

COMMONWEALTH OF VIRGINIA



Information Technology Resource Management (ITRM)

GUIDANCE DOCUMENT
~~Identity Proofing~~**Identity Proofing** and Verification

Virginia Information Technologies Agency (VITA)

Table of Contents

1	Publication Version Control	1
2	Reviews	1
3	Statutory Authority	2
4	Definitions	3
5	Background	16
6	Minimum Specifications	18
7	Alignment Comparison	25

DRAFT

1 Publication Version Control

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

Publication Version	Date	Revision Description
1.0	05/02/2016	Initial Draft of Document
<u>1.0</u>	<u>05/02/2016</u>	<u>Document revised by IMSAC at public workshop</u>
<u>1.0</u>	<u>06/23/2016</u>	<u>Document revised by VITA staff based on comments from IMSAC during May 2, 2016, public workshop</u>
<u>1.0</u>	<u>09/12/2016</u>	<u>Document revised by VITA staff based on public comment received pursuant to § 2.2-437.C, Code of Virginia</u>

2 Reviews

- The initial version of the document was prepared by the staff analysts for the Identity Management Standards Advisory Council, within Commonwealth Data Governance, Enterprise Architecture, Virginia Information Technologies Agency.
- The document was reviewed by IMSAC during a council workshop, May 2, 2016.
- The document was revised based on public comment received in written and verbal form during the 30-day comment period, pursuant to § 2.2-437.C, 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 June 30, more than 15 days after the posting and publication. The following comments were received on July 13, 2016, via the Virginia Regulatory Town Hall, with page references to the previous version and the response in brackets []:
 - o For purposes of setting minimum standards for identity proofing and issuance of credentials/tokens/authenticators, continue to use levels of assurance as defined in the latest approved NIST 800-63 document series. This will be especially important to both identity providers and relying parties in the commercial sector. [Noted]
 - o On pages 21 and 22 under discussions of Level of Assurance 2, 3, and 4, add references to "virtual in-person proofing" as an approved method consistent with draft 800-63A. [The Assurance Model in this document has been amended

Formatted: Normal, No bullets or numbering

34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51

to be consistent with the Public Review version of NIST SP 800-63-3. A definition for “virtual in-person proofing” based on NIST SP 800-63A has been added to this document.]

o On page 15, add a definition of "virtual in-person proofing" perhaps based on section 5.4.3 of draft 800-63A. [A definition for “virtual in-person proofing” has been added to this document, consistent with NIST SP 800-63A.]

o On page 12, add a definition of "remote network identity proofing." This could be modeled after language contained in NIST 800-63 series documents. [The term “remote network identity proofing” has not been defined in the NIST SP 800-63 document series. However, the term “Remote” has been defined in the NIST SP 800-63 document series and in this document, and the definition covers remote transactions across a network in an identity proofing context.]

- The document will be reviewed in a manner compliant with the Commonwealth of Virginia’s ITRM Policies, Standards, and Guidelines and §2.2-437.C, Code of Virginia:

Formatted

Comment [JG1]: Use a COV standards based approach to requiring regular review of the document. (N. Moe and M. Watson)
IMSAC may direct staff to update the documents based on updates to standards documents, i.e. NIST 800-63, IDESG IDEF, etc. (L. Kimball)

DRAFT

52 **3 Statutory Authority**

53
54 The following section documents the statutory authority established in the *Code of Virginia* for
55 the development of minimum specifications and standards for Identity Proofing and verification
56 within a Digital Identity System. References to statutes below and throughout this document
57 shall be to the *Code of Virginia*, unless otherwise specified.
58

59 Governing Statutes:

60
61 Secretary of Technology

62 § 2.2-225. Position established; agencies for which responsible; additional powers

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

64
65 Secretary of Transportation

66 § 2.2-228. Position established; agencies for which responsible

67 <http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-228/>

68
69 Identity Management Standards Advisory Council

70 § 2.2-437. Identity Management Standards Advisory Council

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

72
73 Commonwealth Identity Management Standards

74 § 2.2-436. Approval of electronic identity standards

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

76
77 Electronic Identity Management Act

78 Chapter 50. Electronic Identity Management Act

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

80
81 Chief Information Officer (CIO) of the Commonwealth

82 § 2.2-2007. Powers of the CIO

83 <http://law.lis.virginia.gov/vacode/title2.2/chapter20.1/section2.2-2007/>

84
85 Virginia Information Technologies Agency

86 Chapter 20.1. Virginia Information Technologies Agency

87 <http://law.lis.virginia.gov/vacode/title2.2/chapter20.1/>The following section documents the

88 statutory authority established in the *Code of Virginia* for the development of minimum
89 specifications and standards for identity proofing and verification. References to statutes
90 below and throughout this document shall be to the *Code of Virginia*, unless otherwise
91 specified.
92

93 **Governing Statutes:**

94

95 **Secretary of Technology**

96 § 2.2-225. Position established; agencies for which responsible; additional powers
97 <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-225>

98

99 **Secretary of Transportation**

100 § 2.2-225. Position established; agencies for which responsible; additional powers
101 <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-225>

102

103 **Identity Management Standards Advisory Council**

104 § 2.2-437. Identity Management Standards Advisory Council
105 <http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/>

106

107 **Commonwealth Identity Management Standards**

108 § 2.2-436. Approval of electronic identity standards
109 <http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/>

110

111 **Electronic Identity Management Act**

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

114

115 **Chief Information Officer (CIO) of the Commonwealth**

116 § 2.2-2007. Powers of the CIO
117 <http://lis.virginia.gov/cgi-bin/legp604.exe?000+cod+2.2-2007>

118

119 **Virginia Information Technologies Agency**

120 § 2.2-2010. Additional powers of VITA
121 <http://lis.virginia.gov/cgi-bin/legp604.exe?000+cod+2.2-2010>

122

123

124

125

126

127 **4 Definitions**

128

129 Terms used in this document comply with definitions in the Public Review version of the
130 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3),

Comment [JG2]: Make sure all terms are either defined in Section 4 or with examples/footnotes within the document. (N. Moe)

131 and align with adopted definitions in § 59.1-550, Code of Virginia (COV), and the
132 Commonwealth of Virginia’s ITRM Glossary (ITRM Glossary).¹

133
134 Active Attack: An online attack where the attacker transmits data to the claimant, credential
135 service provider, verifier, or relying party. Examples of active attacks include man-in-the-
136 middle, impersonation, and session hijacking.

137
138 Address of Record: The official location where an individual can be found. The address of record
139 always includes the residential street address of an individual and may also include the mailing
140 address of the individual. In very limited circumstances, an Army Post Office box number, Fleet
141 Post Office box number or the street address of next of kin or of another contact individual can
142 be used when a residential street address for the individual is not available.

143
144 Approved: Federal Information Processing Standard (FIPS) approved or NIST recommended. An
145 algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2)
146 adopted in a FIPS or NIST Recommendation.

147
148 Applicable Law: Laws, statutes, regulations, and rules of the jurisdiction in which the members
149 of an Identity Trust Framework operates.

150
151 Applicant: A party undergoing the processes of Registration and Identity Proofing.

152
153 Assertion: A statement from a verifier to a relying party (RP) that contains identity information
154 about a subscriber. Assertions may also contain verified attributes.

155
156 Assertion Reference: A data object, created in conjunction with an assertion, which identifies
157 the verifier and includes a pointer to the full assertion held by the verifier.

158
159

¹ 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

160 Assurance: In the context of [OMB M-04-04]² and this document, assurance is defined as 1) the
161 degree of confidence in the vetting process used to establish the identity of an individual to
162 whom the credential was issued, and 2) the degree of confidence that the individual who uses
163 the credential is the individual to whom the credential was issued.

164
165 Assurance Model: Policies, processes, and protocols that define how Assurance will be
166 established in an Identity Trust Framework.

167
168 Asymmetric Keys: Two related keys, a public key and a private key that are used to perform
169 complementary operations, such as encryption and decryption or signature generation and
170 signature verification.

171
172 Attack: An attempt by an unauthorized individual to fool a verifier or a relying party into
173 believing that the unauthorized individual in question is the subscriber.

174
175 Attacker: A party who acts with malicious intent to compromise an Information System.

176
177 Attribute: A claim of a named quality or characteristic inherent in or ascribed to someone or
178 something.

179
180 Authentication: The process of establishing confidence in the identity of users or Information
181 Systems.

182
183 Authentication Protocol: A defined sequence of messages between a claimant and a verifier
184 that demonstrates that the claimant has possession and control of a valid authenticator to
185 establish his/her identity, and optionally, demonstrates to the claimant that he or she is
186 communicating with the intended verifier.

187
188 Authentication Protocol Run: An exchange of messages between a claimant and a verifier that
189 results in authentication (or authentication failure) between the two parties.

190
191 Authentication Secret: A generic term for any secret value that could be used by an attacker to
192 impersonate the subscriber in an authentication protocol. These are further divided into short-
193 term authentication secrets, which are only useful to an attacker for a limited period of time,
194 and long-term authentication secrets, which allow an attacker to impersonate the subscriber
195 until they are manually reset. The authenticator secret is the canonical example of a long term
196 authentication secret, while the authenticator output, if it is different from the authenticator
197 secret, is usually a short term authentication secret.

198

² [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>.

199 Authenticator: Something that the claimant possesses and controls (typically a cryptographic
200 module or password) that is used to authenticate the claimant’s identity. In previous versions of
201 this guideline, this was referred to as a token.

202
203 Authenticator Assurance Level (AAL): A metric describing robustness of the authentication
204 process proving that the claimant is in control of a given subscriber’s authenticator(s).

205
206 Authenticator Output: The output value generated by an authenticator. The ability to generate
207 valid authenticator outputs on demand proves that the claimant possesses and controls the
208 authenticator. Protocol messages sent to the verifier are dependent upon the authenticator
209 output, but they may or may not explicitly contain it.

210
211 Authenticator Secret: The secret value contained within an authenticator.
212 Authenticity: The property that data originated from its purported source.

213
214 Bearer Assertion: An assertion that does not provide a mechanism for the subscriber to prove
215 that he or she is the rightful owner of the assertion. The RP has to assume that the assertion
216 was issued to the subscriber who presents the assertion or the corresponding assertion
217 reference to the RP.

218
219 Bit: A binary digit: 0 or 1.

220
221 Biometrics: Automated recognition of individuals based on their behavioral and biological
222 characteristics. In this document, biometrics may be used to unlock authenticators and prevent
223 repudiation of Registration.

224
225 Certificate Authority (CA): A trusted entity that issues and revokes public key certificates.

226
227 Certificate Revocation List (CRL): A list of revoked public key certificates created and digitally
228 signed by a Certificate Authority. [RFC 5280]³

229
230 Challenge-Response Protocol: An authentication protocol where the verifier sends the claimant
231 a challenge (usually a random value or a nonce) that the claimant combines with a secret (such
232 as by hashing the challenge and a shared secret together, or by applying a private key operation
233 to the challenge) to generate a response that is sent to the verifier. The verifier can
234 independently verify the response generated by the claimant (such as by re-computing the hash
235 of the challenge and the shared secret and comparing to the response, or performing a public
236 key operation on the response) and establish that the claimant possesses and controls the
237 secret.

238
239 Claimant: A party whose identity is to be verified using an authentication protocol.

³ [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>.

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

245
246 Claimed Identity: A declaration by the applicant of their current Personal Name, date of birth
247 and address. [GPG45]⁴

248
249 Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA): An
250 interactive feature added to web-forms to distinguish use of the form by humans as opposed to
251 automated agents. Typically, it requires entering text corresponding to a distorted image or
252 from a sound stream.

253
254 Cookie: A character string, placed in a web browser’s memory, which is available to websites
255 within the same Internet domain as the server that placed them in the web browser.

256
257 Credential: An object or data structure that authoritatively binds an identity (and optionally,
258 additional attributes) to an authenticator possessed and controlled by a subscriber. While
259 common usage often assumes that the credential is maintained by the subscriber, this
260 document also uses the term to refer to electronic records maintained by the CSP which
261 establish a binding between the subscriber’s authenticator(s) and identity.

262
263 Credential Service Provider (CSP): A trusted entity that issues or registers subscriber
264 authenticators and issues electronic credentials to subscribers. The CSP may encompass
265 Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third
266 party, or may issue credentials for its own use.

267
268 Cross Site Request Forgery (CSRF): An attack in which a subscriber who is currently
269 authenticated to an RP and connected through a secure session, browses to an attacker’s
270 website which causes the subscriber to unknowingly invoke unwanted actions at the RP. For
271 example, if a bank website is vulnerable to a CSRF attack, it may be possible for a subscriber to
272 unintentionally authorize a large money transfer, merely by viewing a malicious link in a
273 webmail message while a connection to the bank is open in another browser window.

274
275 Cross Site Scripting (XSS): A vulnerability that allows attackers to inject malicious code into an
276 otherwise benign website. These scripts acquire the permissions of scripts generated by the
277 target website and can therefore compromise the confidentiality and integrity of data transfers

⁴ [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>.

278 between the website and client. Websites are vulnerable if they display user supplied data from
279 requests or forms without sanitizing the data so that it is not executable.
280
281 Cryptographic Key: A value used to control cryptographic operations, such as decryption,
282 encryption, signature generation or signature verification. For the purposes of this document,
283 key requirements shall meet the minimum requirements stated in Table 2 of NIST SP 800-57
284 Part 1. See also Asymmetric keys, Symmetric key.
285
286 Cryptographic Authenticator: An authenticator where the secret is a cryptographic key.
287
288 Data Integrity: The property that data has not been altered by an unauthorized entity.
289
290 Derived Credential: A credential issued based on proof of possession and control of an
291 authenticator associated with a previously issued credential, so as not to duplicate the Identity
292 Proofing process.
293
294 Digital Identity System: An Information System that supports Electronic Authentication and the
295 management of a person’s Identity in a digital environment. [Referenced in § 59.1-550, COV]
296
297 Digital Signature: An asymmetric key operation where the private key is used to digitally sign
298 data and the public key is used to verify the signature. Digital signatures provide authenticity
299 protection, integrity protection, and non-repudiation.
300
301 Eavesdropping Attack: An attack in which an attacker listens passively to the authentication
302 protocol to capture information which can be used in a subsequent active attack to
303 masquerade as the claimant.
304
305 Electronic Authentication: The process of establishing confidence in user identities
306 electronically presented to an Information System.
307
308 Entropy: A measure of the amount of uncertainty that an attacker faces to determine the value
309 of a secret. Entropy is usually stated in bits.
310
311 Extensible Mark-up Language (XML): Extensible Markup Language, abbreviated XML, describes
312 a class of data objects called XML documents and partially describes the behavior of computer
313 programs which process them.
314
315 Federal Bridge Certification Authority (FBCA): The FBCA is the entity operated by the Federal
316 Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI
317 Policy Authority to create, sign, and issue public key certificates to Principal CAs.
318
319 Federal Information Security Management Act (FISMA): Title III of the E-Government Act
320 requiring each federal agency to develop, document, and implement an agency-wide program
321 to provide information security for the information and Information Systems that support the

322 operations and assets of the agency, including those provided or managed by another agency,
323 contractor, or other source.

324 Federal Information Processing Standard (FIPS): Under the Information Technology
325 Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards
326 and guidelines that are developed by the National Institute of Standards and Technology (NIST)
327 for Federal computer systems. These standards and guidelines are issued by NIST as Federal
328 Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when
329 there are compelling Federal government requirements such as for security and interoperability
330 and there are no acceptable industry standards or solutions.⁵

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

333 Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string.
334 Approved hash functions satisfy the following properties:

- 335 • (One-way) It is computationally infeasible to find any input that maps to any pre-
336 specified output, and
- 337 • (Collision resistant) It is computationally infeasible to find any two distinct inputs that
338 map to the same output.

339 Holder-of-Key Assertion: An assertion that contains a reference to a symmetric key or a public
340 key (corresponding to a private key) held by the subscriber. The RP may authenticate the
341 subscriber by verifying that he or she can indeed prove possession and control of the
342 referenced key.

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

344 Identity Assurance Level (IAL): A metric describing degree of confidence that the applicant's
345 claimed identity is their real identity.

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

348 Identity Trust Framework: A Digital Identity System with established identity, security, privacy,
349 technology, and enforcement rules and policies adhered to by certified identity providers that
350 are members of the identity trust framework. Members of an identity trust framework include
351 identity trust framework operators and identity providers. Relying parties may be, but are not
352 required to be, a member of an identity trust framework in order to accept an identity
353 credential issued by a certified identity provider to verify an identity credential holder's
354 identity. [§ 59.1-550, COV]

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

363 Information System: A discrete set of information resources organized for the collection,
364 processing, maintenance, use, sharing, dissemination, or disposition of information. [NIST
365 Interagency/Internal Report (IR) 7298 r. 2]
366

367 Kerberos: A widely used authentication protocol developed at MIT. In “classic” Kerberos, users
368 share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to
369 communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by
370 the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords,
371 the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who
372 capture the initial user-to- KDC exchange. Longer password length and complexity provide
373 some mitigation to this vulnerability, although sufficiently long passwords tend to be
374 cumbersome for users.
375

376 Knowledge Based Authentication: Authentication of an individual based on knowledge of
377 information associated with his or her claimed identity in public databases. Knowledge of such
378 information is considered to be private rather than secret, because it may be used in contexts
379 other than authentication to a verifier, thereby reducing the overall assurance associated with
380 the authentication process.
381

382 Man-in-the-Middle Attack (MitM): An attack on the authentication protocol run in which the
383 attacker positions himself or herself in between the claimant and verifier so that he can
384 intercept and alter data traveling between them.
385

386 Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric
387 key to detect both accidental and intentional modifications of the data. MACs provide
388 authenticity and integrity protection, but not non-repudiation protection.
389

390 Multi-Factor: A characteristic of an authentication system or an authenticator that uses more
391 than one authentication factor. The three types of authentication factors are something you
392 know, something you have, and something you are.
393

394 Network: An open communications medium, typically the Internet, that is used to transport
395 messages between the claimant and other parties. Unless otherwise stated, no assumptions are
396 made about the security of the network; it is assumed to be open and subject to active (i.e.,
397 impersonation, man-in-the-middle, session hijacking) and passive (i.e., eavesdropping) attack at
398 any point between the parties (e.g., claimant, verifier, CSP or RP).
399

400 Nonce: A value used in security protocols that is never repeated with the same key. For
401 example, nonces used as challenges in challenge-response authentication protocols must not
402 be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay
403 attack. Using a nonce as a challenge is a different requirement than a random challenge,
404 because a nonce is not necessarily unpredictable.
405

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

409
410 Online Attack: An attack against an authentication protocol where the attacker either assumes
411 the role of a claimant with a genuine verifier or actively alters the authentication channel.

412
413 Online Guessing Attack: An attack in which an attacker performs repeated logon trials by
414 guessing possible values of the authenticator output.

415
416 Operational Authority: Entity responsible for operations, maintenance, management, and
417 related functions of an Identity Trust Framework.

418
419 Passive Attack: An attack against an authentication protocol where the attacker intercepts data
420 traveling along the network between the claimant and verifier, but does not alter the data (i.e.,
421 eavesdropping).

422
423 Password: A secret that a claimant memorizes and uses to authenticate his or her identity.
424 Passwords are typically character strings.

425
426 Personal Identification Number (PIN): A password consisting only of decimal digits.

427
428 Personal Identity Verification (PIV) Card: Defined by [FIPS 201] as a physical artifact (e.g.,
429 identity card, smart card) issued to federal employees and contractors that contains stored
430 credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that
431 the claimed identity of the cardholder can be verified against the stored credentials by another
432 person (human readable and verifiable) or an automated process (computer readable and
433 verifiable).

434
435 Personally Identifiable Information (PII): As defined by OMB Circular A-130, Personally
436 Identifiable Information means information that can be used to distinguish or trace an
437 individual's identity, either alone or when combined with other information that is linked or
438 linkable to a specific individual.

439
440 Pharming: An attack in which an attacker corrupts an infrastructure service such as DNS
441 (Domain Name Service) causing the subscriber to be misdirected to a forged verifier/RP, which
442 could cause the subscriber to reveal sensitive information, download harmful software or
443 contribute to a fraudulent act.

444
445 Phishing: An attack in which the subscriber is lured (usually through an email) to interact with a
446 counterfeit verifier/RP and tricked into revealing information that can be used to masquerade
447 as that subscriber to the real verifier/RP.

448

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

451

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

455

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

458

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

461

462 Protected Session: A session wherein messages between two participants are encrypted and
463 integrity is protected using a set of shared secrets called session keys. A participant is said to be
464 authenticated if, during the session, he, she or it proves possession of a long term authenticator
465 in addition to the session keys, and if the other party can verify the identity associated with that
466 authenticator. If both participants are authenticated, the protected session is said to be
467 mutually authenticated.

468

469 Pseudonymous Identifier: A meaningless, but unique number that does not allow the RP to
470 infer the subscriber but which does permit the RP to associate multiple interactions with the
471 subscriber's claimed identity.

472

473 Public Credentials: Credentials that describe the binding in a way that does not compromise the
474 authenticator.

475

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

478

479 Public Key Certificate: A digital document issued and digitally signed by the private key of a
480 Certificate authority that binds the name of a subscriber to a public key. The certificate
481 indicates that the subscriber identified in the certificate has sole control and access to the
482 private key. See also [RFC 5280].

483

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

487

488 Registration: The process through which an applicant applies to become a subscriber of a CSP
489 and an RA validates the identity of the applicant on behalf of the CSP.

490

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

494

495 Relying Party (RP): An entity that relies upon the subscriber’s authenticator(s) and credentials
496 or a verifier’s assertion of a claimant’s identity, typically to process a transaction or grant access
497 to information or a system.

498

499 Remote: (As in remote authentication or remote transaction) An information exchange
500 between network-connected devices where the information cannot be reliably protected end-
501 to-end by a single organization’s security controls. Note: Any information exchange across the
502 Internet is considered remote.

503

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

507

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

511

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

514

515 Secondary Authenticator: A temporary secret, issued by the verifier to a successfully
516 authenticated subscriber as part of an assertion protocol. This secret is subsequently used, by
517 the subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer
518 assertions, assertion references, and Kerberos session keys.

519

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

523

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

528

529 SAML Authentication Assertion: A SAML assertion that conveys information from a verifier to
530 an RP about a successful act of authentication that took place between the verifier and a
531 subscriber.

532

533

534 Session Hijack Attack: An attack in which the attacker is able to insert himself or herself
535 between a claimant and a verifier subsequent to a successful authentication exchange between
536 the latter two parties. The attacker is able to pose as a subscriber to the verifier or vice versa to
537 control session data exchange. Sessions between the claimant and the relying party can also be
538 similarly compromised.

539

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

541

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

544

545 Special Publication (SP): A type of publication issued by NIST. Specifically, the Special
546 Publication 800-series reports on the Information Technology Laboratory’s research, guidelines,
547 and outreach efforts in computer security, and its collaborative activities with industry,
548 government, and academic organizations.

549

550 Strongly Bound Credentials: Credentials that describe the binding between a user and
551 authenticator in a tamper-evident fashion.

552

553 Subscriber: A party who has received a credential or authenticator from a CSP.

554

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

558

559 Token: See Authenticator.

560

561 Token Authenticator: See Authenticator Output.

562

563 Token Secret: See Authenticator Secret.

564

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

570

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

574

575 Unverified Name: A subscriber name that is not verified as meaningful by Identity Proofing.

576

577 Valid: In reference to an ID, the quality of not being expired or revoked.

578 Verified Name: A subscriber name that has been verified by Identity Proofing.
579
580 Verifier: An entity that verifies the claimant's identity by verifying the claimant's possession and
581 control of one or two authenticators using an authentication protocol. To do this, the verifier
582 may also need to validate credentials that link the authenticator(s) and identity and check their
583 status.
584
585 Verifier Impersonation Attack: A scenario where the attacker impersonates the verifier in an
586 authentication protocol, usually to capture information that can be used to masquerade as a
587 claimant to the real verifier.
588
589 Virtual In-Person Proofing: A remote identity person proofing process that employs technical
590 and procedural measures that provide sufficient confidence that the remote session can be
591 considered equivalent to a physical, in-person identity proofing encounter. [NIST SP 800-63A]
592
593 Weakly Bound Credentials: Credentials that describe the binding between a user and
594 authenticator in a manner than can be modified without invalidating the credential.
595
596 Zeroize: Overwrite a memory location with data consisting entirely of bits with the value zero
597 so that the data is destroyed and not recoverable. This is often contrasted with deletion
598 methods that merely destroy reference to data within a file system rather than the data itself.
599
600 Zero-knowledge Password Protocol: A password based authentication protocol that allows a
601 claimant to authenticate to a Verifier without revealing the password to the verifier. Examples
602 of such protocols are EKE, SPEKE and SRP.

603 5 Background

604 In 2015, Virginia’s General Assembly passed the Electronic Identity Management Act (Chapter
605 50, Code of Virginia) to address demand in the state’s digital economy for secure, privacy
606 enhancing Electronic Authentication and identity management. Growing numbers of
607 “communities of interest” have advocated for stronger, scalable and interoperable identity
608 solutions to increase consumer protection and reduce liability for principal actors in the identity
609 ecosystem – Identity Providers, Credential Service Providers and Relying Parties.

610 The following guidance document has been developed by the Virginia Information Technologies
611 Agency (VITA), acting on behalf of the Secretary of Technology and Chief Information Officer of
612 the Commonwealth, at the direction of IMSAC. IMSAC was created by the General Assembly as
613 part of the Act and advises the Secretary of Technology on the adoption of identity
614 management standards and the creation of guidance documents pursuant to §2.2-436. A copy
615 of the IMSAC Charter has been provided in **Appendix 1.**

616 The Advisory Council recommends to the Secretary of Technology guidance documents relating
617 to (i) nationally recognized technical and data standards regarding the verification and
618 authentication of identity in digital and online transactions; (ii) the minimum specifications and
619 standards that should be included in an Identity Trust Framework, as defined in §59.1-550, so
620 as to warrant liability protection pursuant to the Electronic Identity Management Act (§59.1-
621 550 et seq.); and (iii) any other related data standards or specifications concerning reliance by
622 third parties on identity credentials, as defined in §59.1-550. The following guidance document
623 has been developed by the Virginia Information Technologies Agency (VITA), acting on behalf of
624 the Secretary of Technology and Chief Information Officer of the Commonwealth, at the
625 direction of IMSAC. IMSAC was created by the General Assembly and advises the Secretary of
626 Technology on the adoption of identity management standards and the creation of guidance
627 documents pursuant to §2.2-436. A copy of the IMSAC Charter has been provided in **Appendix**
628 **1.**

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

641 Purpose Statement

642 The purpose of this document is to establish minimum specifications for Identity Proofing and
643 verification to enable Registration and Electronic Authentication events within a Digital Identity
644 System. The document assumes that the Digital Identity System will be supported by an
645

646 ~~Identity Trust Framework, compliant with Applicable Law.~~⁶ The minimum specifications have
647 ~~been stated based on language in NIST SP 800-63-3.~~
648 ~~The purpose of this document is to establish minimum specifications for identity proofing and~~
649 ~~verification to enable registration and electronic authentication events within a system. The~~
650 ~~document assumes that the identity management system will be supported by a , compliant~~
651 ~~with Applicable Law.~~⁷

652
653 The document defines minimum requirements, components, process flows, ~~levels of~~
654 ~~assurance~~assurance levels, and privacy and security provisions for ~~identity proofing~~Identity
655 ~~Proofing~~Proofing and verification. The document assumes that specific business, legal and technical
656 requirements for ~~identity proofing~~Identity Proofing and verification will be established in the
657 ~~Identity Trust Framework~~Identity Trust Framework for each distinct ~~identity management system~~Digital Identity System,
658 ~~and that these requirements will be designed based on the Identity Assurance Level (IAL) and~~
659 ~~Authenticator Assurance Level (AAL) requirements for the system and that these requirements~~
660 ~~will be designed based on the specific model supported by the system.~~

661
662 The document limits its focus to ~~identity proofing~~Proofing and verification. Minimum
663 specifications for other components of ~~an identity management a system~~Digital Identity System
664 ~~will be have been~~ defined in separate IMSAC guidance documents in this series, pursuant to
665 §2.2-436 and §2.2-437.
666

⁶ ~~For the purpose of this guidance document, the term “Applicable Law” shall mean laws, statutes, regulations and rules of the jurisdiction in which each member of an Identity Trust Framework operates.~~

⁷ ~~For the purpose of this guidance document, the term “Applicable Law” shall mean laws, statutes, regulations, and rules of the jurisdiction in which the member of an Identity Trust Framework operates. For the purpose of this guidance document, the term “Applicable Law” shall mean laws, statutes, regulations and rules of the jurisdiction in which each of a system operates.~~

667 6 Minimum Specifications

668 ~~National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3)~~
 669 ~~defines “Electronic Authentication” as “the process of establishing confidence in user identities~~
 670 ~~electronically presented to an Information System.”⁸ Information Systems may use the~~
 671 ~~authenticated identity to determine if that user is authorized to perform an electronic~~
 672 ~~transaction.~~ ~~National Institute of Standards and Technology Special Publication 800-63-2 (NIST~~
 673 ~~SP 800-63-2) defines “electronic authentication” (e-authentication) as “the process of~~
 674 ~~establishing confidence in user identities electronically presented to an information system.”⁹~~
 675 ~~Information systems may use the authenticated identity to determine if that user is authorized~~
 676 ~~to perform an electronic transaction.~~

677 ~~E-a~~ ~~Electronic Authentication begins with registration~~Registration (also referred to as
 679 ~~enrollment).~~ The Registration process involves an Applicant applying to a CSP. If approved, the
 680 ~~CSP creates a Credential and binds it to one or more Authenticators. The Credential includes an~~
 681 ~~identifier, which can be pseudonymous, and one or more Attributes that the CSP has verified.~~
 682 ~~The Authenticators may be issued by the CSP, generated/provided directly by the Subscriber, or~~
 683 ~~provided by a third party. The Authenticator and Credential may be used in subsequent~~
 684 ~~authentication events~~Registration generally consists of an Applicant applying to a Registration
 685 ~~Authority (RA) to become a Subscriber of a Credential Service Provider (CSP). The first step in~~
 686 ~~the registration process involves identity proofing and verification of the Applicant by the RA.~~
 687 ~~This process assumes a trusted relationship between the RA and CSP, with specific~~
 688 ~~requirements for registration documented in the governing for the identity management~~
 689 ~~system.~~

690
 691
 692 ~~The process used to verify an Applicant’s association with their real world identity is called~~
 693 ~~Identity Proofing. The strength of Identity Proofing is described by a categorization called the~~
 694 ~~Identity Assurance Level (IAL, see subsection on Assurance Level Model below in this~~
 695 ~~document).~~

696
 697 This document establishes minimum specifications for the ~~identity proofing~~Identity Proofing
 698 and verification components of a trust-based ~~registration~~Registration process. ~~Identity Trust~~
 699 ~~Frameworks~~ for ~~identity management system~~Digital Identity Systems should document the
 700 business, legal and technical requirements for these components, as well as requirements for
 701 the remaining components of the system. Subsequent guidance documents in the IMSAC series
 702 will address other components of an ~~identity management system~~Digital Identity System,
 703 pursuant to §2.2-436 and §2.2-437.

Formatted: Font: Not Italic

⁸ ~~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.~~

⁹ ~~National Institute of Standards and Technology Special Publication 800-63-2 (NIST SP 800-63-2) may be accessed at <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>~~

704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741

~~Identity Proofing~~ Identity Proofing Requirements

~~Identity proofing~~ Identity Proofing and verification for ~~registration~~ Registration should be designed to meet the specific requirements for each ~~assurance level~~ defined by the governing ~~Identity Trust Framework~~ for the ~~identity management system~~ Digital Identity System.⁴⁰ A trusted ~~registration~~ Registration process ensures that (i) the RA and CSP have established the true ~~identity~~ Identity of the Applicant, (ii) the ~~registration~~ Registration protocols satisfy the requirements for each ~~assurance level~~, (iii) the RA and CSP maintain a record of the ~~identity evidence and transaction flows to meet audit and compliance requirements~~, and (iv) the RA and CSP implement enforcement mechanisms to ensure compliance with all applicable provisions established in the ~~Identity Trust Framework~~.

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

- A person with the Applicant’s claimed attributes exists, and those attributes are sufficient to uniquely identify a single person;
- The Applicant whose ~~token~~ Authenticator is registered is in fact the person who is entitled to the ~~identity~~ Identity;
- It is difficult for the Claimant to later repudiate the ~~registration~~ Registration and dispute an authentication using the Subscriber’s ~~token~~ Authenticator.

Registration, and the associated ~~identity proofing~~ Identity Proofing and verification processes, may be completed through ~~remote~~ Remote or in-person protocols. Provisions for ~~remote~~ Remote versus in-person ~~identity proofing~~ Identity Proofing and verification should be established in the ~~Identity Trust Framework~~ for the ~~identity management system~~ Digital Identity System and satisfy applicable requirements of the applicable Assurance Model.

Components and Process Flow

The ~~registration~~ Registration process, during which ~~identity proofing~~ Identity Proofing and verification protocols are invoked, generally involve the following components:

- The Applicant’s assertion of an ~~Identity Claim~~ identity claim
- The Applicant’s presentation of evidence to prove the existence of the claimed ~~identity~~ identity
- The RA’s review and validation of the Applicant’s ~~Identity Claim~~ identity claim and supporting evidence

Comment [JG3]: Add language regarding maintenance of the record of the identity evidence. (M. Watson)

Comment [JG4]: Should there be a statement regarding enforcement? (L. Kimball)
Add a placeholder for enforcement. (T. Moran)

Formatted: List Paragraph, Indent: Left: 0", Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

⁴⁰ The term “Level of Assurance” has been used in this document to describe the continuum for the degree of certainty in the user’s identity established by the RA during the ~~registration~~ Registration process. The term aligns with the levels defined for federal agencies in the U.S. Office of Management and Budget Memorandum M04-04 and NIST SP 800-63-2 (i.e., Levels 1-4) but provides for a more general framework to accommodate other ~~identity management standards and protocols~~.

- 742 • The CSP’s verification of the Applicant’s ~~Identity Claim~~identity claim
743 • The CSP’s issuance or ~~registration~~Registration of a ~~credential~~Credential bound to the
744 Applicant’s ~~identity~~Authenticator~~token~~

745
746 The process flow for implementing the components of the ~~identity proofing~~Identity Proofing
747 and verification for ~~registration~~Registration generally consists of the following (Figure 1):

- 748 1. The Applicant asserts to the trusted RA an ~~Identity Claim~~identity claim at a specified
749 ~~assurance level~~(~~Identity Claim~~)
750 2. The Applicant provides the RA either ~~remotely~~Remotely or in person, depending on ~~the~~
751 ~~Assurance Model requirements of the Identity Trust Framework requirements~~, evidence to
752 prove the existence of the claimed identity (~~Identity Proofing~~Identity Proofing) ~~Note: Source~~
753 ~~of original identity document(s) must meet the Assurance Model and related compliance~~
754 ~~requirements set by the RA and defined in the Identity Trust Framework~~
755 3. The RA transmits the ~~Identity Proofing~~Identity Proofing evidence to the CSP to verify
756 whether the evidence may be considered valid (Identity Validation)
757 4. The CSP compares the Applicant’s ~~Identity Claim~~identity claim to information associated
758 with the ~~Identity Claim~~identity claim to determine whether it relates to the Applicant
759 (Attribute Verification)¹¹
760

Comment [JG5]: Add a requirement statement regarding the source of the initial document. (M. Watson, K. Crepps, L. Kimball)

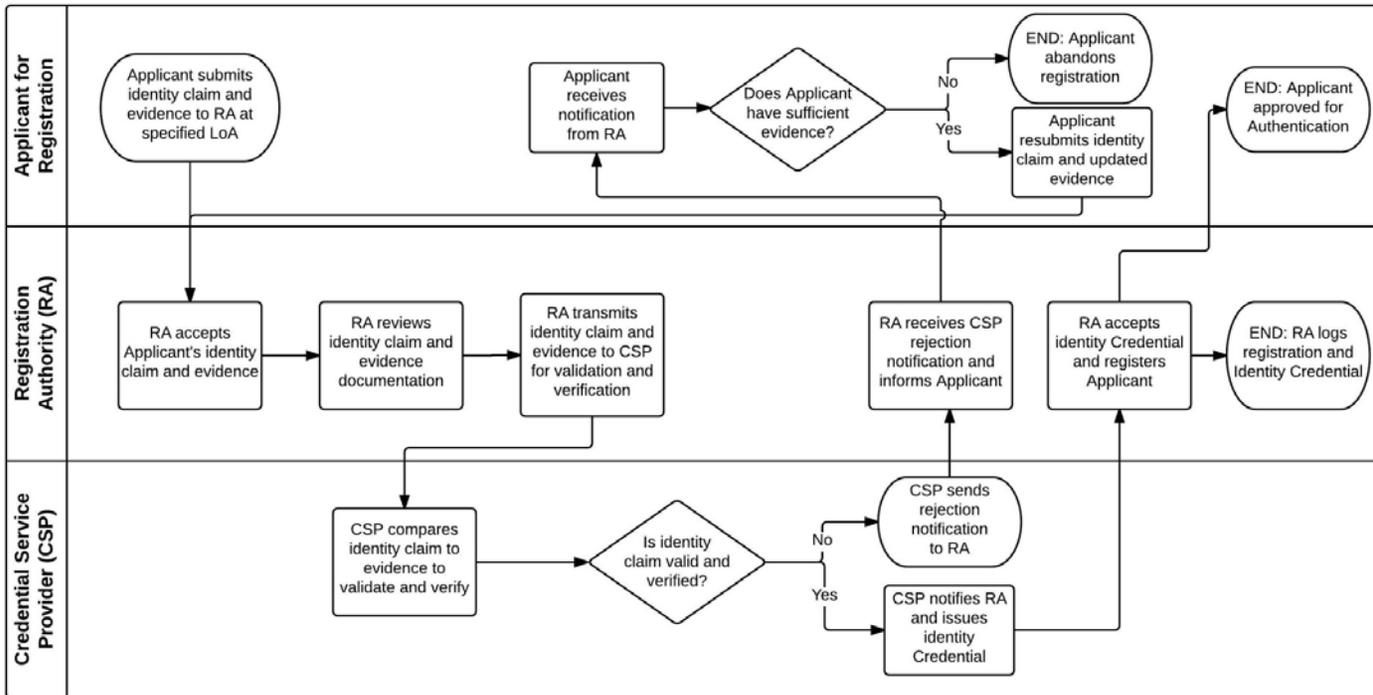
¹¹ The Attribute Verification process may consist of multiple steps and factors, including attribute information, knowledge-based tests, biometrics, activity history, counter-fraud checks, etc., depending on ~~the Assurance Model~~ requirements ~~established in the Identity Trust Framework~~. Specific Attribute Verification requirements should be defined in the governing ~~Identity Trust Framework~~ for the ~~identity management system~~Digital Identity System. Minimum specifications for Attribute Verification will be addressed in a forthcoming guidance document in the IMSAC series, pursuant to §2.2-436 and §2.2-437.

761 5. Upon successful completion of the Attribute Verification process, the CSP issues to the RA a
762 ~~credential~~Credential bound to a ~~token~~Authenticator for the Applicant, confirming the
763 Applicant's ~~Identity Claim~~identity claim at the appropriate assurance level defined in the
764 Identity Trust Framework for the Digital Identity System (~~Credential Issuance or~~
765 ~~Registration~~)
766 ~~5-6.~~ RA maintains a record of the evidence and transaction for the Registration ~~process~~.

Comment [JG6]: Add language re maintenance of identity evidence. (M. Watson)

DRAFT

Figure 1. Identity Proofing and Verification Process Flow



1 **Levels of Assurance**

2
3 The minimum specifications established in this document for identity proofing and verification
4 assume that s for identity management systems will define a specific model. Therefore, the
5 Level of Assurance (LoA) Model presented below should be viewed as a recommended
6 framework for identity proofing and verification in a registration process. The LoA Model aligns
7 with the Assurance Level Model published by the National Association of State Chief
8 Information Officers (NASCIO) in its State Identity Credential and Access Management (SICAM)
9 Guidance, with OMB M04-04 and NIST SP 800-63.⁴²

10 **Level of Assurance 1**

11 LoA 1 has no identity proofing or verification requirement. Identity proofing and verification
12 protocols at LoA 1 provide only minimal assurance that the same Applicant is completing the
13 registration process.

14
15 Plaintext passwords or secrets are not transmitted across a network at LoA 1. However, this
16 level does not require cryptographic methods that block offline attacks by an eavesdropper. For
17 example, simple password challenge response protocols are allowed. At LoA 1, long-term
18 shared authentication secrets may be revealed to verifiers. Assertions issued about Applicants
19 as a result of a successful identity proofing and verification are either cryptographically
20 authenticated by Relying Parties (using approved methods), or are obtained directly from a
21 trusted party via a secure registration protocol.

22
23 **Level of Assurance 2**

24 LoA 2 allows identity proofing and verification through a single factor remote network. At this
25 level, identity proofing and verification requirements are introduced, prompting the Applicant
26 to present identifying materials or information. A range of identity proofing and verification
27 technologies can be employed at LoA 2. This level allows any of the token methods of LoAs 3 or
28 4, as well as passwords and PINs. Successful identity proofing and verification requires the
29 Applicant to demonstrate control of the identity token through a secure registration protocol.

30
31 Long-term shared authentication secrets, if used, are never revealed to any party except the
32 Applicant and verifiers operated by the CSP; however, session (temporary) shared secrets may
33 be provided to independent verifiers by the CSP. Approved cryptographic techniques are
34 required. Assertions issued about Applicants as a result of a successful identity proofing and
35 verification are either cryptographically authenticated by Relying Parties (using approved
36 methods), or are obtained directly from a trusted party via a secure registration protocol.

⁴² -The Assurance Level Model published by NASCIO in its SICAM Guidance and Roadmap may be accessed at <http://www.nascio.org/Portals/0/Publications/Documents/SICAM.pdf>.

Level of Assurance 3

Multi-factor remote network identity proofing and verification supported at this level. Identity proofing and verification procedures at LoA 3 require verification of identifying materials and information. LoA 3 is based on proof of possession of a key or a one-time password through a cryptographic protocol. Identity proofing and verification at this level requires cryptographic strength mechanisms that protect the primary identity token. A minimum of two Attribute Verification factors is required. While tokens may evolve, there are currently three kinds of tokens that may be used: “soft” cryptographic tokens, “hard” cryptographic tokens and “one-time password” device tokens.

LoA 3 requires that the Applicant prove through secure identity proofing and verification protocols that he or she controls the token, and must first unlock the token with a password or biometric, or must also use a password in a secure protocol, to establish two factor authentication. Long-term shared authentication secrets, if used, are never revealed to any party except the Applicant and verifiers operated directly by the CSP; however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are used for all operations. Assertions issued about Applicants as a result of a successful identity proofing and verification are either cryptographically authenticated by Relying Parties (using approved methods), or are obtained directly from a trusted party via secure registration protocols.

Level of Assurance 4

Highest practical remote network identity proofing and verification provided at this level. LoA 4 protocols are based on proof of possession of a key through a cryptographic protocol. LoA 4 is similar to LoA 3 except that only “hard” cryptographic tokens are required, Federal Information Processing Standard (FIPS) 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token must be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security.⁴³ By requiring a physical token, which cannot readily be copied and because FIPS 140-2 requires operator authentication at LoA 2 and higher, LoA 4 ensures strong, two-factor authentication.

LoA 4 requires strong cryptographic identity proofing and verification among all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used, as are biometrics. Registration requires that the Applicant prove through a secure authentication protocol that he or she controls the token. Long-term shared authentication secrets, if used, are never revealed to any party except the Applicant and verifiers operated directly by the CSP; however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Compliant cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the registration process.

⁴³ -Federal Information Processing Standard (FIPS) 140-2 may be accessed at <http://csrc.nist.gov/groups/STM/cmvp/standards.html>

Assurance Model

The minimum specifications defined in this document for Electronic Authentication assume that the Identity Trust Framework for a Digital Identity System will define a specific assurance model for that system.¹⁴ Therefore, the assurance model presented below, which is based on NIST SP 800-63-3, should be viewed as a recommended framework for Electronic Authentication. Other assurance models have been established in OMB M-04-04 and the State Identity, Credential, and Access Management (SICAM) guidelines, published by the National Association of Chief Information Officers (NASCIO). A crosswalk showing disparities in the NIST SP 800-63-3, OMB M-04-04, and SICAM assurance models has been provided in **Figure 2**.

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

Identity Assurance Level 2 – IAL 2 introduces the need for either remote or in-person Identity Proofing. IAL 2 requires identifying attributes to have been verified in person or remotely using, at a minimum, the procedures given in NIST 800-63A.

Identity Assurance Level 3 – At IAL 3, in-person Identity Proofing is required. Identifying attributes must be verified by an authorized representative of the CSP through examination of physical documentation as described in NIST 800-63A.

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

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

¹⁴ 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.

¹⁵ Approved cryptographic techniques shall be FIPS approved, NIST recommended, or otherwise compliant with Commonwealth IT Information Security Standard (SECS01): http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/HostedEnvironmentInformationSecurityStandardSECS2501.pdf

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

124 **Figure 2. Assurance Model Crosswalk**

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

127

128 Privacy and Security

129

130 The minimum specifications established in this document for privacy and security in the use of
 131 person information for ~~identity proofing~~Identity Proofing and verification apply the Fair
 132 Information Practice Principles (FIPPs).¹⁶ The FIPPs have been endorsed by the National
 133 Strategy for Trusted Identities in Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.¹⁷

134

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

138

139 The minimum specifications for ~~identity proofing~~Identity Proofing and verification apply the
 140 following FIPPs:

141

- 142 • Transparency: RAs and CSPs should be transparent and provide notice to Applicants
 143 regarding collection, use, dissemination, and maintenance of person information required
 144 during the ~~registration~~Registration, ~~identity proofing~~Identity Proofing and verification
 145 processes.
- 146 • Individual Participation: RAs and CSPs should involve the Applicant in the process of using
 147 person information and, to the extent practicable, seek consent for the collection, use,
 148 dissemination, and maintenance of that information. RAs and CSPs also should provide
 149 mechanisms for appropriate access, correction, and redress of person information.
- 150 • Purpose Specification: RAs and CSPs should specifically articulate the authority that permits
 151 the collection of person information and specifically articulate the purpose or purposes for
 152 which the information is intended to be used.
- 153 • Data Minimization: RAs and CSPs should collect only the person information directly
 154 relevant and necessary to accomplish the ~~registration~~Registration and related processes,
 155 and only retain that information for as long as necessary to fulfill the specified purpose.
- 156 • Use Limitation/Minimal Disclosure: RAs and CSPs should use person information solely for
 157 the purpose specified in the notice. Disclosure or sharing that information should be limited
 158 to the specific purpose for which the information was collected.
- 159 • Data Quality and Integrity: RAs and CSPs should, to the extent practicable, ensure that
 160 person information is accurate, relevant, timely, and complete.
- 161 • Security: RAs and CSPs should protect personal information through appropriate security
 162 safeguards against risks such as loss, unauthorized access or use, destruction, modification,
 or unintended or inappropriate disclosure.

Comment [JG7]: Should language for FIPPs be changed from “should” to “shall” or “must?” (L. Kimball)
 Should IDESG IDEF Privacy and Security Requirements be included here? (J. Grant)
 Keep FIPPs but incorporate IDEF requirements, as directed by IMSAC members (J. Grubbs)

Comment [JG8]: FIPPs kept, as published. IDESG IDEF Requirements added as Appendix 2.

¹⁶ 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 ~~identity management system~~Digital Identity System.

¹⁷ 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>.

- 163 • Accountability and Auditing: RAs and CSPs should be accountable for complying with these
164 principles, providing training to all employees and contractors who use person information,
165 and auditing the actual use of person information to demonstrate compliance with these
166 principles and all applicable privacy protection requirements.

167 7 Alignment Comparison

168
169 The minimum specifications for ~~identity proofing~~Identity Proofing and verification established
170 in this document have been developed to align with existing national and international
171 standards for e-authentication and identity management. Specifically, the minimum
172 specifications reflect basic requirements set forth in national standards at the federal and state
173 level, ensuring compliance while accommodating other identity management standards and
174 protocols. This document assumes that each ~~system~~Digital Identity System and supporting
175 Identity Trust Framework will comply with those governing standards and protocols required by
176 Applicable Law.

177
178 The following section outlines the alignment and disparities between the minimum
179 specifications in this document and core national standards. A crosswalk documenting the
180 alignment and areas of misalignment has been provided in **Appendix 3**.

182 NIST SP 800-63-23

183
184 The minimum specifications in this document conform with the basic requirements for
185 Electronic Authentication set forth in NIST SP 800-63-3 (Public Review version). However, as
186 the NIST guidance defines specific requirements for federal agencies, the minimum
187 specifications in this document provide flexibility for Digital Identity Systems across industries in
188 the private sector and levels of governance. This flexibility enables Digital Identity Systems to
189 adhere to the specifications but do so in a manner appropriate and compliant with their
190 governing Identity Trust Frameworks~~The minimum specifications in this document conform~~
191 ~~with the basic requirements for identity proofing and verification set forth in NIST SP 800-63-2.~~
192 ~~However, as the NIST guidance defines specific requirements for federal agencies, the minimum~~
193 ~~specifications in this document provide flexibility for systems across industries in the private~~
194 ~~sector and levels of governance. This flexibility enables identity management systems to~~
195 ~~adhere to the specifications but do so in a manner appropriate and compliant with their~~
196 ~~governing s.~~

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

199
200 The minimum specifications in this document conform with the basic requirements for ~~identity~~
201 ~~proofing~~Identity Proofing and verification set forth by NASCIO in the SICAM Guidance and
202 Roadmap. The NASCIO guidance defines specific requirements for state agencies. Similar to the
203 contrast with the NIST guidance for federal agencies, the minimum specifications in this

204 | document provide flexibility for ~~-system~~Digital Identity System~~s~~ across industries in the private
205 | sector and levels of governance.

206

207 | IDESG Identity Ecosystem Framework (IDEF) Functional Model

208

209 | The minimum specifications in this document conform with the core operations and basic
210 | requirements for privacy and security set forth by IDESG in the IDEF Functional Model and
211 | Baseline Functional Requirements. The IDESG/IDEF requirements apply the FIPPs but extend
212 | them to cover the Guiding Principles of the National Strategy for Trusted Identities in
213 | Cyberspace (NSTIC). The minimum specifications in this document encourage adherence to the
214 | IDEF Functional Model, Baseline Functional Requirements and the NSTIC Guiding Principles.
215

DRAFT

216 Appendix 1. IMSAC Charter

217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257

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

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

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

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

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

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

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

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

260
261 The statutory authority and requirements for public notice and comment periods for guidance
262 documents have been established pursuant to § 2.2-437.C, as follows:

263
264 C. Proposed guidance documents and general opportunity for oral or written submittals as to
265 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published
266 in the Virginia Register of Regulations as a general notice following the processes and
267 procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§
268 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written
269 comments following the posting and publication and shall hold at least one meeting dedicated
270 to the receipt of oral comment no less than 15 days after the posting and publication. The
271 Advisory Council shall also develop methods for the identification and notification of interested
272 parties and specific means of seeking input from interested persons and groups. The Advisory
273 Council shall send a copy of such notices, comments, and other background material relative to
274 the development of the recommended guidance documents to the Joint Commission on
275 Administrative Rules.

276
277
278 This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the
279 minutes of the meeting and related IMSAC documents, visit:
280 <https://vita.virginia.gov/About/default.aspx?id=6442474173>

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

283 PRIVACY-1. DATA MINIMIZATION

284 Entities MUST limit the collection, use, transmission and storage of personal information to the
285 minimum necessary to fulfill that transaction’s purpose and related legal requirements. Entities
286 providing claims or attributes MUST NOT provide any more personal information than what is
287 requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to
288 accommodate information requests of variable granularity, to support data minimization.

290 PRIVACY-2. PURPOSE LIMITATION

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

297 PRIVACY-3. ATTRIBUTE MINIMIZATION

298 Entities requesting attributes MUST evaluate the need to collect specific attributes in a
299 transaction, as opposed to claims regarding those attributes. Wherever feasible, entities MUST
300 collect, generate, use, transmit, and store claims about USERS rather than attributes. Wherever
301 feasible, attributes MUST be transmitted as claims, and transmitted credentials and identities
302 MUST be bound to claims instead of actual attribute values.

304 PRIVACY-4. CREDENTIAL LIMITATION

305 Entities MUST NOT request USERS’ credentials unless necessary for the transaction and then
306 only as appropriate to the risk associated with the transaction or to the risks to the parties
307 associated with the transaction.

309 PRIVACY-5. DATA AGGREGATION RISK

310 Entities MUST assess the privacy risk of aggregating personal information, in systems and
311 processes where it is collected, generated, used, transmitted, or stored, and wherever feasible,
312 MUST design and operate their systems and processes to minimize that risk. Entities MUST
313 assess and limit linkages of personal information across multiple transactions without the
314 USER’s explicit consent.

316 PRIVACY-6. USAGE NOTICE

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

320 PRIVACY-7. USER DATA CONTROL

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

324 PRIVACY-8. THIRD-PARTY LIMITATIONS

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

328
329 PRIVACY-9. USER NOTICE OF CHANGES

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

335
336 PRIVACY-10. USER OPTION TO DECLINE

337 USERS MUST have the opportunity to decline Registration; decline credential provisioning;
338 decline the presentation of their credentials; and decline release of their attributes or claims.

339
340 PRIVACY-11. OPTIONAL INFORMATION

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

343
344 PRIVACY-12. ANONYMITY

345 Wherever feasible, entities MUST utilize identity systems and processes that enable
346 transactions that are anonymous, anonymous with validated attributes, pseudonymous, or
347 where appropriate, uniquely identified. Where applicable to such transactions, entities
348 employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES
349 collecting USER personal information. Organizations MUST request individuals' credentials only
350 when necessary for the transaction and then only as appropriate to the risk associated with the
351 transaction or only as appropriate to the risks to the parties associated with the transaction.

352
353 PRIVACY-13. CONTROLS PROPORTIONATE TO RISK

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

358
359 PRIVACY-14. DATA RETENTION AND DISPOSAL

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

365
366 PRIVACY-15. ATTRIBUTE SEGREGATION

367 Wherever feasible, identifier data MUST be segregated from attribute data.

368 SECURE-1. SECURITY PRACTICES

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

371
372 SECURE-2. DATA INTEGRITY

373 Entities MUST implement industry-accepted practices to protect the confidentiality and
374 integrity of identity data—including authentication data and attribute values—during the
375 execution of all digital identity management functions, and across the entire data lifecycle
376 (collection through destruction).

377
378 SECURE-3. CREDENTIAL REPRODUCTION

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

381
382 SECURE-4. CREDENTIAL PROTECTION

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

386
387 SECURE-5. CREDENTIAL ISSUANCE

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

393
394 SECURE-6. CREDENTIAL UNIQUENESS

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

397
398 SECURE-7. TOKEN CONTROL

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

401
402 SECURE-8. MULTIFACTOR AUTHENTICATION

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

405
406 SECURE-9. AUTHENTICATION RISK ASSESSMENT

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

409
410
411

412 SECURE-10. UPTIME

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

416 SECURE-11. KEY MANAGEMENT

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

419 SECURE-12. RECOVERY AND REISSUANCE

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

423 SECURE-13. REVOCATION

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

426 SECURE-14. SECURITY LOGS

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

431 SECURE-15. SECURITY AUDITS

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

441

Appendix 3. Identity Proofing Standards Alignment Comparison Matrix

Comment [JG9]: Document alignment and lack of alignment; single table. (M. Watson, K. Crepps)

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