successful act of authentication that took place between the verifier and a  
485 Subscriber.  
486

487 Session Hijack Attack: An attack in which the attacker is able to insert himself or herself  
488 between a claimant and a verifier subsequent to a successful authentication exchange between  
489 the latter two Participants. The attacker is able to pose as a Subscriber to the verifier or vice  
490 versa to control session data exchange. Sessions between the claimant and the relying  
491 Participant can also be similarly compromised.  
492

493 Shared Secret: A secret used in authentication that is known to the claimant and the verifier.  
494

495 Social Engineering: The act of deceiving an individual into revealing sensitive information by  
496 associating with the individual to gain confidence and trust.  
497

498 Special Publication (SP): A type of publication issued by NIST. Specifically, the Special  
499 Publication 800-series reports on the Information Technology Laboratory's research, guidelines,  
500 and outreach efforts in computer security, and its collaborative activities with industry,  
501 government, and academic organizations.  
502

503 Strongly Bound Credentials: Credentials that describe the binding between a user and  
504 authenticator in a tamper-evident fashion.  
505

506 Subscriber: A Participant who has received a credential or authenticator from a CSP.  
507

508 Symmetric Key: A cryptographic key that is used to perform both the cryptographic operation  
509 and its inverse, for example to encrypt and decrypt, or create a message authentication code  
510 and to verify the code.  
511

512 Token: See Authenticator.  
513

514 Token Authenticator: See Authenticator Output.  
515

516 Token Secret: See Authenticator Secret.  
517

518 Transport Layer Security (TLS): An authentication and security protocol widely implemented in  
519 browsers and web servers. TLS is defined by [RFC 5246]. TLS is similar to the older Secure  
520 Sockets Layer (SSL) protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52,  
521 Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations specifies  
522 how TLS is to be used in government applications.  
523

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

527 Unverified Name: A Subscriber name that is not verified as meaningful by Identity Proofing.  
528  
529 Valid: In reference to an ID, the quality of not being expired or revoked.  
530  
531 Verified Name: A Subscriber name that has been verified by Identity Proofing.  
532  
533 Verifier: An entity that verifies the claimant's identity by verifying the claimant's possession and  
534 control of one or two authenticators using an authentication protocol. To do this, the verifier  
535 may also need to validate credentials that link the authenticator(s) and identity and check their  
536 status.  
537  
538 Verifier Impersonation Attack: A scenario where the attacker impersonates the verifier in an  
539 authentication protocol, usually to capture information that can be used to masquerade as a  
540 claimant to the real verifier.  
541  
542 Virtual In-Person Proofing: A remote identity person proofing process that employs technical  
543 and procedural measures that provide sufficient confidence that the remote session can be  
544 considered equivalent to a physical, in-person identity proofing encounter. [NIST SP 800-63A]  
545  
546 Weakly Bound Credentials: Credentials that describe the binding between a user and  
547 authenticator in a manner than can be modified without invalidating the credential.  
548  
549 Zeroize: Overwrite a memory location with data consisting entirely of bits with the value zero  
550 so that the data is destroyed and not recoverable. This is often contrasted with deletion  
551 methods that merely destroy reference to data within a file system rather than the data itself.  
552  
553 Zero-knowledge Password Protocol: A password based authentication protocol that allows a  
554 claimant to authenticate to a Verifier without revealing the password to the verifier. Examples  
555 of such protocols are EKE, SPEKE and SRP.

## 556 6 Background

---

557

558 In 2015, Virginia’s General Assembly passed the Electronic Identity Management Act (Chapter  
559 50 of Title 59.1, *Code of Virginia*) to address demand in the state’s digital economy for secure,  
560 privacy enhancing Electronic Authentication and identity management. Growing numbers of  
561 “communities of interest” have advocated for stronger, scalable and interoperable identity  
562 solutions to increase consumer protection and reduce liability for principal actors in the identity  
563 ecosystem – Identity Providers, Credential Service Providers and Relying Parties.

564

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

570

571 The Advisory Council recommends to the Secretary of Technology guidance documents relating  
572 to (i) nationally recognized technical and data standards regarding the verification and  
573 authentication of identity in digital and online transactions; (ii) the minimum specifications and  
574 standards that should be included in an Identity Trust Framework, as defined in §59.1-550, so  
575 as to warrant liability protection pursuant to the Electronic Identity Management Act (§59.1-  
576 550 et seq.); and (iii) any other related data standards or specifications concerning reliance by  
577 third parties on identity credentials, as defined in §59.1-550.

578

### 579 Purpose Statement

580

581 This guidance document, as defined in § 2.2-4001, was developed by the Identity Management  
582 Standards Advisory Council (IMSAC), on behalf of the Secretary of Technology, to provide  
583 information or guidance of general applicability to the public for interpreting or implementing  
584 the Electronic Identity Management Act. Specifically, the document establishes minimum  
585 specifications for Authenticators and lifecycle management within a Digital Identity System. The  
586 minimum specifications have been designed to be conformant with NIST SP 800-63B.

587

588 The document defines minimum requirements, assurance levels, privacy, and security  
589 provisions for Authenticators and lifecycle management. The document assumes that specific  
590 business, legal, and technical requirements for Authenticators will be established in the Identity  
591 Trust Framework for each distinct Digital Identity System, and that these requirements will be  
592 designed based on the Identity Assurance Level (IAL) and Authenticator Assurance Level (AAL)  
593 requirements for the system.

594

595 The document limits its focus to Authenticators and lifecycle management. Minimum  
596 specifications for other components of a Digital Identity System have been defined in separate  
597 IMSAC guidance documents in this series, pursuant to §2.2-436 and §2.2-437.

## 598 7 Minimum Specifications

---

599  
600 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3)  
601 defines “Electronic Authentication” as “the process of establishing confidence in user identities  
602 electronically presented to an Information System.”<sup>12</sup> Information systems may use the  
603 authenticated identity to determine if that user is authorized to perform an electronic  
604 transaction.

605  
606 This document establishes minimum specifications for Authenticators and lifecycle  
607 management conformant with NIST SP 800-63B. However, the minimum specifications defined  
608 in this document have been developed to accommodate requirements for Authenticators  
609 established under other national and international standards.<sup>13</sup> The minimum specifications in  
610 this document also assume that specific business, legal, and technical requirements for a Digital  
611 Identity System will be documented in the Identity Trust Framework for that system. Minimum  
612 specifications for other components of a Digital Identity System have been documented in  
613 separate guidance documents in the IMSAC series, pursuant to §2.2-436 and §2.2-437.

### 614 615 Electronic Authentication Model

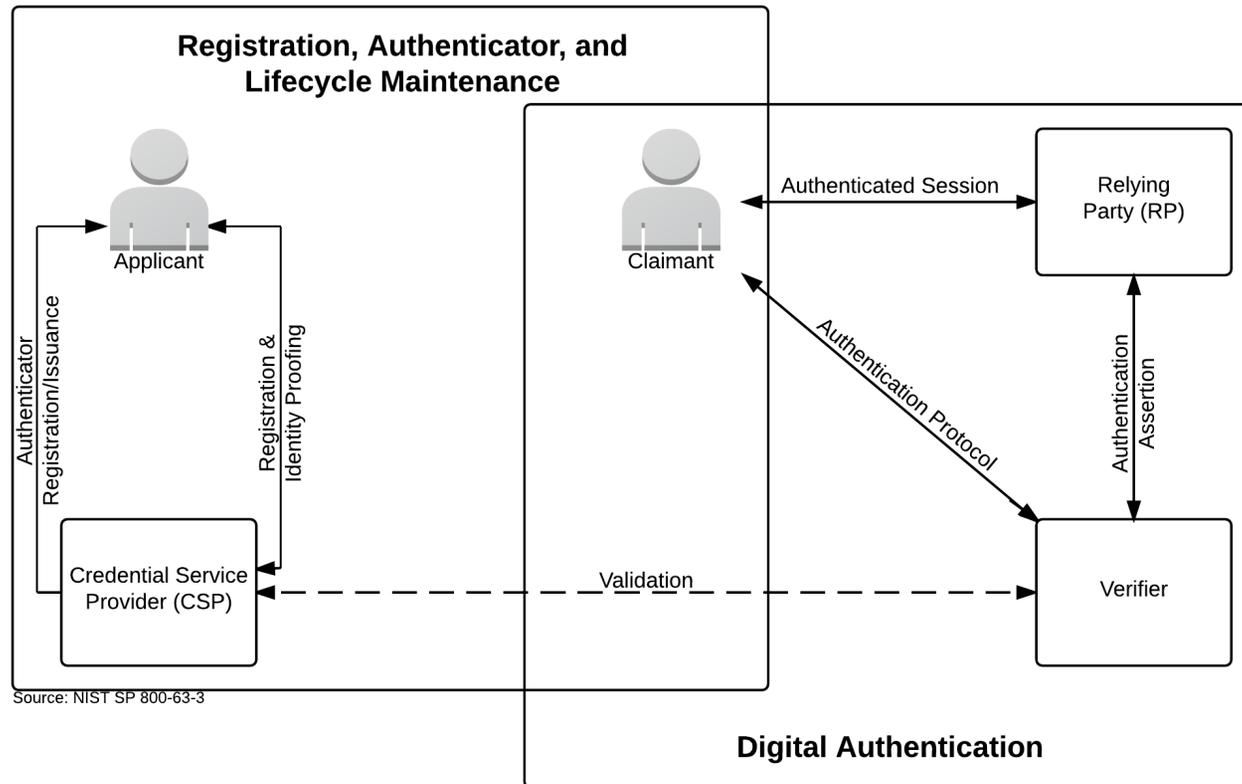
616  
617 Electronic Authentication is the process of establishing confidence in individual identities  
618 presented to a Digital Identity System. The minimum specifications in this document assume  
619 that the authentication and transaction take place across a network. The Electronic  
620 Authentication model used for these minimum specifications has been shown in Figure 1.  
621 Minimum specifications for the full Electronic Authentication model reflected in this document  
622 have been defined in *IMSAC Guidance Document: Electronic Authentication*.

---

<sup>12</sup> The Public Review version of National Institute of Standards and Technology Special Publication 800-63B (NIST SP 800-63B) may be accessed at <https://pages.nist.gov/800-63-3/sp800-63b.html>. At the time of the publication of this document, NIST SP 800-63B was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3.

<sup>13</sup> 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>.

623 **Figure 1. Electronic Authentication Model**



624  
625  
626 Source: NIST SP 800-63-3, accessible at <https://pages.nist.gov/800-63-3/sp800-63-3.html>  
627 Note: Figure 1 illustrates the model for Electronic Authentication in a Digital Identity System, as documented in NIST SP 800-63-3 (Public  
628 Review), containing all components, requirements, and specifications recommended by IMSAC. However, the minimum specifications  
629 defined in this document have been developed to accommodate requirements for Authenticators and lifecycle management established  
630 under other national and international standards.  
631

## 632 Assurance Model

633

634 The minimum specifications defined in this document for Authenticators and lifecycle  
635 management assume that the Identity Trust Framework for a Digital Identity System will define  
636 a specific Assurance Model for that system.<sup>14</sup> Therefore, the Assurance Model presented below,  
637 which is based on NIST SP 800-63-3, should be viewed as a recommended framework. Other  
638 Assurance Models have been established in OMB M-04-04 and the State Identity, Credential,  
639 and Access Management (SICAM) guidelines, published by the National Association of State  
640 Chief Information Officers (NASCIO). A crosswalk showing disparities in the NIST SP 800-63-3,  
641 OMB M-04-04, and SICAM Assurance Models has been provided in **Figure 2**.

642

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

645

646 Identity Assurance Level 2 – IAL 2 introduces the need for either Remote or In-Person (Physical  
647 or Virtual) Identity Proofing. IAL 2 requires identifying Attributes to have been verified in person  
648 or remotely using, at a minimum, the procedures given in NIST 800-63A.

649

650 Identity Assurance Level 3 – At IAL 3, In-Person (Physical or Virtual) Identity Proofing is  
651 required. Identifying Attributes must be verified by an authorized representative of the CSP  
652 through examination of physical documentation as described in NIST 800-63A.

653

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

661

662 Authenticator Assurance Level 2 – AAL 2 provides higher assurance that the same claimant who  
663 participated in previous transactions is accessing the protected transaction or data. Two  
664 different authentication factors are required. Various types of Authenticators, including multi-  
665 factor Software Cryptographic Authenticators, may be used as described in NIST 800-63B. AAL 2  
666 also permits any of the authentication methods of AAL 3. AAL 2 authentication requires  
667 cryptographic mechanisms that protect the primary Authenticator against compromise by the  
668 protocol threats for all threats at AAL 1 as well as verifier impersonation attacks. Approved  
669 cryptographic techniques are required for all Assertion protocols used at AAL 2 and above.<sup>15</sup>

---

<sup>14</sup> Identity Trust Frameworks for Digital Identity Systems also should set requirements for how the assurance for each credential will be documented in the metadata for the credential to support audit and compliance.

<sup>15</sup> Approved cryptographic techniques must be FIPS approved, NIST recommended, or otherwise compliant with Commonwealth IT Information Security Standard (SEC501):  
[http://www.vita.virginia.gov/uploadedFiles/VITA\\_Main\\_Public/Library/PSGs/HostedEnvironmentInformationSecurityStandardSEC52501.pdf](http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/HostedEnvironmentInformationSecurityStandardSEC52501.pdf)

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

678  
 679  
 680

**Figure 2. Assurance Model Crosswalk**

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

681  
 682  
 683  
 684

**Authenticator Assurance Levels**

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

690

**Authenticator Assurance Level 1**

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

699  
 700

701 Permitted Authenticator Types – AAL 1

702 AAL 1 permits the use of any of the following Authenticator types:

- 703 • Memorized Secret
- 704 • Look-up Secret
- 705 • Out of Band (Partially deprecated)
- 706 • Single Factor OTP Device
- 707 • Multi-Factor OTP Device
- 708 • Single Factor Cryptographic Device
- 709 • Multi-Factor Software Cryptographic Authenticator
- 710 • Multi-Factor Cryptographic Device

711

712 Authenticator and Verifier Requirements – AAL 1

713 Cryptographic Authenticators used at AAL 1 must use approved cryptography.

714 Verifiers operated by government agencies at AAL 1 must be validated to meet the requirements of [FIPS 140] Level 1.

715

716

717 Assertion Requirements – AAL 1

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

719

720

721 Reauthentication – AAL 1

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

723

724

725 Security Controls – AAL 1

726 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.

727

728

729

730 Records Retention – AAL 1

731 The CSP must comply with their respective records retention policies in accordance with whatever laws and/or regulations apply. Otherwise, no retention period is required.

732

733

734 Authenticator Assurance Level 2

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

736

737

738

739

740

741

742

743

## 744 Permitted Authenticator Types – AAL 2

745 At AAL 2, it is required to have (a) a multi-factor Authenticator, or (b) a combination of two  
746 single-factor Authenticators.

747

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

- 749 • Multi-Factor OTP Device
- 750 • Multi-Factor Software Cryptographic Authenticator
- 751 • Multi-Factor Cryptographic Device

752

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

- 756 • Look-up Secret
- 757 • Out of Band
- 758 • Single Factor OTP Device
- 759 • Single Factor Cryptographic Device

760

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

765

## 766 Authenticator and Verifier Requirements – AAL 2

767 Cryptographic Authenticators used at AAL 2 must use approved cryptography. Authenticators  
768 developed by government agencies must be validated to meet the requirements of [FIPS 140]  
769 Level 1. Verifiers operated by government agencies at AAL 2 must be validated to meet the  
770 requirements of [FIPS 140] Level 1.

771

## 772 Assertion Requirements – AAL 2

773 In order to be valid at AAL 2, authentication Assertions must meet the requirements defined in  
774 NIST SP 800-63C. Bearer Assertions may be used.

775

## 776 Reauthentication – AAL 2

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

781

## 782 Security Controls – AAL 2

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

786

787

## 788 Records Retention – AAL 2

789 CSPs must comply with their respective records retention policies in accordance with whatever  
790 laws and/or regulations apply to those entities. Otherwise, retention of records is required for  
791 seven years and 6 months.

792

## 793 Authenticator Assurance Level 3

794 AAL 3 is intended to provide the highest practical remote network authentication assurance.  
795 Authentication at AAL 3 is based on proof of possession of a key through a cryptographic  
796 protocol. AAL 3 is similar to AAL 2 except only “hard” cryptographic Authenticators are allowed.

797

## 798 Permitted Authenticator Types – AAL 3

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

800

1. Multi-Factor OTP Device

801

2. Multi-Factor Cryptographic Device

802

3. Single-Factor Cryptographic Device used in conjunction with Memorized Secret

803

## 804 Authenticator and Verifier Requirements – AAL 3

805 Multi-factor Authenticators used at AAL 3 must be hardware cryptographic modules validated  
806 at [FIPS 140] Level 2 or higher overall with at least [FIPS 140] Level 3 physical security. Single-  
807 factor cryptographic devices used at AAL 3 must be validated at [FIPS 140] Level 1 or higher  
808 overall with at least [FIPS 140] Level 3 physical security. These requirements may be met by  
809 using the PIV authentication key of a [FIPS 201] compliant Personal Identity Verification (PIV)  
810 Card. Verifiers at AAL 3 must be validated at [FIPS 140] Level 1 or higher.

811

## 812 Assertion Requirements – AAL 3

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

815

## 816 Reauthentication – AAL 3

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

821

## 822 Security Controls – AAL 3

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

826

## 827 Records Retention – AAL 3

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

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

832

<b>Requirement</b>	<b>AAL 1</b>	<b>AAL 2</b>	<b>AAL 3</b>
<b>Authenticator types</b>	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
<b>FIPS 140 verification</b>	Level 1 (Government agency verifiers)	Level 1 (Government agency Authenticators and verifiers)	Level 2 overall (MF Authenticators) Level 1 overall (Verifiers and SF Crypto Devices) Level 3 physical security (all Authenticators)
<b>Assertions</b>	Bearer or proof of possession	Bearer or proof of possession	Proof of possession only
<b>Reauthentication</b>	30 days	12 hours or 30 minutes inactivity; may use one authentication factor	12 hours or 15 minutes inactivity; must use both authentication factors
<b>Security Controls</b>	[SP 800-53] Low Baseline (or equivalent)	[SP 800-53] Moderate Baseline (or equivalent)	[SP 800-53] High Baseline (or equivalent)
<b>Records Retention</b>	Not required	7 years, 6 months	10 years, 6 months

833

## 834 Authenticator and Verifier Requirements

835

836 The minimum specifications defined in this document for Authenticators establish the following  
837 requirements for each Authenticator type. The technical requirements for each Authenticator  
838 type are the same regardless of the AAL.

839

### 840 Requirements by Authenticator Type

841

#### 842 Memorized Secrets

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

847

#### 848 Memorized Secret Authenticators

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

854

#### 855 Memorized Secret Verifiers

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

860

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

867

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

871

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

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

879

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

882

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

887

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

893

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

898

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

906

#### 907 Look-up Secrets

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

913

#### 914 Look-up Secret Authenticators

915 CSPs creating look-up secret Authenticators must use an approved random number generator  
916 to generate the list of secrets, and must deliver the Authenticator securely to the Subscriber.  
917 Look-up secrets must have at least 64 bits of entropy, or must have at least 20 bits of entropy if  
918 the number of failed authentication attempts is limited as described in Section 5.2.2.

919 If the Authenticator uses look-up secrets sequentially from a list, the Subscriber may dispose of  
920 used secrets, but only after a successful authentication.

## 921 Look-up Secret Verifiers

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

927

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

935

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

940

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

945

## 946 Out of Band

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

951

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

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

957

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

963

964 If the Authenticator responds directly to the verifier via the secondary communications  
965 channel, the verifier must send and the Authenticator must display information, such as a  
966 transaction ID or description, allowing the claimant to uniquely associate the authentication  
967 operation on the primary channel with the request on the secondary channel.  
968

969 Ability to receive email messages or other types of instant message does not generally prove  
970 the possession of a specific device, so they must not be used as out of band authentication  
971 methods.  
972

### 973 Out of Band Authenticators

974 The out of band Authenticator must establish an authenticated protected channel in order to  
975 retrieve the out of band secret or authentication request. This channel is considered to be out  
976 of band with respect to the primary communication channel, even if it terminates on the same  
977 device, provided the device does not leak information from one to the other.  
978

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

- 981 • Authentication to the verifier using approved cryptography. The key should be stored in  
982 the most secure storage available on the device (e.g., keychain storage, trusted platform  
983 module, or trusted execution environment if available).
- 984 • Authentication to a public mobile telephone network using a SIM card or equivalent that  
985 uniquely identifies the device  
986

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

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

- 993 • The Authenticator must display identifying information about the authentication  
994 transaction to the claimant prior to their approval.
- 995 • The secondary communication channel must be an authenticated protected channel.  
996

### 997 Out of Band Verifiers

998 Out of band verifiers must generate a random authentication secret with at least 20 bits of  
999 entropy using an approved random number generator. They then optionally signal the device  
1000 containing the Subscriber's Authenticator to indicate readiness to authenticate.  
1001

1002 If the out of band verification is to be made using a SMS message on a public mobile telephone  
1003 network, the verifier must verify that the pre-registered telephone number being used is  
1004 actually associated with a mobile network and not with a VoIP (or other software-based)  
1005 service. It then sends the SMS message to the pre-registered telephone number.  
1006

1007 Changing the pre-registered telephone number must not be possible without two-factor  
1008 authentication at the time of the change.

1009

1010 If out of band verification is to be made using a secure application (e.g., on a smart phone), the  
1011 verifier may send a push notification to that device. The verifier then waits for a establishment  
1012 of an authenticated protected channel and verifies the Authenticator's identifying key. The  
1013 verifier must not store the identifying key itself, but must use a verification method such as  
1014 hashing (using an approved hash function) or proof of possession of the identifying key to  
1015 uniquely identify the Authenticator. Once authenticated, the verifier transmits the  
1016 authentication secret to the Authenticator.

1017

1018 Depending on the type of out-of-band Authenticator, either:

- 1019 • The verifier waits for the secret to be returned on the primary communication channel.
- 1020 • The verifier waits for the secret, or some type of approval message, to be returned over  
1021 the secondary communication channel.

1022

1023 If approval is made over the secondary communication channel, the request to the verifier  
1024 must include a transaction identifier, such as a transaction ID or description, for display by the  
1025 verifier.

1026

1027 In collecting the authentication secret from the claimant, the verifier must use approved  
1028 encryption and must authenticate itself to the claimant. The authentication secret must be  
1029 considered invalid if not received within 5 minutes.

1030

1031 If the authentication secret has less than 64 bits of entropy, the verifier must implement a  
1032 throttling mechanism that effectively limits the number of failed authentication attempts an  
1033 attacker can make on the Subscriber's account as described in Section 5.2.2.

1034

1035 Single Factor OTP Device

1036 A single factor OTP device is a hardware device that supports the time-based generation of one-  
1037 time passwords. This includes software-based OTP generators installed on devices such as  
1038 mobile phones. This device has an embedded secret that is used as the seed for generation of  
1039 one-time passwords and does not require activation through a second factor. Authentication is  
1040 accomplished by using the Authenticator output (i.e., the one-time password) in an  
1041 authentication protocol, thereby proving possession and control of the device. A one-time  
1042 password device may, for example, display 6 characters at a time.

1043

1044 Single factor OTP devices are similar to look-up secret Authenticators with the exception that  
1045 the secrets are cryptographically generated by the Authenticator and verifier and compared by  
1046 the verifier. The secret is computed based on a nonce that may be time-based or from a  
1047 counter on the Authenticator and verifier.

1048

1049

1050

### 1051 Single Factor OTP Authenticators

1052 Single factor OTP Authenticators contain two persistent values. The first is a symmetric key that  
1053 persists for the lifetime of the device. The second is a nonce that is changed each time the  
1054 Authenticator is used or is based on a real-time clock.

1055

1056 The secret key must be of at least the minimum approved length as defined in the latest  
1057 revision of [SP 800-131A] (currently 112 bits). The nonce must be of sufficient length to ensure  
1058 that it is unique for each operation of the device over its lifetime.

1059

1060 The Authenticator output is obtained by using an approved block cipher or hash function to  
1061 combine the key and nonce in a secure manner. The Authenticator output may be truncated to  
1062 as few as 6 decimal digits (approximately 20 bits of entropy).

1063

1064 If the nonce used to generate the Authenticator output is based on a real-time clock, the nonce  
1065 must be changed at least once every 2 minutes. The OTP value associated with a given nonce  
1066 must be accepted only once.

1067

1068 If the Authenticator supplies its output via an electronic interface such as USB, it should require  
1069 a physical input (e.g., pressing a button on the device) to cause a one-time password to be  
1070 generated.

1071

### 1072 Single Factor OTP Verifiers

1073 Single factor OTP verifiers effectively duplicate the process of generating the OTP used by the  
1074 Authenticator. As such, the symmetric keys used by Authenticators are also present in the  
1075 verifier, and must be strongly protected against compromise.

1076

1077 In collecting the OTP from the claimant, the verifier must use approved encryption and must  
1078 authenticate itself to the claimant.

1079

1080 If the Authenticator output has less than 64 bits of entropy, the verifier must implement a  
1081 throttling mechanism that effectively limits the number of failed authentication attempts an  
1082 attacker can make on the Subscriber's account as described in Section 5.2.2.

1083

### 1084 Multi-Factor OTP Devices

1085 A multi-factor (MF) OTP device hardware device generates one-time passwords for use in  
1086 authentication and requires activation through a second factor of authentication. The second  
1087 factor of authentication may be achieved through some kind of integral entry pad, an integral  
1088 biometric (e.g., fingerprint) reader or a direct computer interface (e.g., USB port). The one-time  
1089 password is typically displayed on the device and manually input to the verifier, although direct  
1090 electronic output from the device as input to a computer is also allowed. For example, a one-  
1091 time password device may display 6 characters at a time. The MF OTP device is *something you*  
1092 *have*, and it may be activated by either *something you know* or *something you are*.

1093

1094

## 1095 Multi-Factor OTP Authenticators

1096 Multi-factor OTP Authenticators operate in a similar manner to single-factor OTP  
1097 Authenticators, except that they require the entry of either a memorized secret or use of a  
1098 biometric to obtain a password from the Authenticator. Each use of the Authenticator must  
1099 require the input of the additional factor.

1100  
1101 The Authenticator output must have at least 6 decimal digits (approximately 20 bits) of entropy.  
1102 The output must be generated by using an approved block cipher or hash function to combine a  
1103 symmetric key stored on a personal hardware device with a nonce to generate a one-time  
1104 password. The nonce may be based on the date and time or on a counter generated on the  
1105 device.

1106  
1107 Any memorized secret used by the Authenticator for activation must be at least 6 decimal digits  
1108 (approximately 20 bits) in length or of equivalent complexity. A biometric activation factor must  
1109 meet the requirements of Section 5.2.3, including limits on number of successive  
1110 authentication failures.

1111  
1112 The unencrypted key and activation secret or biometric sample (and any biometric data derived  
1113 from the biometric sample such as a probe produced through signal processing) must be  
1114 immediately erased from storage immediately after a password has been generated.

## 1115 Multi-Factor OTP Verifiers

1117 Multi-factor OTP verifiers effectively duplicate the process of generating the OTP used by the  
1118 Authenticator, but without the requirement that a second factor be provided. As such, the  
1119 symmetric keys used by Authenticators must be strongly protected against compromise.  
1120 In collecting the OTP from the claimant, the verifier must use approved encryption and must  
1121 authenticate itself to the claimant. Time-based one-time passwords must have a lifetime of less  
1122 than 2 minutes.

1123  
1124 If the Authenticator output or activation secret has less than 64 bits of entropy, the verifier  
1125 must implement a throttling mechanism that effectively limits the number of failed  
1126 authentication attempts an attacker can make on the Subscriber's account.

## 1127 Single Factor Cryptographic Devices

1129 A single-factor cryptographic device is a hardware device that performs cryptographic  
1130 operations on input provided to the device. This device does not require activation through a  
1131 second factor of authentication. This device uses embedded symmetric or asymmetric  
1132 cryptographic keys. Authentication is accomplished by proving possession of the device. The  
1133 Authenticator output is highly dependent on the specific cryptographic device and protocol, but  
1134 it is generally some type of signed message.

1135

1136

1137

1138

### 1139 Single Factor Cryptographic Device Authenticators

1140 Single-factor cryptographic device Authenticators encapsulate a secret key that is unique to the  
1141 device and must not be exportable (removed from the device). They operate by signing a  
1142 challenge nonce, usually presented through a direct computer interface such as a USB port.  
1143 The secret key must be of at least the minimum approved length as defined in the latest  
1144 revision of [SP 800-131A] (currently 112 bits). The challenge nonce must be at least 64 bits in  
1145 length. The Authenticator output is normally provided via a computer interface (usually the  
1146 same one from which the challenge value was received).

1147

1148 Single-factor cryptographic device Authenticators should require a physical input such as the  
1149 pressing of a button in order to operate. This provides defense against unintended operation of  
1150 the device, which might occur if the device to which it is connected is compromised.

1151

### 1152 Single Factor Cryptographic Device Verifiers

1153 Single-factor cryptographic device verifiers generate a challenge nonce, send it to the  
1154 corresponding Authenticator, and use the Authenticator output to verify possession of the  
1155 device. The Authenticator output is highly dependent on the specific cryptographic device and  
1156 protocol, but it is generally some type of signed message.

1157

1158 The verifier contains either symmetric or asymmetric public keys corresponding to each  
1159 Authenticator. While both types of keys must be protected against modification, symmetric  
1160 keys must additionally be strongly protected against unauthorized disclosure.

1161

1162 The challenge nonce must be at least 64 bits in length, and must either be unique over the  
1163 lifetime of the Authenticator or statistically unique (generated using an approved random  
1164 number generator).

1165

### 1166 Multi-Factor Cryptographic Software

1167 A multi-factor software cryptographic Authenticator is a cryptographic key is stored on disk or  
1168 some other "soft" media that requires activation through a second factor of authentication.  
1169 Authentication is accomplished by proving possession and control of the key. The Authenticator  
1170 output is highly dependent on the specific cryptographic protocol, but it is generally some type  
1171 of signed message. The MF software cryptographic Authenticator is *something you have*, and it  
1172 may be activated by either *something you know* or *something you are*.

1173

### 1174 Multi-Factor Cryptographic Software Authenticators

1175 Multi-factor software cryptographic Authenticators encapsulate a secret key that is unique to  
1176 the Authenticator and is accessible only through the input of an additional factor, either a  
1177 memorized secret or a biometric. The key should be stored in the most secure storage available  
1178 on the device (e.g., keychain storage, trusted platform module, or trusted execution  
1179 environment if available). Each authentication operation using the Authenticator must require  
1180 the input of the additional factor.

1181

1182 Any memorized secret used by the Authenticator for activation must be at least 6 decimal digits  
1183 (approximately 20 bits) in length or of equivalent complexity.

1184

1185 The unencrypted key and activation secret or biometric sample (and any biometric data derived  
1186 from the biometric sample such as a probe produced through signal processing) must be  
1187 immediately erased from storage immediately after an authentication transaction has taken  
1188 place.

1189

1190 Multi-Factor Cryptographic Software Verifiers

1191 The requirements for a multi-factor cryptographic software verifier are identical to those for a  
1192 multi-factor cryptographic device verifier, described in Section 5.1.8.2.

1193

1194 Multi-Factor Cryptographic Devices

1195 A multi-factor cryptographic device is a hardware device that contains a protected  
1196 cryptographic key that requires activation through a second authentication factor.

1197 Authentication is accomplished by proving possession of the device and control of the key. The  
1198 Authenticator output is highly dependent on the specific cryptographic device and protocol, but  
1199 it is generally some type of signed message. The MF Cryptographic device is *something you*  
1200 *have*, and it may be activated by either *something you know* or *something you are*.

1201

1202 Multi-Factor Cryptographic Device Authenticators

1203 Multi-factor cryptographic device Authenticators use tamper-resistant hardware to encapsulate  
1204 a secret key that is unique to the Authenticator and is accessible only through the input of an  
1205 additional factor, either a memorized secret or a biometric.

1206

1207 Each authentication operation using the Authenticator should require the input of the  
1208 additional factor. Input of the additional factor may be accomplished via either direct input on  
1209 the device or via a hardware connection (e.g., USB or smartcard).

1210

1211 Any memorized secret used by the Authenticator for activation must be at least 6 decimal digits  
1212 (approximately 20 bits) in length or of equivalent complexity. A biometric activation factor must  
1213 meet the requirements of Section 5.2.3, including limits on number of successive  
1214 authentication failures.

1215

1216 The unencrypted key and activation secret or biometric sample (and any biometric data derived  
1217 from the biometric sample such as a probe produced through signal processing) must be  
1218 immediately erased from storage immediately after an authentication transaction has taken  
1219 place.

1220

1221 Multi-Factor Cryptographic Device Verifiers

1222 Multi-factor cryptographic device verifiers generate a challenge nonce, send it to the  
1223 corresponding Authenticator, and use the Authenticator output to verify possession of the  
1224 device and activation factor. The Authenticator output is highly dependent on the specific  
1225 cryptographic device and protocol, but it is generally some type of signed message.

1226 The verifier contains either symmetric or asymmetric public keys corresponding to each  
1227 Authenticator. While both types of keys must be protected against modification, symmetric  
1228 keys must additionally be strongly protected against unauthorized disclosure.  
1229 The challenge nonce must be at least 64 bits in length, and must either be unique over the  
1230 lifetime of the Authenticator or statistically unique (generated using an approved random  
1231 number generator). The verification operation must use approved cryptography.

1232  
1233 General Authenticator Requirements

1234  
1235 Physical Authenticators

1236 CSPs must provide Subscriber instructions on how to appropriately protect the Authenticator  
1237 against theft or loss. The CSP must provide a mechanism to revoke or suspend the  
1238 Authenticator immediately upon notification from Subscriber that loss or theft of the  
1239 Authenticator is suspected.

1240  
1241 Rate Limiting (Throttling)

1242 When the Authenticator output or activation secret does not have sufficient entropy, the  
1243 verifier must implement controls to protect against online guessing attacks. Unless otherwise  
1244 specified in the description of a given Authenticator, the verifier must effectively limit online  
1245 attackers to 100 consecutive failed attempts on a single account in any 30-day period.

1246  
1247 Additional techniques may be used to prioritize authentication attempts that are likely to come  
1248 from the Subscriber over those that are more likely to come from an attacker:

- 1249 • Requiring the claimant to complete a Completely Automated Public Turing test to tell  
1250 Computers and Humans Apart (CAPTCHA) before attempting authentication
- 1251 • Requiring the claimant to wait for a short period of time (anything from 30 seconds to  
1252 an hour, depending on how close the system is to its maximum allowance for failed  
1253 attempts) before attempting Authentication following a failed attempt
- 1254 • Only accepting authentication requests from a white list of IP addresses at which the  
1255 Subscriber has been successfully authenticated before
- 1256 • Leveraging other risk-based or adaptive authentication techniques to identify user  
1257 behavior that falls within, or out of, typical norms.

1258  
1259 Since these measures often create user inconvenience, the verifier should allow a certain  
1260 number of failed authentication attempts before employing the above techniques.

1261 When the Subscriber successfully authenticates, the verifier should disregard any previous  
1262 failed attempts from the same IP address.

1263  
1264 Use of Biometrics

1265 For a variety of reasons, this document supports only limited use of biometrics for  
1266 authentication. These include:

- 1267 • Biometric False Match Rates (FMR) and False Non-Match Rates (FNMR) do not provide  
1268 confidence in the authentication of the Subscriber by themselves. In addition, FMR and  
1269 FNMR do not account for spoofing attacks.

- 1270 • Biometric matching is probabilistic, whereas the other authentication factors are
- 1271 deterministic.
- 1272 • Biometric template protection schemes provide a method for revoking biometric
- 1273 credentials that are comparable to other authentication factors (e.g., PKI certificates
- 1274 and passwords). However, the availability of such solutions is limited, and standards for
- 1275 testing these methods are under development.
- 1276 • Biometric characteristics do not constitute secrets. They can be obtained online or by
- 1277 taking a picture of someone with a camera phone (e.g. facial images) with or without
- 1278 their knowledge, lifted from through objects someone touches (e.g., latent fingerprints),
- 1279 or captured with high resolution images (e.g., iris patterns for blue eyes). While
- 1280 presentation attack detection (PAD) technologies such as liveness detection can
- 1281 mitigate the risk of these types of attacks, additional trust in the sensor is required to
- 1282 ensure that PAD is operating properly in accordance with the needs of the CSP and the
- 1283 Subscriber.

1284

1285 Therefore, the use of biometrics for authentication is supported, with the following  
1286 requirements and guidelines:

1287

- 1288 • Biometrics must be used with another authentication factor (something you know or
- 1289 something you have).
- 1290 • Testing of the biometric system to be deployed must demonstrate an equal error rate of
- 1291 **1 in 1000** or better with respect to matching performance. The biometric system must
- 1292 operate with a false match rate of **1 in 1000** or better.
- 1293 • When the biometric sensor and subsequent processing are not part of an integral unit
- 1294 that resists replacement of the sensor, the sensor must demonstrate that it is a certified
- 1295 or qualified sensor meeting these requirements by authenticating itself to the
- 1296 processing element.
- 1297 • Testing of the biometric system to be deployed must demonstrate at least 90%
- 1298 resistance to presentation attacks for each relevant attack type (aka species), where
- 1299 resistance is defined as the number of thwarted presentation attacks divided by the
- 1300 number of trial presentation attacks. The biometric system must implement
- 1301 presentation attack protection (PAD).
- 1302 • The biometric system must allow no more than 10 consecutive failed authentication
- 1303 attempts. Once that limit has been reached, the claimant must be required to use a
- 1304 different Authenticator or to activate their Authenticator with a different factor such as
- 1305 a memorized secret.
- 1306 • Biometric matching should be performed locally on claimant's device or may be
- 1307 performed at a central verifier.

1308

1309 If matching is performed centrally:

- 1310 • Use of the biometric must be bound tightly to a single, specific device that is identified
- 1311 using approved cryptography.
- 1312 • Biometric revocation must be implemented.

- 1313
- 1314
- 1315
- 1316
- 1317
- An authenticated protected channel between sensor and central verifier must be established, and the sensor authenticated, **prior** to capturing the biometric sample from the claimant.
  - All transmission of biometrics must be over the authenticated protected channel.

1318 Biometric samples collected in the authentication process may be used to train matching  
1319 algorithms or, with user consent, for other research purposes. Biometric samples (and any  
1320 biometric data derived from the biometric sample such as a probe produced through signal  
1321 processing) must be immediately erased from storage immediately after a password has been  
1322 generated.

1323

1324 Biometrics are also used in some cases to prevent repudiation of registration and to verify that  
1325 the same individual participates in all phases of the registration process as described in NIST SP  
1326 800-63A.

#### 1327 Attestation

1329 Authenticators that are directly connected to or embedded in endpoints may convey  
1330 attestation information such as the provenance or health and integrity of the Authenticator  
1331 (and possibly the endpoint as well) to the verifier as part of the authentication protocol. If this  
1332 attestation is signed, the verifier should validate its signature. This information may be used as  
1333 part of a risk-based authentication decision.

1334

1335 When federated authentication is being performed as described in NIST SP 800-63C, the verifier  
1336 should include any such attestation information in the Assertion it provides to the relying party.

1337

1338

## 1339 Authenticator Lifecycle Management

1340

1341 During the lifecycle of an Authenticator bound to a Subscriber's identity, a number of events  
1342 may occur that affect the use of that Authenticator. These events include binding, loss, theft,  
1343 unauthorized duplication, expiration, and revocation. This section describes the actions that  
1344 must be taken in response to those events.

1345

### 1346 Authenticator binding

1347 Authenticators may be provided by a CSP as part of a process such as enrollment; in other  
1348 cases, the Subscriber may provide their own, such as software or hardware cryptographic  
1349 modules. For this reason, we refer to the *binding* of an Authenticator rather than the issuance,  
1350 but this does not exclude the possibility that an Authenticator is issued as well.

1351

1352 Throughout the online identity lifecycle, CSPs must maintain a record of all Authenticators that  
1353 are or have been associated with the identity. It must also maintain the information required  
1354 for throttling authentication attempts when required.

1355

1356 The record created by the CSP must contain the date and time the Authenticator was bound to  
1357 the account and should include information about the binding, such as the IP address or other  
1358 device identifier associated with the enrollment. It should also contain information about  
1359 unsuccessful authentications attempted with the Authenticator.

1360

### 1361 Registration

1362 The following requirements apply when an Authenticator is bound to an identity as a result of a  
1363 successful identity proofing transaction, as described in NIST SP 800-63A.

1364

1365 At IAL 2, the CSP must bind at least one, and should bind at least two, Authenticators to the  
1366 Subscriber's online identity. Binding of multiple Authenticators is preferred in order to recover  
1367 from loss or theft of their primary Authenticator. While at IAL 1 all identifying information is  
1368 self-asserted, creation of online material or an online reputation makes it undesirable to lose  
1369 control of an account as result of the loss of an Authenticator. The second Authenticator makes  
1370 it possible to securely recover from that situation.

1371

1372 At IAL 2 and above, identifying information is associated with the online identity and the  
1373 Subscriber has undergone an identity proofing process as described in NIST SP 800-63A.

1374 Authenticators at the same AAL as the desired IAL must be bound to the account. For example,  
1375 if the Subscriber has successfully completed proofing at IAL 2, AAL 2 or 3 Authenticators are  
1376 appropriate to bind to the IAL 2 identity. As above, the availability of additional Authenticators  
1377 provides backup methods of authentication if an Authenticator is lost or stolen.

1378

1379 Registration and binding may be broken up into a number of separate physical encounters or  
1380 electronic transactions. (Two electronic transactions are considered to be separate if they are  
1381 not part of the same protected session.)

1382 In these cases, the following methods must be used to ensure that the same party acts as  
1383 applicant throughout the processes:

1384 1. For remote transactions:

1385 a. The applicant must identify himself/herself in each new transaction by  
1386 presenting a temporary secret which was established during a prior transaction  
1387 or encounter, or sent to the Applicant's phone number, email address, or postal  
1388 address of record.

1389 b. Permanent secrets must only be issued to the Applicant within a protected  
1390 session.

1391 2. For physical transactions:

1392 a. The applicant must identify himself/herself in person by either using a secret as  
1393 described above, or through the use of a biometric that was recorded during a  
1394 prior encounter.

1395 b. Temporary secrets must not be reused.

1396 c. If the CSP issues permanent secrets during a physical transaction, then they must  
1397 be loaded locally onto a physical device that is issued in person to the applicant  
1398 or delivered in a manner that confirms the address of record.

1399

1400 Post-Registration Binding

1401 Following registration, binding an additional Authenticator to an account requires the use of an  
1402 existing Authenticator of the same type (or types). For example, binding a new single-factor  
1403 OTP device requires the Subscriber to authenticate with another *something you have*  
1404 authentication factor. If the account has only one authentication factor bound to it (which is  
1405 possible only at IAL 1/AAL 1), an additional Authenticator of the same factor may be bound to  
1406 it.

1407

1408 Binding an additional Authenticator must require the use of two different authentication  
1409 factors, except as provided below.

1410

1411 If the Subscriber has only one of the two authentication factors, they must repeat the identity  
1412 proofing process, using the remaining authentication and should verify knowledge of some  
1413 information collected during the proofing process to bind to the existing identity. In order to  
1414 reestablish authentication factors at IAL 3, they must verify the biometric collected during the  
1415 proofing process.

1416

1417 Binding Identity to a Subscriber Provided Authenticator

1418 In some instances, a claimant may already possess Authenticators at a suitable AAL without  
1419 having been proofed at the equivalent IAL. For example, a user may have a two-factor  
1420 Authenticator from a social network provider, considered AAL2 and IAL1, and would like to use  
1421 those credentials at a relying party that requires IAL2.

1422

1423 The following requirements apply when a claimant chooses to increase IAL in order to bind to a  
1424 suitable Authenticator they already have.

1425 1. The CSP may accept an existing Authenticator at or above the desired IAL

- 1426 2. The CSP must require the user to authenticate using their existing Authenticator  
1427 3. The CSP must execute all required identity proofing processes for the desired IAL  
1428 4. If the user successfully completes identity proofing, the CSP may issue an enrollment  
1429 code (temporary secret) that confirms address of record as per [800-63-A, Section 5.3.1,](#)  
1430 [Address Confirmation Requirements](#), **OR** may request the claimant to register their own  
1431 Authenticator by proving proof of possession (for example, activating a private key by  
1432 physically touching the token)

1433

1434 **Renewal**

1435 The CSP should bind an updated Authenticator an appropriate amount of time in advance of an  
1436 existing Authenticator's expiration. The process for this should conform closely to the initial  
1437 Authenticator issuance process (e.g., confirming address of record, etc.). Following successful  
1438 use of the new Authenticator, the CSP may revoke the Authenticator that it is replacing.

1439

1440 **Loss, Theft, and Unauthorized Duplication**

1441 Loss, theft, and unauthorized duplication of an Authenticator are handled similarly, because in  
1442 most cases one must assume that a lost Authenticator has potentially been stolen or recovered  
1443 by someone that is not the legitimate claimant of the Authenticator. One notable exception is  
1444 when a memorized secret is forgotten without other indication of having been compromised  
1445 (duplicated by an attacker).

1446

1447 To facilitate secure reporting of loss or theft of an Authenticator, the CSP should provide the  
1448 Subscriber a method to authenticate to the CSP using a backup Authenticator; either a  
1449 memorized secret or a physical Authenticator may be used for this purpose (only one  
1450 authentication factor is required for this purpose). Alternatively, the Subscriber may establish  
1451 an authenticated protected channel to the CSP and verify information collected during the  
1452 proofing process. Alternatively, the CSP may verify an address of record (email, telephone, or  
1453 postal) and suspend Authenticator(s) reported to have been compromised. The suspension  
1454 must be reversible if the Subscriber successfully authenticates to the CSP and requests  
1455 reactivation of an Authenticator suspended in this manner.

1456

1457 **Expiration**

1458 CSP's should issue Authenticators that expire. When an Authenticator expires, it must not be  
1459 usable for authentication. When an authentication is attempted, the CSP should give an  
1460 indication to the Subscriber that the authentication failure is due to expiration rather than  
1461 some other cause.

1462

1463 The CSP must require Subscribers to surrender any physical Authenticator containing trustable  
1464 Attributes as soon as practical after expiration or after receipt of a renewed Authenticator.

1465

1466 **Revocation**

1467 CSPs must revoke the binding of Authenticators promptly when an online identity ceases to  
1468 exist or when requested by the Subscriber.

1469

## 1470 Privacy and Security

1471

1472 The minimum specifications established in this document for privacy and security in the use of  
 1473 person information for Electronic Authentication apply the Fair Information Practice Principles  
 1474 (FIPPs).<sup>16</sup> The FIPPs have been endorsed by the National Strategy for Trusted Identities in  
 1475 Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.<sup>17</sup>

1476

1477 The minimum specifications also adhere to the Identity Ecosystem Framework (IDEF) Baseline  
 1478 Functional Requirements (v.1.0) for privacy and security, adopted by the Identity Ecosystem  
 1479 Steering Group (IDESG) in October 2015 (**Appendix 2**).

1480

1481 The minimum specifications apply the following FIPPs:

- 1482 • Transparency: RAs and CSPs should be transparent and provide notice to Applicants  
 1483 regarding collection, use, dissemination, and maintenance of person information required  
 1484 during the registration, identity proofing and verification processes.
- 1485 • Individual Participation: RAs and CSPs should involve the Applicant in the process of using  
 1486 person information and, to the extent practicable, seek consent for the collection, use,  
 1487 dissemination, and maintenance of that information. RAs and CSPs also should provide  
 1488 mechanisms for appropriate access, correction, and redress of person information.
- 1489 • Purpose Specification: RAs and CSPs should specifically articulate the authority that permits  
 1490 the collection of person information and specifically articulate the purpose or purposes for  
 1491 which the information is intended to be used.
- 1492 • Data Minimization: RAs and CSPs should collect only the person information directly  
 1493 relevant and necessary to accomplish the registration and related processes, and only retain  
 1494 that information for as long as necessary to fulfill the specified purpose.
- 1495 • Use Limitation/Minimal Disclosure: RAs and CSPs should use person information solely for  
 1496 the purpose specified in the notice. Disclosure or sharing that information should be limited  
 1497 to the specific purpose for which the information was collected.
- 1498 • Data Quality and Integrity: RAs and CSPs should, to the extent practicable, ensure that  
 1499 person information is accurate, relevant, timely, and complete.
- 1500 • Security: RAs and CSPs should protect personal information through appropriate security  
 1501 safeguards against risks such as loss, unauthorized access or use, destruction, modification,  
 1502 or unintended or inappropriate disclosure.
- 1503 • Accountability and Auditing: RAs and CSPs should be accountable for complying with these  
 1504 principles, providing training to all employees and contractors who use person information,  
 1505 and auditing the actual use of person information to demonstrate compliance with these  
 1506 principles and all applicable privacy protection requirements.

---

<sup>16</sup> The term “person information” refers to protected data for person entities, governed by Applicable Law. This includes Personally Identifiable Information (PII), Protected Health Information (PHI), Federal Tax Information (FTI), Protected Education Records, and related categories. Specific requirements for the privacy and security of person information should be defined by the Identity Trust Framework for the Digital Identity System.

<sup>17</sup> 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>.

## 1507 Appendix 1. IMSAC Charter

1508

1509

**COMMONWEALTH OF VIRGINIA**

1510

**IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL**

1511

**CHARTER**

1512

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

1514

1515 The Identity Management Standards Advisory Council (the Advisory Council) advises the  
1516 Secretary of Technology on the adoption of identity management standards and the creation of  
1517 guidance documents pursuant to § 2.2-436.

1518

1519 The Advisory Council recommends to the Secretary of Technology guidance documents relating  
1520 to (i) nationally recognized technical and data standards regarding the verification and  
1521 authentication of identity in digital and online transactions; (ii) the minimum specifications and  
1522 standards that should be included in an Identity Trust Framework, as defined in § 59.1-550, so  
1523 as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-  
1524 550 et seq.); and (iii) any other related data standards or specifications concerning reliance by  
1525 third parties on identity credentials, as defined in § 59.1-550.

1526

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

1528

1529 The Advisory Council's membership and governance structure is as follows:

1530

1531 1. The Advisory Council consists of seven members, to be appointed by the Governor, with  
1532 expertise in electronic identity management and information technology. Members include  
1533 a representative of the Department of Motor Vehicles, a representative of the Virginia  
1534 Information Technologies Agency, and five representatives of the business community with  
1535 appropriate experience and expertise. In addition to the seven appointed members, the  
1536 Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex  
1537 officio member of the Advisory Council.

1537

1538 2. The Advisory Council designates one of its members as chairman.

1539

1540 3. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure  
1541 of the Governor, and may be reappointed.

1542

1543 4. Members serve without compensation but may be reimbursed for all reasonable and  
1544 necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.

1545

1546 5. Staff to the Advisory Council is provided by the Office of the Secretary of Technology.

1547

1548

1549 The formation, membership and governance structure for the Advisory Council has been  
1550 codified pursuant to § 2.2-437.A, § 2.2-437.B, as cited above in this charter.

1551

1552 The statutory authority and requirements for public notice and comment periods for guidance  
1553 documents have been established pursuant to § 2.2-437.C, as follows:

1554

1555 C. Proposed guidance documents and general opportunity for oral or written submittals as to  
1556 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published  
1557 in the Virginia Register of Regulations as a general notice following the processes and  
1558 procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§  
1559 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written  
1560 comments following the posting and publication and shall hold at least one meeting dedicated  
1561 to the receipt of oral comment no less than 15 days after the posting and publication. The  
1562 Advisory Council shall also develop methods for the identification and notification of interested  
1563 parties and specific means of seeking input from interested persons and groups. The Advisory  
1564 Council shall send a copy of such notices, comments, and other background material relative to  
1565 the development of the recommended guidance documents to the Joint Commission on  
1566 Administrative Rules.

1567

1568

1569 This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the  
1570 minutes of the meeting and related IMSAC documents, visit:  
1571 <https://vita.virginia.gov/About/default.aspx?id=6442474173>

1572 Appendix 2. IDESG Identity Ecosystem Framework (IDEF) Baseline  
1573 Functional Requirements (v.1.0) for Privacy and Security

1574

1575 PRIVACY-1. DATA MINIMIZATION

1576 Entities MUST limit the collection, use, transmission and storage of personal information to the  
1577 minimum necessary to fulfill that transaction's purpose and related legal requirements. Entities  
1578 providing claims or Attributes MUST not provide any more personal information than what is  
1579 requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to  
1580 accommodate information requests of variable granularity, to support data minimization.

1581

1582 PRIVACY-2. PURPOSE LIMITATION

1583 Entities MUST limit the use of personal information that is collected, used, transmitted, or  
1584 stored to the specified purposes of that transaction. Persistent records of contracts, assurances,  
1585 consent, or legal authority MUST be established by entities collecting, generating, using,  
1586 transmitting, or storing personal information, so that the information, consistently is used in  
1587 the same manner originally specified and permitted.

1588

1589 PRIVACY-3. ATTRIBUTE MINIMIZATION

1590 Entities requesting Attributes MUST evaluate the need to collect specific Attributes in a  
1591 transaction, as opposed to claims regarding those Attributes. Wherever feasible, entities MUST  
1592 collect, generate, use, transmit, and store claims about USERS rather than Attributes. Wherever  
1593 feasible, Attributes MUST be transmitted as claims, and transmitted credentials and identities  
1594 MUST be bound to claims instead of actual Attribute values.

1595

1596 PRIVACY-4. CREDENTIAL LIMITATION

1597 Entities MUST not request USERS' credentials unless necessary for the transaction and then  
1598 only as appropriate to the risk associated with the transaction or to the risks to the parties  
1599 associated with the transaction.

1600

1601 PRIVACY-5. DATA AGGREGATION RISK

1602 Entities MUST assess the privacy risk of aggregating personal information, in systems and  
1603 processes where it is collected, generated, used, transmitted, or stored, and wherever feasible,  
1604 MUST design and operate their systems and processes to minimize that risk. Entities MUST  
1605 assess and limit linkages of personal information across multiple transactions without the  
1606 USER's explicit consent.

1607

1608 PRIVACY-6. USAGE notICE

1609 Entities MUST provide concise, meaningful, and timely communication to USERS describing how  
1610 they collect, generate, use, transmit, and store personal information.

1611

1612 PRIVACY-7. USER DATA CONTROL

1613 Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete  
1614 personal information.

## 1615 PRIVACY-8. THIRD-PARTY LIMITATIONS

1616 Wherever USERS make choices regarding the treatment of their personal information, those  
1617 choices MUST be communicated effectively by that entity to any THIRD-PARTIES to which it  
1618 transmits the personal information.

1619

## 1620 PRIVACY-9. USER notice OF CHANGES

1621 Entities MUST, upon any material changes to a service or process that affects the prior or  
1622 ongoing collection, generation, use, transmission, or storage of USERS' personal information,  
1623 notify those USERS, and provide them with compensating controls designed to mitigate privacy  
1624 risks that may arise from those changes, which may include seeking express affirmative consent  
1625 of USERS in accordance with relevant law or regulation.

1626

## 1627 PRIVACY-10. USER OPTION TO DECLINE

1628 USERS MUST have the opportunity to decline registration; decline credential provisioning;  
1629 decline the presentation of their credentials; and decline release of their Attributes or claims.

1630

## 1631 PRIVACY-11. OPTIONAL INFORMATION

1632 Entities MUST clearly indicate to USERS what personal information is mandatory and what  
1633 information is optional prior to the transaction.

1634

## 1635 PRIVACY-12. ANONYMITY

1636 Wherever feasible, entities MUST utilize identity systems and processes that enable  
1637 transactions that are anonymous, anonymous with validated Attributes, pseudonymous, or  
1638 where appropriate, uniquely identified. Where applicable to such transactions, entities  
1639 employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES  
1640 collecting USER personal information. Organizations MUST request individuals' credentials only  
1641 when necessary for the transaction and then only as appropriate to the risk associated with the  
1642 transaction or only as appropriate to the risks to the parties associated with the transaction.

1643

## 1644 PRIVACY-13. CONTROLS PROPORTIONATE TO RISK

1645 Controls on the processing or use of USERS' personal information MUST be commensurate with  
1646 the degree of risk of that processing or use. A privacy risk analysis MUST be conducted by  
1647 entities who conduct digital identity management functions, to establish what risks those  
1648 functions pose to USERS' privacy.

1649

## 1650 PRIVACY-14. DATA RETENTION AND DISPOSAL

1651 Entities MUST limit the retention of personal information to the time necessary for providing  
1652 and administering the functions and services to USERS for which the information was collected,  
1653 except as otherwise required by law or regulation. When no longer needed, personal  
1654 information MUST be securely disposed of in a manner aligning with appropriate industry  
1655 standards and/or legal requirements.

1656

## 1657 PRIVACY-15. ATTRIBUTE SEGREGATION

1658 Wherever feasible, identifier data MUST be segregated from Attribute data.

## 1659 SECURE-1. SECURITY PRACTICES

1660 Entities MUST apply appropriate and industry-accepted information security STANDARDS,  
1661 guidelines, and practices to the systems that support their identity functions and services.

1662

## 1663 SECURE-2. DATA INTEGRITY

1664 Entities MUST implement industry-accepted practices to protect the confidentiality and  
1665 integrity of identity data—including authentication data and Attribute values—during the  
1666 execution of all digital identity management functions, and across the entire data lifecycle  
1667 (collection through destruction).

1668

## 1669 SECURE-3. CREDENTIAL REPRODUCTION

1670 Entities that issue or manage credentials and tokens MUST implement industry-accepted  
1671 processes to protect against their unauthorized disclosure and reproduction.

1672

## 1673 SECURE-4. CREDENTIAL PROTECTION

1674 Entities that issue or manage credentials and tokens MUST implement industry-accepted data  
1675 integrity practices to enable individuals and other entities to verify the source of credential and  
1676 token data.

1677

## 1678 SECURE-5. CREDENTIAL ISSUANCE

1679 Entities that issue or manage credentials and tokens MUST do so in a manner designed to  
1680 assure that they are granted to the appropriate and intended USER(s) only. Where registration  
1681 and credential issuance are executed by separate entities, procedures for ensuring accurate  
1682 exchange of registration and issuance information that are commensurate with the stated  
1683 assurance level MUST be included in business agreements and operating policies.

1684

## 1685 SECURE-6. CREDENTIAL UNIQUENESS

1686 Entities that issue or manage credentials MUST ensure that each account to credential pairing is  
1687 uniquely identifiable within its namespace for authentication purposes.

1688

## 1689 SECURE-7. TOKEN CONTROL

1690 Entities that authenticate a USER MUST employ industry-accepted secure authentication  
1691 protocols to demonstrate the USER's control of a valid token.

1692

## 1693 SECURE-8. MULTIFACTOR AUTHENTICATION

1694 Entities that authenticate a USER MUST offer authentication mechanisms which augment or are  
1695 alternatives to a password.

1696

## 1697 SECURE-9. AUTHENTICATION RISK ASSESSMENT

1698 Entities MUST have a risk assessment process in place for the selection of authentication  
1699 mechanisms and supporting processes.

1700

1701

1702

## 1703 SECURE-10. UPTIME

1704 Entities that provide and conduct digital identity management functions MUST have established  
1705 policies and processes in place to maintain their stated assurances for availability of their  
1706 services.

1707

## 1708 SECURE-11. KEY MANAGEMENT

1709 Entities that use cryptographic solutions as part of identity management MUST implement key  
1710 management policies and processes that are consistent with industry-accepted practices.

1711

## 1712 SECURE-12. RECOVERY AND REISSUANCE

1713 Entities that issue credentials and tokens MUST implement methods for reissuance, updating,  
1714 and recovery of credentials and tokens that preserve the security and assurance of the original  
1715 registration and credentialing operations.

1716

## 1717 SECURE-13. REVOCATION

1718 Entities that issue credentials or tokens MUST have processes and procedures in place to  
1719 invalidate credentials and tokens.

1720

## 1721 SECURE-14. SECURITY LOGS

1722 Entities conducting digital identity management functions MUST log their transactions and  
1723 security events, in a manner that supports system audits and, where necessary, security  
1724 investigations and regulatory requirements. Timestamp synchronization and detail of logs  
1725 MUST be appropriate to the level of risk associated with the environment and transactions.

1726

## 1727 SECURE-15. SECURITY AUDITS

1728 Entities MUST conduct regular audits of their compliance with their own information security  
1729 policies and procedures, and any additional requirements of law, including a review of their  
1730 logs, incident reports and credential loss occurrences, and MUST periodically review the  
1731 effectiveness of their policies and procedures in light of that data.