

# COMMONWEALTH OF VIRGINIA



## IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

**GUIDANCE DOCUMENT**  
**Electronic Authentication**

## 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
8	Alignment Comparison .....	28

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.

37

DRAFT

## 38 4 Statutory Authority

---

39

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

44

45 **Governing Statutes:**

46

47 **Secretary of Technology**

48 § 2.2-225. Position established; agencies for which responsible; additional powers

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

50

51 **Identity Management Standards Advisory Council**

52 § 2.2-437. Identity Management Standards Advisory Council

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

54

55 **Commonwealth Identity Management Standards**

56 § 2.2-436. Approval of electronic identity standards

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

58

59 **Electronic Identity Management Act**

60 Chapter 50. Electronic Identity Management Act

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

62

63

64

65

66

67

## 68 5 Definitions

---

69  
70 Terms used in this document comply with definitions in the Public Review version of the  
71 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3),  
72 and align with adopted definitions in § 59.1-550, *Code of Virginia* (COV), and the  
73 Commonwealth of Virginia's ITRM Glossary (ITRM Glossary).<sup>1</sup>  
74

75 Active Attack: An online attack where the attacker transmits data to the claimant, credential  
76 service provider, verifier, or relying Participant. Examples of active attacks include man-in-the-  
77 middle, impersonation, and session hijacking.  
78

79 Address of Record: The official location where an individual can be found. The address of record  
80 always includes the residential street address of an individual and may also include the mailing  
81 address of the individual. In very limited circumstances, an Army Post Office box number, Fleet  
82 Post Office box number or the street address of next of kin or of another contact individual can  
83 be used when a residential street address for the individual is not available.  
84

85 Approved: Federal Information Processing Standard (FIPS) approved or NIST recommended. An  
86 algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2)  
87 adopted in a FIPS or NIST Recommendation.  
88

89 Applicable Law: Laws, statutes, regulations, and rules of the jurisdiction in which the members  
90 of an Identity Trust Framework operates.  
91

92 Applicant: A Participant undergoing the processes of Registration and Identity Proofing.  
93

94 Assertion: A statement from a verifier to a relying Participant (RP) that contains identity  
95 information about a Subscriber. Assertions may also contain verified attributes.  
96

97 Assertion Reference: A data object, created in conjunction with an Assertion, which identifies  
98 the verifier and includes a pointer to the full Assertion held by the verifier.  
99

100 Assurance: In the context of [OMB M-04-04]<sup>2</sup> and this document, assurance is defined as 1) the  
101 degree of confidence in the vetting process used to establish the identity of an individual to  
102 whom the credential was issued, and 2) the degree of confidence that the individual who uses  
103 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>.

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

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

149

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

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

152

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

157

158 Bit: A binary digit: 0 or 1.

159

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

163

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

165

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

168

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

177

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

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

184

185 Claimed Identity: A declaration by the applicant of their current Personal Name, date of birth  
186 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>.

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

191

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

194

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

200

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

205

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

212

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

218

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

223

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

225

---

<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>.

226 Data Integrity: The property that data has not been altered by an unauthorized entity.  
227

228 Derived Credential: A credential issued based on proof of possession and control of an  
229 authenticator associated with a previously issued credential, so as not to duplicate the Identity  
230 Proofing process.  
231

232 Digital Identity System: An Information System that supports Electronic Authentication and the  
233 management of a person's Identity in a digital environment. [Referenced in § 59.1-550, COV]  
234

235 Digital Signature: An asymmetric key operation where the private key is used to digitally sign  
236 data and the public key is used to verify the signature. Digital signatures provide authenticity  
237 protection, integrity protection, and non-repudiation.  
238

239 Eavesdropping Attack: An attack in which an attacker listens passively to the authentication  
240 protocol to capture information which can be used in a subsequent active attack to  
241 masquerade as the claimant.  
242

243 Electronic Authentication: The process of establishing confidence in user identities  
244 electronically presented to an Information System.  
245

246 Entropy: A measure of the amount of uncertainty that an attacker faces to determine the value  
247 of a secret. Entropy is usually stated in bits.  
248

249 Extensible Mark-up Language (XML): Extensible Markup Language, abbreviated XML, describes  
250 a class of data objects called XML documents and partially describes the behavior of computer  
251 programs which process them.  
252

253 Federal Bridge Certification Authority (FBCA): The FBCA is the entity operated by the Federal  
254 Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI  
255 Policy Authority to create, sign, and issue public key certificates to Principal CAs.  
256

257 Federal Information Security Management Act (FISMA): Title III of the E-Government Act  
258 requiring each federal agency to develop, document, and implement an agency-wide program  
259 to provide information security for the information and Information Systems that support the  
260 operations and assets of the agency, including those provided or managed by another agency,  
261 contractor, or other source.  
262

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

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

270

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

274

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

277

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

279 Approved hash functions satisfy the following properties:

280

- (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and

281

- (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.

282

283

284

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

289

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

291

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

294

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

297

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

301

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

309

---

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

310 Information System: A discrete set of information resources organized for the collection,  
311 processing, maintenance, use, sharing, dissemination, or disposition of information. [NIST  
312 Interagency/Internal Report (IR) 7298 r. 2]  
313

314 Kerberos: A widely used authentication protocol developed at MIT. In “classic” Kerberos, users  
315 share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to  
316 communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by  
317 the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords,  
318 the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who  
319 capture the initial user-to- KDC exchange. Longer password length and complexity provide  
320 some mitigation to this vulnerability, although sufficiently long passwords tend to be  
321 cumbersome for users.  
322

323 Knowledge Based Authentication: Authentication of an individual based on knowledge of  
324 information associated with his or her Claimed Identity in public databases. Knowledge of such  
325 information is considered to be private rather than secret, because it may be used in contexts  
326 other than authentication to a verifier, thereby reducing the overall assurance associated with  
327 the authentication process.  
328

329 Man-in-the-Middle Attack (MitM): An attack on the authentication protocol run in which the  
330 attacker positions himself or herself in between the claimant and verifier so that he can  
331 intercept and alter data traveling between them.  
332

333 Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric  
334 key to detect both accidental and intentional modifications of the data. MACs provide  
335 authenticity and integrity protection, but not non-repudiation protection.  
336

337 Multi-Factor: A characteristic of an authentication system or an authenticator that uses more  
338 than one authentication factor. The three types of authentication factors are something you  
339 know, something you have, and something you are.  
340

341 Network: An open communications medium, typically the Internet, that is used to transport  
342 messages between the claimant and other Participants. Unless otherwise stated, no  
343 assumptions are made about the security of the network; it is assumed to be open and subject  
344 to active (i.e., impersonation, man-in-the-middle, session hijacking) and passive (i.e.,  
345 eavesdropping) attack at any point between the Participants (e.g., claimant, verifier, CSP or RP).  
346

347 Nonce: A value used in security protocols that is never repeated with the same key. For  
348 example, nonces used as challenges in challenge-response authentication protocols must not  
349 be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay  
350 attack. Using a nonce as a challenge is a different requirement than a random challenge,  
351 because a nonce is not necessarily unpredictable.  
352

353 Off-line Attack: An attack where the attacker obtains some data (typically by eavesdropping on  
354 an authentication protocol run or by penetrating a system and stealing security files) that  
355 he/she is able to analyze in a system of his/her own choosing.  
356

357 Online Attack: An attack against an authentication protocol where the attacker either assumes  
358 the role of a claimant with a genuine verifier or actively alters the authentication channel.  
359

360 Online Guessing Attack: An attack in which an attacker performs repeated logon trials by  
361 guessing possible values of the authenticator output.  
362

363 Operational Authority: Entity responsible for operations, maintenance, management, and  
364 related functions of an Identity Trust Framework.  
365

366 Participant Requirements: A set of rules and policies in an Identity Trust Framework addressing  
367 identity, security, privacy, technology, and enforcement, which are assigned to each member  
368 type in a Digital Identity System. Member types include Registration Authorities (RAs), Identity  
369 Providers (IdPs), Credential Service Providers (CSPs), Verifiers, and Relying Parties (RPs).  
370 [§ 59.1-550, COV]  
371

372 Passive Attack: An attack against an authentication protocol where the attacker intercepts data  
373 traveling along the network between the claimant and verifier, but does not alter the data (i.e.,  
374 eavesdropping).  
375

376 Password: A secret that a claimant memorizes and uses to authenticate his or her identity.  
377 Passwords are typically character strings.  
378

379 Personal Identification Number (PIN): A password consisting only of decimal digits.  
380

381 Personal Identity Verification (PIV) Card: Defined by [FIPS 201] as a physical artifact (e.g.,  
382 identity card, smart card) issued to federal employees and contractors that contains stored  
383 credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that  
384 the Claimed Identity of the cardholder can be verified against the stored credentials by another  
385 person (human readable and verifiable) or an automated process (computer readable and  
386 verifiable).  
387

388 Personally Identifiable Information (PII): As defined by OMB Circular A-130, Personally  
389 Identifiable Information means information that can be used to distinguish or trace an  
390 individual's identity, either alone or when combined with other information that is linked or  
391 linkable to a specific individual.  
392

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

397 Phishing: An attack in which the Subscriber is lured (usually through an email) to interact with a  
398 counterfeit verifier/RP and tricked into revealing information that can be used to masquerade  
399 as that Subscriber to the real verifier/RP.  
400

401 Physical In-Person: Method of Identity Proofing in which Applicants are required to physically  
402 present themselves and identity evidence to a representative of the Registration Authority or  
403 Identity Trust Framework. [NIST SP 800-63-2]  
404

405 Possession and control of an authenticator: The ability to activate and use the authenticator in  
406 an authentication protocol.  
407

408 Practice Statement: A formal statement of the practices followed by the Participants to an  
409 authentication process (i.e., RA, CSP, or verifier). It usually describes the policies and practices  
410 of the Participants and can become legally binding.  
411

412 Private Credentials: Credentials that cannot be disclosed by the CSP because the contents can  
413 be used to compromise the authenticator.  
414

415 Private Key: The secret part of an asymmetric key pair that is used to digitally sign or decrypt  
416 data.  
417

418 Protected Session: A session wherein messages between two participants are encrypted and  
419 integrity is protected using a set of shared secrets called session keys. A participant is said to be  
420 authenticated if, during the session, he, she or it proves possession of a long term authenticator  
421 in addition to the session keys, and if the other Participant can verify the identity associated  
422 with that authenticator. If both participants are authenticated, the protected session is said to  
423 be mutually authenticated.  
424

425 Pseudonymous Identifier: A meaningless, but unique number that does not allow the RP to  
426 infer the Subscriber but which does permit the RP to associate multiple interactions with the  
427 Subscriber's Claimed Identity.  
428

429 Public Credentials: Credentials that describe the binding in a way that does not compromise the  
430 authenticator.  
431

432 Public Key: The public part of an asymmetric key pair that is used to verify signatures or encrypt  
433 data.  
434

435 Public Key Certificate: A digital document issued and digitally signed by the private key of a  
436 Certificate authority that binds the name of a Subscriber to a public key. The certificate  
437 indicates that the Subscriber identified in the certificate has sole control and access to the  
438 private key. See also [RFC 5280].  
439

440 Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software and  
441 workstations used for the purpose of administering certificates and public-private key pairs,  
442 including the ability to issue, maintain, and revoke public key certificates.  
443

444 Registration: The process through which an applicant applies to become a Subscriber of a CSP  
445 and an RA validates the identity of the applicant on behalf of the CSP.  
446

447 Registration Authority (RA): A trusted entity that establishes and vouches for the identity or  
448 attributes of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be  
449 independent of a CSP, but it has a relationship to the CSP(s).  
450

451 Relying Party (RP): An entity that relies upon the Subscriber's authenticator(s) and credentials  
452 or a verifier's Assertion of a claimant's identity, typically to process a transaction or grant access  
453 to information or a system.  
454

455 Remote: (As in remote authentication or remote transaction) An information exchange  
456 between network-connected devices where the information cannot be reliably protected end-  
457 to-end by a single organization's security controls. Note: Any information exchange across the  
458 Internet is considered remote.  
459

460 Replay Attack: An attack in which the attacker is able to replay previously captured messages  
461 (between a legitimate claimant and a verifier) to masquerade as that claimant to the verifier or  
462 vice versa.  
463

464 Risk Assessment: The process of identifying the risks to system security and determining the  
465 probability of occurrence, the resulting impact, and additional safeguards that would mitigate  
466 this impact. Part of Risk Management and synonymous with Risk Analysis.  
467

468 Salt: A non-secret value that is used in a cryptographic process, usually to ensure that the  
469 results of computations for one instance cannot be reused by an attacker.  
470

471 Secondary Authenticator: A temporary secret, issued by the verifier to a successfully  
472 authenticated Subscriber as part of an Assertion protocol. This secret is subsequently used, by  
473 the Subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer  
474 Assertions, Assertion references, and Kerberos session keys.  
475

476 Secure Sockets Layer (SSL): An authentication and security protocol widely implemented in  
477 browsers and web servers. SSL has been superseded by the newer Transport Layer Security  
478 (TLS) protocol; TLS 1.0 is effectively SSL version 3.1.  
479

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

484 SAML Authentication Assertion: A SAML Assertion that conveys information from a verifier to  
485 an RP about a successful act of authentication that took place between the verifier and a  
486 Subscriber.  
487

488 Session Hijack Attack: An attack in which the attacker is able to insert himself or herself  
489 between a claimant and a verifier subsequent to a successful authentication exchange between  
490 the latter two Participants. The attacker is able to pose as a Subscriber to the verifier or vice  
491 versa to control session data exchange. Sessions between the claimant and the relying  
492 Participant can also be similarly compromised.  
493

494 Shared Secret: A secret used in authentication that is known to the claimant and the verifier.  
495

496 Social Engineering: The act of deceiving an individual into revealing sensitive information by  
497 associating with the individual to gain confidence and trust.  
498

499 Special Publication (SP): A type of publication issued by NIST. Specifically, the Special  
500 Publication 800-series reports on the Information Technology Laboratory's research, guidelines,  
501 and outreach efforts in computer security, and its collaborative activities with industry,  
502 government, and academic organizations.  
503

504 Strongly Bound Credentials: Credentials that describe the binding between a user and  
505 authenticator in a tamper-evident fashion.  
506

507 Subscriber: A Participant who has received a credential or authenticator from a CSP.  
508

509 Symmetric Key: A cryptographic key that is used to perform both the cryptographic operation  
510 and its inverse, for example to encrypt and decrypt, or create a message authentication code  
511 and to verify the code.  
512

513 Token: See Authenticator.  
514

515 Token Authenticator: See Authenticator Output.  
516

517 Token Secret: See Authenticator Secret.  
518

519 Transport Layer Security (TLS): An authentication and security protocol widely implemented in  
520 browsers and web servers. TLS is defined by [RFC 5246]. TLS is similar to the older Secure  
521 Sockets Layer (SSL) protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52,  
522 Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations specifies  
523 how TLS is to be used in government applications.  
524

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

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

## 557 6 Background

---

558

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

565

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

571

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

579

### 580 Purpose Statement

581

582 This guidance document, as defined in § 2.2-4001, was developed by the Identity Management  
583 Standards Advisory Council (IMSAC), on behalf of the Secretary of Technology, to provide  
584 information or guidance of general applicability to the public for interpreting or implementing  
585 the Electronic Identity Management Act. Specifically, the document establishes minimum  
586 specifications for Electronic Authentication within a Digital Identity System. The minimum  
587 specifications have been designed to be conformant with NIST SP 800-63-3.

588

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

595

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

## 599 7 Minimum Specifications

---

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

606  
607 This document establishes minimum specifications for Electronic Authentication conformant  
608 with NIST SP 800-63-3. However, the minimum specifications defined in this document have  
609 been developed to accommodate requirements for Electronic Authentication established under  
610 other national and international standards.<sup>13</sup> The minimum specifications in this document also  
611 assume that specific business, legal, and technical requirements for a Digital Identity System  
612 will be documented in the Identity Trust Framework for that system. Minimum specifications  
613 for other components of a Digital Identity System have been documented in separate guidance  
614 documents in the IMSAC series, pursuant to §2.2-436 and §2.2-437.

### 615 616 Electronic Authentication Model

617  
618 Electronic Authentication is the process of establishing confidence in individual identities  
619 presented to a Digital Identity System. Digital Identity Systems can use the authenticated  
620 identity to determine if that individual is authorized to perform an online transaction. The  
621 minimum specifications in this document assume that the authentication and transaction take  
622 place across a network.

623  
624 The Electronic Authentication model defined in these minimum specifications reflects current  
625 technologies and architectures used primarily by governmental entities. More complex models  
626 that separate functions among a broader range of parties are also available and may have  
627 advantages in some classes of applications. While a simpler model has been defined in these  
628 minimum specifications, it does not preclude members in Digital Identity Systems from  
629 separating these functions.

630  
631 In addition, certain Registration, Identity Proofing, and issuance processes performed by the  
632 credential service provider (CSP) may be delegated to an entity known as the Registration  
633 authority (RA) or identity manager (IM). A close relationship between the RA/IM and CSP is

---

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

<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>.

634 typical, and the nature of this relationship may differ among RAs, IMs, and CSPs. The minimum  
635 specifications defined in this document assume that relationships between members and their  
636 requirements are established in the Identity Trust Framework for the Digital Identity System.

637

638 Electronic authentication begins with Registration (also referred to as enrollment). The usual  
639 sequence for Registration proceeds as follows. An applicant applies to a CSP. If approved, the  
640 CSP creates a credential and binds it to one or more authenticators. The credential includes an  
641 identifier, which can be pseudonymous, and one or more Attributes that the CSP has verified.  
642 The authenticators may be issued by the CSP, generated/provided directly by the Subscriber, or  
643 provided by a third party. The authenticator and credential may be used in subsequent  
644 authentication events.

645

646 The process used to verify an applicant's association with their real world identity is called  
647 Identity Proofing. The strength of Identity Proofing is described by a categorization called the  
648 identity assurance level (IAL, see subsection on Assurance Level Model below in this document).  
649 Minimum specifications for Identity Proofing and verification during the Registration process  
650 have been established in *IMSAC Guidance Document: Identity Proofing and Verification*.

651

652 At IAL 1, Identity Proofing is not required, therefore any Attribute information provided by the  
653 Subscriber is self-asserted and not verified. At IAL 2 and 3, Identity Proofing is required, but the  
654 CSP may assert verified Attribute values, verified Attribute claims, pseudonymous identifiers, or  
655 nothing. This information assists Relying Parties (RPs) in making access control or authorization  
656 decisions. RPs may decide that their required IAL is 2 or 3, but may only need specific  
657 Attributes, and perhaps Attributes that retain an individual's pseudonymity. A relying party may  
658 also employ a federated identity approach where the RP outsources all Identity Proofing,  
659 Attribute collection, and Attribute storage to a CSP.

660

661 In these minimum specifications, the party to be authenticated is called a claimant and the  
662 party verifying that identity is called a verifier. When a claimant successfully demonstrates  
663 possession and control of one or more authenticators to a verifier through an authentication  
664 protocol, the verifier can verify that the claimant is a valid Subscriber. The verifier passes on an  
665 Assertion about the Subscriber, who may be either pseudonymous or non-pseudonymous, to  
666 the RP. That Assertion includes an identifier, and may include identity information about the  
667 Subscriber, such as the name, or other Attributes that were verified in the enrollment process  
668 (subject to the policies of the CSP and the Identity Trust Framework for the system). When the  
669 verifier is also the RP, the Assertion may be implicit. The RP can use the authenticated  
670 information provided by the verifier to make access control or authorization decisions.

671

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

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

683

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

691

## 692 Authentication Components and Process Flows

693

694 The various entities and interactions that comprise the Electronic Authentication model defined  
695 in these minimum specifications have been illustrated below in **Figure 1**. The left shows the  
696 enrollment, credential issuance, lifecycle management activities, and the stages an individual  
697 transitions, based on the specific phase of the Identity Proofing and authentication process.

698

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

703

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

709

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

715

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

721

722 The usual sequence of interactions in the authentication process is as follows:

- 723 1. An applicant applies to a CSP through a Registration process.
- 724 2. The CSP identity proofs that applicant. Upon successful proofing, the applicant becomes  
725 a Subscriber.
- 726 3. An authenticator and a corresponding credential are established between the CSP and  
727 the new Subscriber.
- 728 4. The CSP maintains the credential, its status, and the enrollment data collected for the  
729 lifetime of the credential. The Subscriber maintains his or her authenticator.

730

731 Other sequences are less common, but could also achieve the same functional requirements.

732 The right side of Figure 1 shows the entities and the interactions related to using an  
733 authenticator to perform Electronic Authentication. When the Subscriber needs to authenticate  
734 to perform a transaction, he or she becomes a claimant to a verifier. The interactions are as  
735 follows:

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

744

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

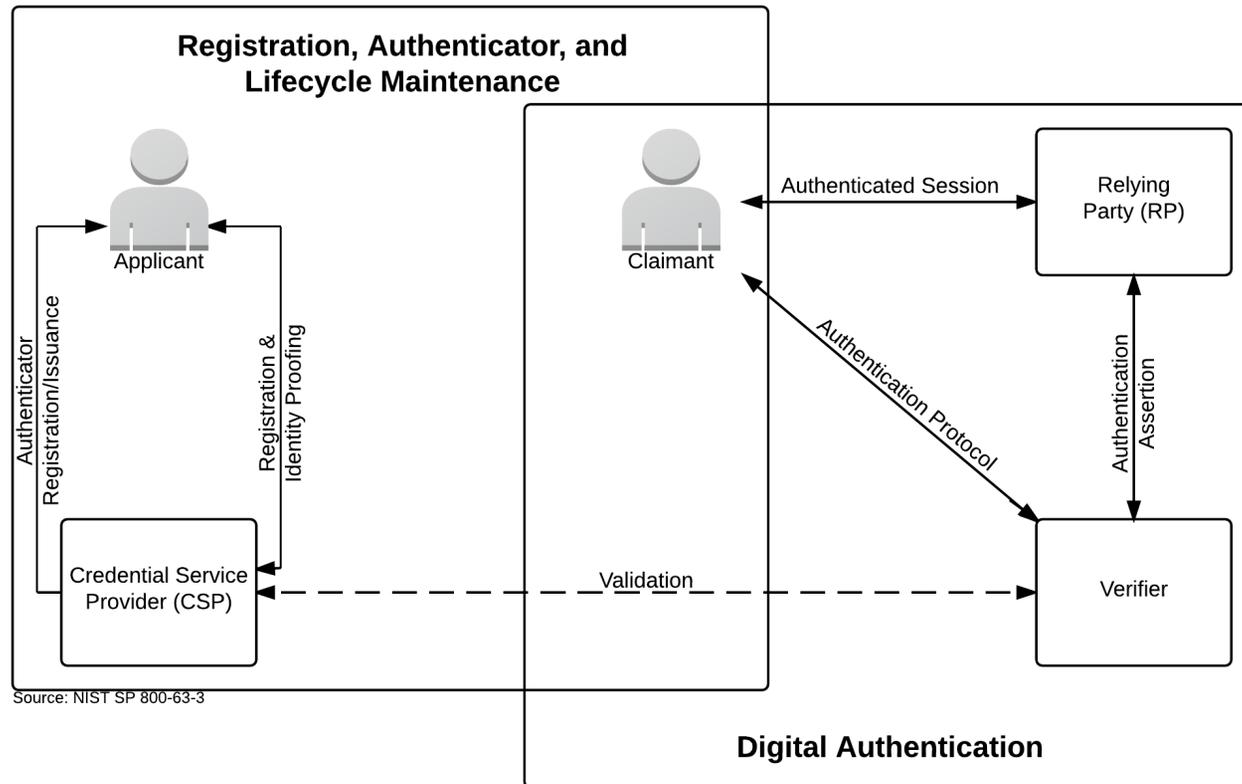
748

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

756

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

766 **Figure 1. Electronic Authentication Model**



767  
 768  
 769 Source: NIST SP 800-63-3, accessible at <https://pages.nist.gov/800-63-3/sp800-63-3.html>  
 770 Note: Figure 1 illustrates the model for Electronic Authentication in a Digital Identity System, as documented in NIST SP 800-63-3 (Public  
 771 Review), containing all components, requirements, and specifications recommended by IMSAC. However, the minimum specifications  
 772 defined in this document have been developed to accommodate requirements for Electronic Authentication established under other  
 773 national and international standards.  
 774

## 775 Authentication Protocols and Lifecycle Management

776

### 777 Authenticators

778 The established paradigm for Electronic Authentication identifies three factors as the  
779 cornerstone of authentication:

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

783

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

791

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

797

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

805

806 Shared secrets stored on authenticators may be either symmetric keys or passwords. While  
807 they can be used in similar protocols, one important difference between the two is how they  
808 relate to the Subscriber. While symmetric keys are generally stored in hardware or software  
809 that the Subscriber controls, passwords are intended to be memorized by the Subscriber. As  
810 such, keys are something the Subscriber has, while passwords are something he or she knows.  
811 Since passwords are committed to memory, they usually do not have as many possible values  
812 as cryptographic keys, and, in many protocols, are severely vulnerable to network attacks that  
813 are more restricted for keys.

814

815 Moreover, the entry of passwords into systems (usually through a keyboard) presents the  
816 opportunity for very simple keyboard logging attacks, and may also allow those nearby to learn  
817 the password by watching it being entered. Therefore, keys and passwords demonstrate  
818 somewhat separate authentication properties (something you have rather than something you

819 know). When using either public key pairs or shared secrets, the Subscriber has a duty to  
820 maintain exclusive control of his or her authenticator, since possession and control of the  
821 authenticator is used to authenticate the claimant's identity.

822

823 The minimum specifications defined in this document assume that authenticators always  
824 contain a secret. Authentication factors classified as something you know are not necessarily  
825 secrets. Knowledge based authentication, where the claimant is prompted to answer questions  
826 that can be confirmed from public databases, also does not constitute an acceptable secret for  
827 Electronic Authentication. More generally, something you are does not generally constitute a  
828 secret. However, the requirements for some Digital Identity Systems may allow the use of  
829 biometrics as an authenticator.

830

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

838

839 The minimum specifications in this document encourage Digital Identity Systems to use  
840 authentication processes and protocols that incorporate all three factors, as a means of  
841 enhancing system security. An Electronic Authentication system may incorporate multiple  
842 factors in either of two ways. The system may be implemented so that multiple factors are  
843 presented to the verifier, or some factors may be used to protect a secret presented to the  
844 verifier. If multiple factors are presented to the verifier, each will need to be an authenticator  
845 (and therefore contain a secret). If a single factor is presented to the verifier, the additional  
846 factors are used to protect the authenticator and need not themselves be authenticators.

847

848 Credentials

849 As described in the preceding sections, credentials bind an authenticator to the Subscriber as  
850 part of the issuance process. Credentials are stored and maintained by the CSP. The claimant  
851 possesses an authenticator, but is not necessarily in possession of the electronic credentials.  
852 For example, database entries containing the user Attributes are considered to be credentials  
853 for the purpose of this document but are possessed by the verifier.

854

855 Assertions

856 Upon completion of the Electronic Authentication process, the verifier generates an Assertion  
857 containing the result of the authentication and provides it to the RP. If the verifier is  
858 implemented in combination with the RP, the Assertion is implicit. If the verifier is a separate  
859 entity from the RP, as in typical federated identity models, the Assertion is used to  
860 communicate the result of the authentication process, and optionally information about the  
861 Subscriber, from the verifier to the RP. Minimum specifications for Assertions have been  
862 defined in *IMSAC Guidance Document: Digital Identity Assertions*.

863 Assertions may be communicated directly to the RP, or can be forwarded through the  
864 Subscriber, which has further implications for system design. An RP trusts an Assertion based  
865 on the source, the time of creation, and the corresponding Identity Trust Framework that  
866 governs the policies and process of CSPs and RPs. The verifier is responsible for providing a  
867 mechanism by which the integrity of the Assertion can be confirmed.

868

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

877

878 Examples of Assertions include:

- 879 • SAML Assertions – SAML Assertions are specified using a mark-up language intended for  
880 describing security Assertions. They can be used by a verifier to make a statement to an  
881 RP about the identity of a claimant. SAML Assertions may be digitally signed.
- 882 • Kerberos Tickets – Kerberos Tickets allow a ticket granting authority to issue session  
883 keys to two authenticated parties using symmetric key based encapsulation schemes.
- 884 • OpenID Connect Claims - OpenID Connect are specified using JavaScript Object Notation  
885 (JSON) for describing security, and optionally, user claims. JSON user info claims may be  
886 digitally signed.
- 887 •

888

889 Relying Parties

890 An RP relies on results of an authentication protocol to establish confidence in the identity or  
891 Attributes of a Subscriber for the purpose of conducting an online transaction. RPs may use a  
892 Subscriber's authenticated identity (pseudonymous or non-pseudonymous), the IAL, AAL, and  
893 other factors to make access control or authorization decisions. The verifier and the RP may be  
894 the same entity, or they may be separate entities. If they are separate entities, the RP normally  
895 receives an Assertion from the verifier. The RP ensures that the Assertion came from a verifier  
896 trusted by the RP. The RP also processes any additional information in the Assertion, such as  
897 personal Attributes or expiration times.

898

899

## 900 Assurance Model

901

902 The minimum specifications defined in this document for Electronic Authentication assume that  
903 the Identity Trust Framework for a Digital Identity System will define a specific Assurance  
904 Model for that system.<sup>14</sup> Therefore, the Assurance Model presented below, which is based on  
905 NIST SP 800-63-3, should be viewed as a recommended framework for Electronic  
906 Authentication. A full discussion of the NIST SP 800-63-3 Assurance Model has been provided  
907 in *IMSAC Guidance Document: Authenticators and Lifecycle Management*.

908

909 Other Assurance Models have been established in OMB M-04-04 and the State Identity,  
910 Credential, and Access Management (SICAM) guidelines, published by the National Association  
911 of State Chief Information Officers (NASCIO). A crosswalk showing disparities in the NIST SP  
912 800-63-3, OMB M-04-04, and SICAM Assurance Models has been provided in **Figure 2**.

913

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

916

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

920

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

924

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

932

933 Authenticator Assurance Level 2 – AAL 2 provides higher assurance that the same claimant who  
934 participated in previous transactions is accessing the protected transaction or data. Two  
935 different authentication factors are required. Various types of authenticators, including multi-  
936 factor Software Cryptographic Authenticators, may be used as described in NIST 800-63B. AAL 2  
937 also permits any of the authentication methods of AAL 3. AAL 2 authentication requires  
938 cryptographic mechanisms that protect the primary authenticator against compromise by the

---

<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.

939 protocol threats for all threats at AAL 1 as well as verifier impersonation attacks. Approved  
 940 cryptographic techniques are required for all Assertion protocols used at AAL 2 and above.<sup>15</sup>  
 941

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

950

951 **Figure 2. Assurance Model Crosswalk**

952

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

953

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

## 954 Privacy and Security

955

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

960

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

964

965 The minimum specifications for Electronic Authentication apply the following FIPPs:

- 966 • Transparency: RAs and CSPs should be transparent and provide notice to Applicants  
967 regarding collection, use, dissemination, and maintenance of person information required  
968 during the Registration, Identity Proofing and verification processes.
- 969 • Individual Participation: RAs and CSPs should involve the Applicant in the process of using  
970 person information and, to the extent practicable, seek consent for the collection, use,  
971 dissemination, and maintenance of that information. RAs and CSPs also should provide  
972 mechanisms for appropriate access, correction, and redress of person information.
- 973 • Purpose Specification: RAs and CSPs should specifically articulate the authority that permits  
974 the collection of person information and specifically articulate the purpose or purposes for  
975 which the information is intended to be used.
- 976 • Data Minimization: RAs and CSPs should collect only the person information directly  
977 relevant and necessary to accomplish the Registration and related processes, and only  
978 retain that information for as long as necessary to fulfill the specified purpose.
- 979 • Use Limitation/Minimal Disclosure: RAs and CSPs should use person information solely for  
980 the purpose specified in the notice. Disclosure or sharing that information should be limited  
981 to the specific purpose for which the information was collected.
- 982 • Data Quality and Integrity: RAs and CSPs should, to the extent practicable, ensure that  
983 person information is accurate, relevant, timely, and complete.
- 984 • Security: RAs and CSPs should protect personal information through appropriate security  
985 safeguards against risks such as loss, unauthorized access or use, destruction, modification,  
986 or unintended or inappropriate disclosure.
- 987 • Accountability and Auditing: RAs and CSPs should be accountable for complying with these  
988 principles, providing training to all employees and contractors who use person information,  
989 and auditing the actual use of person information to demonstrate compliance with these  
990 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>.

## 991 8 Alignment Comparison

---

992  
993 The minimum specifications for Electronic Authentication defined in this document have been  
994 developed to align with existing national and international standards for Electronic  
995 Authentication and identity management. Specifically, the minimum specifications reflect basic  
996 requirements set forth in national standards at the federal and state level, ensuring compliance  
997 while accommodating other identity management standards and protocols. This document  
998 assumes that each Digital Identity System will comply with those governing standards and  
999 protocols required by Applicable Law.

1000  
1001 The following section outlines the alignment and disparities between the minimum  
1002 specifications in this document and core national standards. A crosswalk documenting the  
1003 alignment and areas of misalignment has been provided in **Appendix 3**.

### 1004 1005 NIST SP 800-63-3

1006  
1007 The minimum specifications in this document conform with the basic requirements for  
1008 Electronic Authentication set forth in NIST SP 800-63-3 (Public Review version). However, as  
1009 the NIST guidance defines specific requirements for federal agencies, the minimum  
1010 specifications in this document provide flexibility for Digital Identity Systems across industries in  
1011 the private sector and levels of governance. This flexibility enables Digital Identity Systems to  
1012 adhere to the specifications but do so in a manner appropriate and compliant with their  
1013 governing Identity Trust Frameworks.

### 1014 1015 State Identity and Access Management Credential (SICAM) Guidance and Roadmap

1016  
1017 The minimum specifications in this document conform with the basic requirements for  
1018 Electronic Authentication set forth by NASCIO in the SICAM Guidance and Roadmap. The  
1019 NASCIO guidance defines specific requirements for state agencies. Similar to the contrast with  
1020 the NIST guidance for federal agencies, the minimum specifications in this document provide  
1021 flexibility for Digital Identity Systems across industries in the private sector and levels of  
1022 governance.

### 1023 1024 IDESG Identity Ecosystem Framework (IDEF) Functional Model

1025  
1026 The minimum specifications in this document conform with the core operations and basic  
1027 requirements for privacy and security set forth by IDESG in the IDEF Functional Model and  
1028 Baseline Functional Requirements. The IDESG/IDEF requirements apply the FIPPs but extend  
1029 them to cover the NSTIC Guiding Principles. The minimum specifications in this document  
1030 encourage adherence to the IDEF Functional Model, Baseline Functional Requirements, and the  
1031 NSTIC Guiding Principles.

1032

## 1033 Appendix 1. IMSAC Charter

1034

1035

1036

1037

1038

**COMMONWEALTH OF VIRGINIA**  
**IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL**  
**CHARTER**

1039 **Advisory Council Responsibilities (§ 2.2-437.A; § 2.2-436.A)**

1040

1041 The Identity Management Standards Advisory Council (the Advisory Council) advises the  
1042 Secretary of Technology on the adoption of identity management standards and the creation of  
1043 guidance documents pursuant to § 2.2-436.

1044

1045 The Advisory Council recommends to the Secretary of Technology guidance documents relating  
1046 to (i) nationally recognized technical and data standards regarding the verification and  
1047 authentication of identity in digital and online transactions; (ii) the minimum specifications and  
1048 standards that should be included in an Identity Trust Framework, as defined in § 59.1-550, so  
1049 as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-  
1050 550 et seq.); and (iii) any other related data standards or specifications concerning reliance by  
1051 third parties on identity credentials, as defined in § 59.1-550.

1052

1053 **Membership and Governance Structure (§ 2.2-437.B)**

1054

1055 The Advisory Council's membership and governance structure is as follows:

1056 1. The Advisory Council consists of seven members, to be appointed by the Governor, with  
1057 expertise in electronic identity management and information technology. Members include  
1058 a representative of the Department of Motor Vehicles, a representative of the Virginia  
1059 Information Technologies Agency, and five representatives of the business community with  
1060 appropriate experience and expertise. In addition to the seven appointed members, the  
1061 Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex  
1062 officio member of the Advisory Council.

1063

1064 2. The Advisory Council designates one of its members as chairman.

1065

1066 3. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure  
1067 of the Governor, and may be reappointed.

1068

1069 4. Members serve without compensation but may be reimbursed for all reasonable and  
1070 necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.

1071

1072 5. Staff to the Advisory Council is provided by the Office of the Secretary of Technology.

1073

1074

1075 The formation, membership and governance structure for the Advisory Council has been  
1076 codified pursuant to § 2.2-437.A, § 2.2-437.B, as cited above in this charter.

1077

1078 The statutory authority and requirements for public notice and comment periods for guidance  
1079 documents have been established pursuant to § 2.2-437.C, as follows:

1080

1081 C. Proposed guidance documents and general opportunity for oral or written submittals as to  
1082 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published  
1083 in the Virginia Register of Regulations as a general notice following the processes and  
1084 procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§  
1085 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written  
1086 comments following the posting and publication and shall hold at least one meeting dedicated  
1087 to the receipt of oral comment no less than 15 days after the posting and publication. The  
1088 Advisory Council shall also develop methods for the identification and notification of interested  
1089 parties and specific means of seeking input from interested persons and groups. The Advisory  
1090 Council shall send a copy of such notices, comments, and other background material relative to  
1091 the development of the recommended guidance documents to the Joint Commission on  
1092 Administrative Rules.

1093

1094

1095 This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the  
1096 minutes of the meeting and related IMSAC documents, visit:  
1097 <https://vita.virginia.gov/About/default.aspx?id=6442474173>

1098 Appendix 2. IDESG Identity Ecosystem Framework (IDEF) Baseline  
1099 Functional Requirements (v.1.0) for Privacy and Security

1100

1101 PRIVACY-1. DATA MINIMIZATION

1102 Entities MUST limit the collection, use, transmission and storage of personal information to the  
1103 minimum necessary to fulfill that transaction's purpose and related legal requirements. Entities  
1104 providing claims or Attributes MUST NOT provide any more personal information than what is  
1105 requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to  
1106 accommodate information requests of variable granularity, to support data minimization.

1107

1108 PRIVACY-2. PURPOSE LIMITATION

1109 Entities MUST limit the use of personal information that is collected, used, transmitted, or  
1110 stored to the specified purposes of that transaction. Persistent records of contracts, assurances,  
1111 consent, or legal authority MUST be established by entities collecting, generating, using,  
1112 transmitting, or storing personal information, so that the information, consistently is used in  
1113 the same manner originally specified and permitted.

1114

1115 PRIVACY-3. ATTRIBUTE MINIMIZATION

1116 Entities requesting Attributes MUST evaluate the need to collect specific Attributes in a  
1117 transaction, as opposed to claims regarding those Attributes. Wherever feasible, entities MUST  
1118 collect, generate, use, transmit, and store claims about USERS rather than Attributes. Wherever  
1119 feasible, Attributes MUST be transmitted as claims, and transmitted credentials and identities  
1120 MUST be bound to claims instead of actual Attribute values.

1121

1122 PRIVACY-4. CREDENTIAL LIMITATION

1123 Entities MUST NOT request USERS' credentials unless necessary for the transaction and then  
1124 only as appropriate to the risk associated with the transaction or to the risks to the parties  
1125 associated with the transaction.

1126

1127 PRIVACY-5. DATA AGGREGATION RISK

1128 Entities MUST assess the privacy risk of aggregating personal information, in systems and  
1129 processes where it is collected, generated, used, transmitted, or stored, and wherever feasible,  
1130 MUST design and operate their systems and processes to minimize that risk. Entities MUST  
1131 assess and limit linkages of personal information across multiple transactions without the  
1132 USER's explicit consent.

1133

1134 PRIVACY-6. USAGE NOTICE

1135 Entities MUST provide concise, meaningful, and timely communication to USERS describing how  
1136 they collect, generate, use, transmit, and store personal information.

1137

1138 PRIVACY-7. USER DATA CONTROL

1139 Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete  
1140 personal information.

## 1141 PRIVACY-8. THIRD-PARTY LIMITATIONS

1142 Wherever USERS make choices regarding the treatment of their personal information, those  
1143 choices MUST be communicated effectively by that entity to any THIRD-PARTIES to which it  
1144 transmits the personal information.

1145

## 1146 PRIVACY-9. USER NOTICE OF CHANGES

1147 Entities MUST, upon any material changes to a service or process that affects the prior or  
1148 ongoing collection, generation, use, transmission, or storage of USERS' personal information,  
1149 notify those USERS, and provide them with compensating controls designed to mitigate privacy  
1150 risks that may arise from those changes, which may include seeking express affirmative consent  
1151 of USERS in accordance with relevant law or regulation.

1152

## 1153 PRIVACY-10. USER OPTION TO DECLINE

1154 USERS MUST have the opportunity to decline Registration; decline credential provisioning;  
1155 decline the presentation of their credentials; and decline release of their Attributes or claims.

1156

## 1157 PRIVACY-11. OPTIONAL INFORMATION

1158 Entities MUST clearly indicate to USERS what personal information is mandatory and what  
1159 information is optional prior to the transaction.

1160

## 1161 PRIVACY-12. ANONYMITY

1162 Wherever feasible, entities MUST utilize identity systems and processes that enable  
1163 transactions that are anonymous, anonymous with validated Attributes, pseudonymous, or  
1164 where appropriate, uniquely identified. Where applicable to such transactions, entities  
1165 employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES  
1166 collecting USER personal information. Organizations MUST request individuals' credentials only  
1167 when necessary for the transaction and then only as appropriate to the risk associated with the  
1168 transaction or only as appropriate to the risks to the parties associated with the transaction.

1169

## 1170 PRIVACY-13. CONTROLS PROPORTIONATE TO RISK

1171 Controls on the processing or use of USERS' personal information MUST be commensurate with  
1172 the degree of risk of that processing or use. A privacy risk analysis MUST be conducted by  
1173 entities who conduct digital identity management functions, to establish what risks those  
1174 functions pose to USERS' privacy.

1175

## 1176 PRIVACY-14. DATA RETENTION AND DISPOSAL

1177 Entities MUST limit the retention of personal information to the time necessary for providing  
1178 and administering the functions and services to USERS for which the information was collected,  
1179 except as otherwise required by law or regulation. When no longer needed, personal  
1180 information MUST be securely disposed of in a manner aligning with appropriate industry  
1181 standards and/or legal requirements.

1182

## 1183 PRIVACY-15. ATTRIBUTE SEGREGATION

1184 Wherever feasible, identifier data MUST be segregated from Attribute data.

## 1185 SECURE-1. SECURITY PRACTICES

1186 Entities MUST apply appropriate and industry-accepted information security STANDARDS,  
1187 guidelines, and practices to the systems that support their identity functions and services.

1188

## 1189 SECURE-2. DATA INTEGRITY

1190 Entities MUST implement industry-accepted practices to protect the confidentiality and  
1191 integrity of identity data—including authentication data and Attribute values—during the  
1192 execution of all digital identity management functions, and across the entire data lifecycle  
1193 (collection through destruction).

1194

## 1195 SECURE-3. CREDENTIAL REPRODUCTION

1196 Entities that issue or manage credentials and tokens MUST implement industry-accepted  
1197 processes to protect against their unauthorized disclosure and reproduction.

1198

## 1199 SECURE-4. CREDENTIAL PROTECTION

1200 Entities that issue or manage credentials and tokens MUST implement industry-accepted data  
1201 integrity practices to enable individuals and other entities to verify the source of credential and  
1202 token data.

1203

## 1204 SECURE-5. CREDENTIAL ISSUANCE

1205 Entities that issue or manage credentials and tokens MUST do so in a manner designed to  
1206 assure that they are granted to the appropriate and intended USER(s) only. Where Registration  
1207 and credential issuance are executed by separate entities, procedures for ensuring accurate  
1208 exchange of Registration and issuance information that are commensurate with the stated  
1209 assurance level MUST be included in business agreements and operating policies.

1210

## 1211 SECURE-6. CREDENTIAL UNIQUENESS

1212 Entities that issue or manage credentials MUST ensure that each account to credential pairing is  
1213 uniquely identifiable within its namespace for authentication purposes.

1214

## 1215 SECURE-7. TOKEN CONTROL

1216 Entities that authenticate a USER MUST employ industry-accepted secure authentication  
1217 protocols to demonstrate the USER's control of a valid token.

1218

## 1219 SECURE-8. MULTIFACTOR AUTHENTICATION

1220 Entities that authenticate a USER MUST offer authentication mechanisms which augment or are  
1221 alternatives to a password.

1222

## 1223 SECURE-9. AUTHENTICATION RISK ASSESSMENT

1224 Entities MUST have a risk assessment process in place for the selection of authentication  
1225 mechanisms and supporting processes.

1226

1227

1228

## 1229 SECURE-10. UPTIME

1230 Entities that provide and conduct digital identity management functions MUST have established  
1231 policies and processes in place to maintain their stated assurances for availability of their  
1232 services.

1233

## 1234 SECURE-11. KEY MANAGEMENT

1235 Entities that use cryptographic solutions as part of identity management MUST implement key  
1236 management policies and processes that are consistent with industry-accepted practices.

1237

## 1238 SECURE-12. RECOVERY AND REISSUANCE

1239 Entities that issue credentials and tokens MUST implement methods for reissuance, updating,  
1240 and recovery of credentials and tokens that preserve the security and assurance of the original  
1241 Registration and credentialing operations.

1242

## 1243 SECURE-13. REVOCATION

1244 Entities that issue credentials or tokens MUST have processes and procedures in place to  
1245 invalidate credentials and tokens.

1246

## 1247 SECURE-14. SECURITY LOGS

1248 Entities conducting digital identity management functions MUST log their transactions and  
1249 security events, in a manner that supports system audits and, where necessary, security  
1250 investigations and regulatory requirements. Timestamp synchronization and detail of logs  
1251 MUST be appropriate to the level of risk associated with the environment and transactions.

1252

## 1253 SECURE-15. SECURITY AUDITS

1254 Entities MUST conduct regular audits of their compliance with their own information security  
1255 policies and procedures, and any additional requirements of law, including a review of their  
1256 logs, incident reports and credential loss occurrences, and MUST periodically review the  
1257 effectiveness of their policies and procedures in light of that data.

1258

### Appendix 3. Electronic Authentication Standards Alignment Comparison Matrix

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