

COMMONWEALTH OF VIRGINIA



IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

GUIDANCE DOCUMENT Identity Proofing and Verification

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 24

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
1.0	05/02/2016	Document revised by IMSAC at public workshop
1.0	06/23/2016	Document revised by VITA staff based on comments from IMSAC during May 2, 2016, public workshop
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

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 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. 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 the response shown in brackets []:
 - 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]

- 30 ○ On pages 21 and 22 under discussions of Level of Assurance 2, 3, and 4, add
31 references to "virtual in-person proofing" as an approved method consistent
32 with draft 800-63A. [The Assurance Model in this document has been amended
33 to be consistent with the Public Review version of NIST SP 800-63-3. A definition
34 for "virtual in-person proofing" based on NIST SP 800-63A has been added to this
35 document.]
- 36 ○ On page 15, add a definition of "virtual in-person proofing" perhaps based on
37 section 5.4.3 of draft 800-63A. [A definition for "virtual in-person proofing" has
38 been added to this document, consistent with NIST SP 800-63A.]
- 39 ○ On page 12, add a definition of "remote network identity proofing." This could
40 be modeled after language contained in NIST 800-63 series documents. [The
41 term "remote network identity proofing" has not been defined in the NIST SP
42 800-63 document series. However, the term "Remote" has been defined in the
43 NIST SP 800-63 document series and in this document, and the definition covers
44 remote transactions across a network in an identity proofing context.]
- 45
- 46 ● The document will be reviewed in a manner compliant with the Commonwealth of Virginia's
47 Administrative Process Act, § 2.2-4000 et seq.
48

49 3 Purpose and Scope

50 Pursuant to § 2.2-436 and § 2.2-437, *Code of Virginia*, this guidance document was developed
51 by the Identity Management Standards Advisory Council (IMSAC), on behalf of the Secretary of
52 Technology, to establish minimum specifications for Digital Identity Systems so as to warrant
53 liability protection pursuant to the Electronic Identity Management Act ("the Act"), Chapter 50
54 of Title 59.1. The guidance document, as defined in § 2.2-4001, was prepared to provide
55 information or guidance of general applicability to the public for interpreting or implementing
56 the Act. The guidance document was not developed as a Commonwealth of Virginia
57 Information Technology Resource Management (ITRM) Policy, Standard, and Guideline,
58 pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive
59 branch agencies of the Commonwealth of Virginia.
60
61

62 4 Statutory Authority

63
64 The following section documents the statutory authority established in the *Code of Virginia* for
65 the development of minimum specifications and standards for Identity Proofing and verification
66 within a Digital Identity System. References to statutes below and throughout this document
67 shall be to the *Code of Virginia*, unless otherwise specified.
68

69 Governing Statutes:

70

71 Secretary of Technology

72 § 2.2-225. Position established; agencies for which responsible; additional powers

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

74

75 Identity Management Standards Advisory Council

76 § 2.2-437. Identity Management Standards Advisory Council

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

78

79 Commonwealth Identity Management Standards

80 § 2.2-436. Approval of electronic identity standards

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

82

83 Electronic Identity Management Act

84 Chapter 50 of Title 59.1 Electronic Identity Management Act

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

86

87

88

89

90

91

92

93 5 Definitions

94

95 Terms used in this document comply with definitions in the Public Review version of the
96 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3),
97 and align with adopted definitions in § 59.1-550, *Code of Virginia* (COV), and the
98 Commonwealth of Virginia's ITRM Glossary (ITRM Glossary).¹

99

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

103

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

109

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

113

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

116

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

118

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

121

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

124

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

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

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>.

- 129 Assurance Model: Policies, processes, and protocols that define how Assurance will be
130 established in an Identity Trust Framework.
- 131
- 132 Asymmetric Keys: Two related keys, a public key and a private key that are used to perform
133 complementary operations, such as encryption and decryption or signature generation and
134 signature verification.
- 135
- 136 Attack: An attempt by an unauthorized individual to fool a verifier or a relying Participant into
137 believing that the unauthorized individual in question is the Subscriber.
- 138
- 139 Attacker: A Participant who acts with malicious intent to compromise an Information System.
- 140
- 141 Attribute: A claim of a named quality or characteristic inherent in or ascribed to someone or
142 something.
- 143
- 144 Authentication: The process of establishing confidence in the identity of users or Information
145 Systems.
- 146
- 147 Authentication Protocol: A defined sequence of messages between a claimant and a verifier
148 that demonstrates that the claimant has possession and control of a valid authenticator to
149 establish his/her identity, and optionally, demonstrates to the claimant that he or she is
150 communicating with the intended verifier.
- 151
- 152 Authentication Protocol Run: An exchange of messages between a claimant and a verifier that
153 results in authentication (or authentication failure) between the two Participants.
- 154
- 155 Authentication Secret: A generic term for any secret value that could be used by an attacker to
156 impersonate the Subscriber in an authentication protocol. These are further divided into short-
157 term authentication secrets, which are only useful to an attacker for a limited period of time,
158 and long-term authentication secrets, which allow an attacker to impersonate the Subscriber
159 until they are manually reset. The authenticator secret is the canonical example of a long term
160 authentication secret, while the authenticator output, if it is different from the authenticator
161 secret, is usually a short term authentication secret.
- 162
- 163 Authenticator: Something that the claimant possesses and controls (typically a cryptographic
164 module or password) that is used to authenticate the claimant's identity. In previous versions of
165 this guideline, this was referred to as a token.
- 166
- 167 Authenticator Assurance Level (AAL): A metric describing robustness of the authentication
168 process proving that the claimant is in control of a given Subscriber's authenticator(s).
- 169
- 170 Authenticator Output: The output value generated by an authenticator. The ability to generate
171 valid authenticator outputs on demand proves that the claimant possesses and controls the

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

174

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

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

177

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

182

183 Bit: A binary digit: 0 or 1.

184

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

188

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

190

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

193

194 Challenge-Response Protocol: An authentication protocol where the verifier sends the claimant
195 a challenge (usually a random value or a nonce) that the claimant combines with a secret (such
196 as by hashing the challenge and a shared secret together, or by applying a private key operation
197 to the challenge) to generate a response that is sent to the verifier. The verifier can
198 independently verify the response generated by the claimant (such as by re-computing the hash
199 of the challenge and the shared secret and comparing to the response, or performing a public
200 key operation on the response) and establish that the claimant possesses and controls the
201 secret.

202

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

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

209

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

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>.

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

216

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

219

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

225

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

230

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

237

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

243

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

248

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

250

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>.

251 Data Integrity: The property that data has not been altered by an unauthorized entity.
252

253 Derived Credential: A credential issued based on proof of possession and control of an
254 authenticator associated with a previously issued credential, so as not to duplicate the Identity
255 Proofing process.
256

257 Digital Identity System: An Information System that supports Electronic Authentication and the
258 management of a person's Identity in a digital environment. [Referenced in § 59.1-550, COV]
259

260 Digital Signature: An asymmetric key operation where the private key is used to digitally sign
261 data and the public key is used to verify the signature. Digital signatures provide authenticity
262 protection, integrity protection, and non-repudiation.
263

264 Eavesdropping Attack: An attack in which an attacker listens passively to the authentication
265 protocol to capture information which can be used in a subsequent active attack to
266 masquerade as the claimant.
267

268 Electronic Authentication: The process of establishing confidence in user identities
269 electronically presented to an Information System.
270

271 Entropy: A measure of the amount of uncertainty that an attacker faces to determine the value
272 of a secret. Entropy is usually stated in bits.
273

274 Extensible Mark-up Language (XML): Extensible Markup Language, abbreviated XML, describes
275 a class of data objects called XML documents and partially describes the behavior of computer
276 programs which process them.
277

278 Federal Bridge Certification Authority (FBCA): The FBCA is the entity operated by the Federal
279 Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI
280 Policy Authority to create, sign, and issue public key certificates to Principal CAs.
281

282 Federal Information Security Management Act (FISMA): Title III of the E-Government Act
283 requiring each federal agency to develop, document, and implement an agency-wide program
284 to provide information security for the information and Information Systems that support the
285 operations and assets of the agency, including those provided or managed by another agency,
286 contractor, or other source.
287

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

293 there are compelling Federal government requirements such as for security and interoperability
294 and there are no acceptable industry standards or solutions.⁵

295

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

299

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

302

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

304 Approved hash functions satisfy the following properties:

- 305 • (One-way) It is computationally infeasible to find any input that maps to any pre-
306 specified output, and
- 307 • (Collision resistant) It is computationally infeasible to find any two distinct inputs that
308 map to the same output.

309

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

314

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

316

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

319

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

322

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

326

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

334

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

335 Information System: A discrete set of information resources organized for the collection,
336 processing, maintenance, use, sharing, dissemination, or disposition of information. [NIST
337 Interagency/Internal Report (IR) 7298 r. 2]
338

339 Kerberos: A widely used authentication protocol developed at MIT. In “classic” Kerberos, users
340 share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to
341 communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by
342 the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords,
343 the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who
344 capture the initial user-to- KDC exchange. Longer password length and complexity provide
345 some mitigation to this vulnerability, although sufficiently long passwords tend to be
346 cumbersome for users.
347

348 Knowledge Based Authentication: Authentication of an individual based on knowledge of
349 information associated with his or her claimed identity in public databases. Knowledge of such
350 information is considered to be private rather than secret, because it may be used in contexts
351 other than authentication to a verifier, thereby reducing the overall assurance associated with
352 the authentication process.
353

354 Man-in-the-Middle Attack (MitM): An attack on the authentication protocol run in which the
355 attacker positions himself or herself in between the claimant and verifier so that he can
356 intercept and alter data traveling between them.
357

358 Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric
359 key to detect both accidental and intentional modifications of the data. MACs provide
360 authenticity and integrity protection, but not non-repudiation protection.
361

362 Multi-Factor: A characteristic of an authentication system or an authenticator that uses more
363 than one authentication factor. The three types of authentication factors are something you
364 know, something you have, and something you are.
365

366 Network: An open communications medium, typically the Internet, that is used to transport
367 messages between the claimant and other Participants. Unless otherwise stated, no
368 assumptions are made about the security of the network; it is assumed to be open and subject
369 to active (i.e., impersonation, man-in-the-middle, session hijacking) and passive (i.e.,
370 eavesdropping) attack at any point between the Participants (e.g., claimant, verifier, CSP or RP).
371

372 Nonce: A value used in security protocols that is never repeated with the same key. For
373 example, nonces used as challenges in challenge-response authentication protocols must not
374 be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay
375 attack. Using a nonce as a challenge is a different requirement than a random challenge,
376 because a nonce is not necessarily unpredictable.
377

378 Off-line Attack: An attack where the attacker obtains some data (typically by eavesdropping on
379 an authentication protocol run or by penetrating a system and stealing security files) that
380 he/she is able to analyze in a system of his/her own choosing.
381

382 Online Attack: An attack against an authentication protocol where the attacker either assumes
383 the role of a claimant with a genuine verifier or actively alters the authentication channel.
384

385 Online Guessing Attack: An attack in which an attacker performs repeated logon trials by
386 guessing possible values of the authenticator output.
387

388 Operational Authority: Entity responsible for operations, maintenance, management, and
389 related functions of an Identity Trust Framework.
390

391 Participant Requirements: A set of rules and policies in an Identity Trust Framework addressing
392 identity, security, privacy, technology, and enforcement, which are assigned to each member
393 type in a Digital Identity System. Member types include Registration Authorities (RAs), Identity
394 Providers (IdPs), Credential Service Providers (CSPs), Verifiers, and Relying Parties (RPs).
395 [§ 59.1-550, COV]
396

397 Passive Attack: An attack against an authentication protocol where the attacker intercepts data
398 traveling along the network between the claimant and verifier, but does not alter the data (i.e.,
399 eavesdropping).
400

401 Password: A secret that a claimant memorizes and uses to authenticate his or her identity.
402 Passwords are typically character strings.
403

404 Personal Identification Number (PIN): A password consisting only of decimal digits.
405

406 Personal Identity Verification (PIV) Card: Defined by [FIPS 201] as a physical artifact (e.g.,
407 identity card, smart card) issued to federal employees and contractors that contains stored
408 credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that
409 the claimed identity of the cardholder can be verified against the stored credentials by another
410 person (human readable and verifiable) or an automated process (computer readable and
411 verifiable).
412

413 Personally Identifiable Information (PII): As defined by OMB Circular A-130, Personally
414 Identifiable Information means information that can be used to distinguish or trace an
415 individual's identity, either alone or when combined with other information that is linked or
416 linkable to a specific individual.
417

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

422 Phishing: An attack in which the Subscriber is lured (usually through an email) to interact with a
423 counterfeit verifier/RP and tricked into revealing information that can be used to masquerade
424 as that Subscriber to the real verifier/RP.
425

426 Physical In-Person: Method of Identity Proofing in which Applicants are required to physically
427 present themselves and identity evidence to a representative of the Registration Authority or
428 Identity Trust Framework. [NIST SP 800-63-2]
429

430 Possession and control of an authenticator: The ability to activate and use the authenticator in
431 an authentication protocol.
432

433 Practice Statement: A formal statement of the practices followed by the Participants to an
434 authentication process (i.e., RA, CSP, or verifier). It usually describes the policies and practices
435 of the Participants and can become legally binding.
436

437 Private Credentials: Credentials that cannot be disclosed by the CSP because the contents can
438 be used to compromise the authenticator.
439

440 Private Key: The secret part of an asymmetric key pair that is used to digitally sign or decrypt
441 data.
442

443 Protected Session: A session wherein messages between two participants are encrypted and
444 integrity is protected using a set of shared secrets called session keys. A participant is said to be
445 authenticated if, during the session, he, she or it proves possession of a long term authenticator
446 in addition to the session keys, and if the other Participant can verify the identity associated
447 with that authenticator. If both participants are authenticated, the protected session is said to
448 be mutually authenticated.
449

450 Pseudonymous Identifier: A meaningless, but unique number that does not allow the RP to
451 infer the Subscriber but which does permit the RP to associate multiple interactions with the
452 Subscriber's claimed identity.
453

454 Public Credentials: Credentials that describe the binding in a way that does not compromise the
455 authenticator.
456

457 Public Key: The public part of an asymmetric key pair that is used to verify signatures or encrypt
458 data.
459

460 Public Key Certificate: A digital document issued and digitally signed by the private key of a
461 Certificate authority that binds the name of a Subscriber to a public key. The certificate
462 indicates that the Subscriber identified in the certificate has sole control and access to the
463 private key. See also [RFC 5280].
464

465 Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software and
466 workstations used for the purpose of administering certificates and public-private key pairs,
467 including the ability to issue, maintain, and revoke public key certificates.
468

469 Registration: The process through which an applicant applies to become a Subscriber of a CSP
470 and an RA validates the identity of the applicant on behalf of the CSP.
471

472 Registration Authority (RA): A trusted entity that establishes and vouches for the identity or
473 attributes of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be
474 independent of a CSP, but it has a relationship to the CSP(s).
475

476 Relying Party (RP): An entity that relies upon the Subscriber's authenticator(s) and credentials
477 or a verifier's Assertion of a claimant's identity, typically to process a transaction or grant access
478 to information or a system.
479

480 Remote: (As in remote authentication or remote transaction) An information exchange
481 between network-connected devices where the information cannot be reliably protected end-
482 to-end by a single organization's security controls. Note: Any information exchange across the
483 Internet is considered remote.
484

485 Replay Attack: An attack in which the attacker is able to replay previously captured messages
486 (between a legitimate claimant and a verifier) to masquerade as that claimant to the verifier or
487 vice versa.
488

489 Risk Assessment: The process of identifying the risks to system security and determining the
490 probability of occurrence, the resulting impact, and additional safeguards that would mitigate
491 this impact. Part of Risk Management and synonymous with Risk Analysis.
492

493 Salt: A non-secret value that is used in a cryptographic process, usually to ensure that the
494 results of computations for one instance cannot be reused by an attacker.
495

496 Secondary Authenticator: A temporary secret, issued by the verifier to a successfully
497 authenticated Subscriber as part of an Assertion protocol. This secret is subsequently used, by
498 the Subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer
499 Assertions, Assertion references, and Kerberos session keys.
500

501 Secure Sockets Layer (SSL): An authentication and security protocol widely implemented in
502 browsers and web servers. SSL has been superseded by the newer Transport Layer Security
503 (TLS) protocol; TLS 1.0 is effectively SSL version 3.1.
504

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

509 SAML Authentication Assertion: A SAML Assertion that conveys information from a verifier to
510 an RP about a successful act of authentication that took place between the verifier and a
511 Subscriber.
512

513 Session Hijack Attack: An attack in which the attacker is able to insert himself or herself
514 between a claimant and a verifier subsequent to a successful authentication exchange between
515 the latter two Participants. The attacker is able to pose as a Subscriber to the verifier or vice
516 versa to control session data exchange. Sessions between the claimant and the relying
517 Participant can also be similarly compromised.
518

519 Shared Secret: A secret used in authentication that is known to the claimant and the verifier.
520

521 Social Engineering: The act of deceiving an individual into revealing sensitive information by
522 associating with the individual to gain confidence and trust.
523

524 Special Publication (SP): A type of publication issued by NIST. Specifically, the Special
525 Publication 800-series reports on the Information Technology Laboratory's research, guidelines,
526 and outreach efforts in computer security, and its collaborative activities with industry,
527 government, and academic organizations.
528

529 Strongly Bound Credentials: Credentials that describe the binding between a user and
530 authenticator in a tamper-evident fashion.
531

532 Subscriber: A Participant who has received a credential or authenticator from a CSP.
533

534 Symmetric Key: A cryptographic key that is used to perform both the cryptographic operation
535 and its inverse, for example to encrypt and decrypt, or create a message authentication code
536 and to verify the code.
537

538 Token: See Authenticator.
539

540 Token Authenticator: See Authenticator Output.
541

542 Token Secret: See Authenticator Secret.
543

544 Transport Layer Security (TLS): An authentication and security protocol widely implemented in
545 browsers and web servers. TLS is defined by [RFC 5246]. TLS is similar to the older Secure
546 Sockets Layer (SSL) protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52,
547 Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations specifies
548 how TLS is to be used in government applications.
549

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

553 Unverified Name: A Subscriber name that is not verified as meaningful by Identity Proofing.
554
555 Valid: In reference to an ID, the quality of not being expired or revoked.
556
557 Verified Name: A Subscriber name that has been verified by Identity Proofing.
558
559 Verifier: An entity that verifies the claimant's identity by verifying the claimant's possession and
560 control of one or two authenticators using an authentication protocol. To do this, the verifier
561 may also need to validate credentials that link the authenticator(s) and identity and check their
562 status.
563
564 Verifier Impersonation Attack: A scenario where the attacker impersonates the verifier in an
565 authentication protocol, usually to capture information that can be used to masquerade as a
566 claimant to the real verifier.
567
568 Virtual In-Person Proofing: A remote identity person proofing process that employs technical
569 and procedural measures that provide sufficient confidence that the remote session can be
570 considered equivalent to a physical, in-person identity proofing encounter. [NIST SP 800-63A]
571
572 Weakly Bound Credentials: Credentials that describe the binding between a user and
573 authenticator in a manner than can be modified without invalidating the credential.
574
575 Zeroize: Overwrite a memory location with data consisting entirely of bits with the value zero
576 so that the data is destroyed and not recoverable. This is often contrasted with deletion
577 methods that merely destroy reference to data within a file system rather than the data itself.
578
579 Zero-knowledge Password Protocol: A password based authentication protocol that allows a
580 claimant to authenticate to a Verifier without revealing the password to the verifier. Examples
581 of such protocols are EKE, SPEKE and SRP.

582 6 Background

583

584 In 2015, Virginia’s General Assembly passed the Electronic Identity Management Act (Chapter
585 50 of Title 59.1, *Code of Virginia*) to address demand in the state’s digital economy for secure,
586 privacy enhancing Electronic Authentication and Identity management. Growing numbers of
587 “communities of interest” have advocated for stronger, scalable and interoperable Identity
588 solutions to increase consumer protection and reduce liability for principal actors in the Identity
589 ecosystem – Identity Providers, Credential Service Providers, and Relying Parties.

590

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

596

597 The Advisory Council recommends to the Secretary of Technology guidance documents relating
598 to (i) nationally recognized technical and data standards regarding the verification and
599 authentication of Identity in digital and online transactions; (ii) the minimum specifications and
600 standards that should be included in an Identity Trust Framework, as defined in § 59.1-550, so
601 as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-
602 550 et seq.); and (iii) any other related data standards or specifications concerning reliance by
603 third parties on Identity credentials, as defined in § 59.1-550.

604

605 Purpose Statement

606

607 This guidance document, as defined in § 2.2-4001, was developed by the Identity Management
608 Standards Advisory Council (IMSAC), on behalf of the Secretary of Technology, to provide
609 information or guidance of general applicability to the public for interpreting or implementing
610 the Electronic Identity Management Act. Specifically, the document establishes minimum
611 specifications for Identity Proofing and verification to enable Registration and Electronic
612 Authentication events within a Digital Identity System. The minimum specifications conform
613 with NIST SP 800-63-3.

614

615 The document defines minimum requirements, components, process flows, Assurance levels,
616 and privacy and security provisions for Identity Proofing and verification. The document
617 assumes that specific business, legal, and technical requirements for Identity Proofing and
618 verification will be established in the Identity Trust Framework for each distinct Digital Identity
619 System, and that these requirements will be designed based on the Identity Assurance Level
620 (IAL) and Authenticator Assurance Level (AAL) requirements for the system.

621

622 The document limits its focus to Identity Proofing and verification. Minimum specifications for
623 other components of a Digital Identity System have been defined in separate IMSAC guidance
624 documents in this series, pursuant to § 2.2-436 and § 2.2-437.

625 7 Minimum Specifications

626
627 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3)
628 defines “Electronic Authentication” as “the process of establishing confidence in user identities
629 electronically presented to an Information System.”⁶ Information Systems may use the
630 authenticated Identity to determine if that user is authorized to perform an electronic
631 transaction.

632
633 Electronic Authentication begins with Registration (also referred to as enrollment). The
634 Registration process involves an Applicant applying to a CSP. If approved, the CSP creates a
635 Credential and binds it to one or more Authenticators. The Credential includes an identifier,
636 which can be pseudonymous, and one or more Attributes that the CSP has verified. The
637 Authenticators may be issued by the CSP, generated/provided directly by the Subscriber, or
638 provided by a third party. The Authenticator and Credential may be used in subsequent
639 authentication events.

640
641 The process used to verify an Applicant’s association with their real world Identity is called
642 Identity Proofing. The strength of Identity Proofing is described by a categorization called the
643 Identity Assurance Level (IAL, see subsection on Assurance Level Model below in this
644 document).

645
646 This document establishes minimum specifications for the Identity Proofing and verification
647 components of Registration events in a Digital Identity System. Identity Trust Frameworks for
648 Digital Identity Systems should document the business, legal, and technical requirements for
649 these components, as well as requirements for the remaining components of the system.
650 Minimum specifications for Identity Trust Frameworks have been defined in *IMSAC Guidance*
651 *Document: Identity Trust Frameworks*.

652 653 Identity Proofing Requirements

654
655 Identity Proofing and verification for Registration should be designed to meet the specific
656 requirements for the Assurance Model defined by the governing Identity Trust Framework for
657 the Digital Identity System. A trusted Registration process ensures that (i) the RA and CSP have
658 established the true Identity of the Applicant, (ii) the Registration protocols satisfy the
659 requirements for each Assurance level, (iii) the RA and CSP maintain a record of the Identity
660 evidence and transaction flows to meet audit and compliance requirements, and (iv) the RA and
661 CSP implement enforcement mechanisms to ensure compliance with all applicable provisions
662 established in the Identity Trust Framework.

663

⁶ 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.

- 664 At a minimum, Identity Proofing and verification requirements should establish that:
- 665 • A person with the Applicant's claimed attributes exists, and those attributes are sufficient to
 - 666 uniquely identify a single person;
 - 667 • The Applicant whose Authenticator is registered is in fact the person who is entitled to the
 - 668 Identity;
 - 669 • It is difficult for the Claimant to later repudiate the Registration and dispute an
 - 670 authentication using the Subscriber's Authenticator.

671

672 Registration, and the associated Identity Proofing and verification processes, may be completed

673 through Remote or In-Person (Physical or Virtual) protocols. Provisions for Remote versus In-

674 Person Identity Proofing and verification should be established in the Identity Trust Framework

675 for the Digital Identity System and satisfy requirements of the applicable Assurance Model.

676

677 Components and Process Flow

678

679 The Registration process, during which Identity Proofing and verification protocols are invoked,

680 generally involve the following components:

- 681 • The Applicant's Assertion of a Claimed Identity
- 682 • The Applicant's presentation of evidence to prove the existence of the claimed Identity
- 683 • The RA's review and validation of the Applicant's Claimed Identity and supporting evidence
- 684 • The CSP's verification of the Applicant's Claimed Identity
- 685 • The CSP's issuance or Registration of a Credential bound to the Applicant's Authenticator

686

687 The process flow for implementing the components of the Identity Proofing and verification for

688 Registration generally consists of the following (**Figure 1**):

- 689 1. The Applicant asserts to the trusted RA a Claimed Identity at a specified Assurance level
- 690 2. The Applicant provides the RA either Remotely or in person, depending on the Assurance
- 691 Model requirements of the Identity Trust Framework, evidence to prove the existence of
- 692 the claimed Identity (Identity Proofing) Note: Source of original Identity document(s) must
- 693 meet the Assurance Model and related compliance requirements set by the RA and defined
- 694 in the Identity Trust Framework
- 695 3. The RA transmits the Identity Proofing evidence to the CSP to verify whether the evidence
- 696 may be considered valid (Identity Validation)
- 697 4. The CSP compares the Applicant's Claimed Identity to information associated with the
- 698 Claimed Identity to determine whether it relates to the Applicant (Attribute Verification)⁷

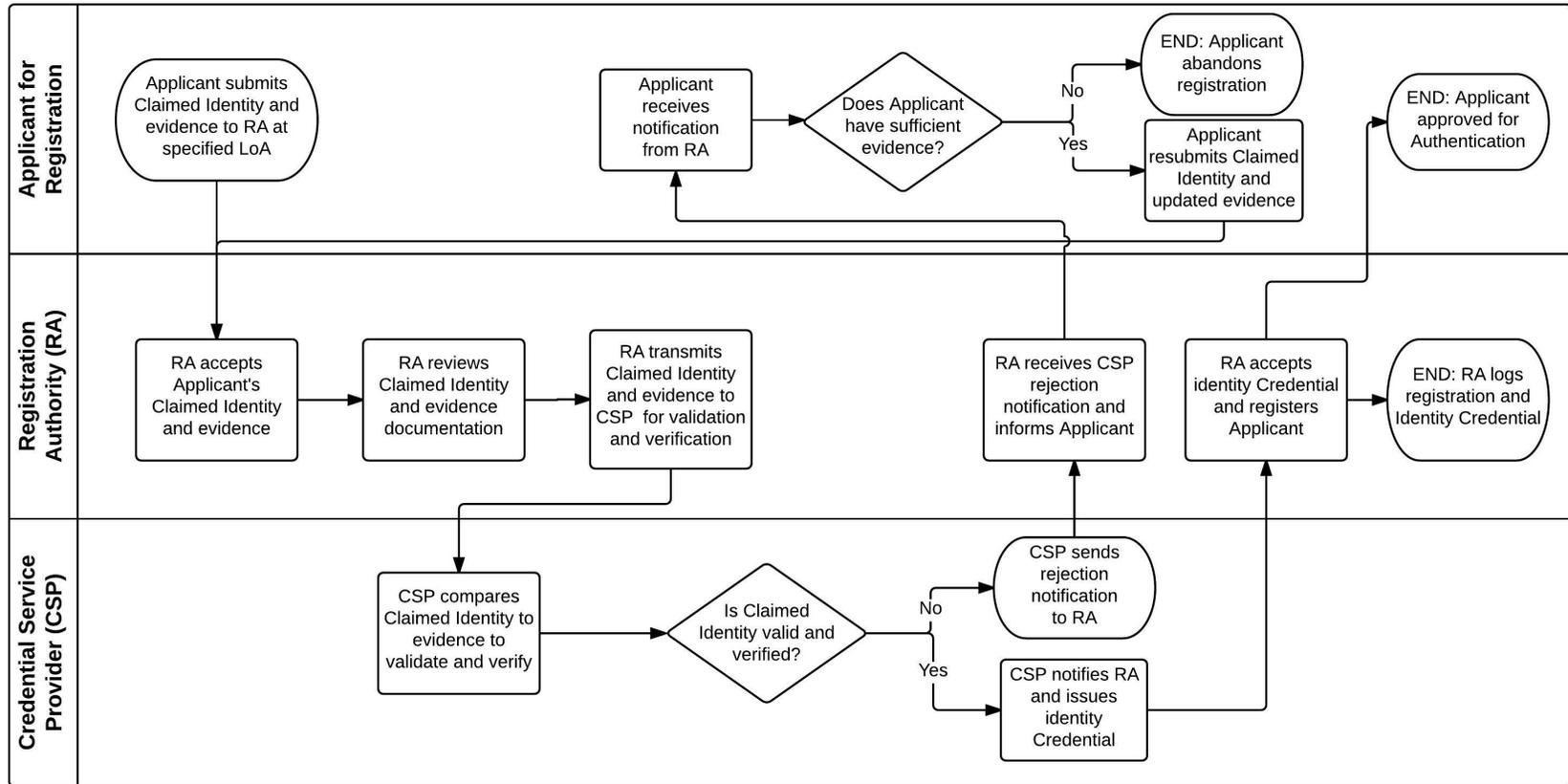
699

⁷ 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 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.

- 700 5. Upon successful completion of the Attribute Verification process, the CSP issues to the RA a
- 701 Credential bound to a Authenticator for the Applicant, confirming the Applicant's Claimed
- 702 Identity at the appropriate Assurance level defined in the Identity Trust Framework for the
- 703 Digital Identity System
- 704 6. RA maintains a record of the evidence and transaction for the Registration process.

DRAFT

Figure 1. Identity Proofing and Verification Process Flow



1 Assurance Model

2
3 The minimum specifications defined in this document for Electronic Authentication assume that
4 the Identity Trust Framework for a Digital Identity System will define a specific Assurance
5 Model for that system.⁸ Therefore, the Assurance Model presented below, which is based on
6 NIST SP 800-63-3, should be viewed as a recommended framework for Electronic
7 Authentication. Other Assurance Models have been established in OMB M-04-04 and the State
8 Identity, Credential, and Access Management (SICAM) guidelines, published by the National
9 Association of State Chief Information Officers (NASCIO). A crosswalk showing disparities in the
10 NIST SP 800-63-3, OMB M-04-04, and SICAM Assurance Models has been provided in **Figure 2**.

11
12 Identity Assurance Level 1 – At this level, attributes provided in conjunction with the
13 authentication process, if any, are self-asserted.

14
15 Identity Assurance Level 2 – IAL 2 introduces the need for either Remote or In-Person Identity
16 Proofing. IAL 2 requires identifying attributes to have been verified in person or remotely using,
17 at a minimum, the procedures given in NIST 800-63A.

18
19 Identity Assurance Level 3 – At IAL 3, In-Person Identity Proofing is required. Identifying
20 attributes must be verified by an authorized representative of the CSP through examination of
21 physical documentation as described in NIST 800-63A.

22
23 Authenticator Assurance Level 1 - AAL 1 provides single factor Electronic Authentication, giving
24 some assurance that the same claimant who participated in previous transactions is accessing
25 the protected transaction or data. AAL 1 allows a wide range of available authentication
26 technologies to be employed and requires only a single authentication factor to be used. It also
27 permits the use of any of the authentication methods of higher authenticator Assurance levels.
28 Successful authentication requires that the claimant prove through a secure authentication
29 protocol that he or she possesses and controls the authenticator.

30
31 Authenticator Assurance Level 2 – AAL 2 provides higher assurance that the same claimant who
32 participated in previous transactions is accessing the protected transaction or data. Two
33 different authentication factors are required. Various types of authenticators, including multi-
34 factor Software Cryptographic Authenticators, may be used as described in NIST 800-63B. AAL 2
35 also permits any of the authentication methods of AAL 3. AAL 2 authentication requires
36 cryptographic mechanisms that protect the primary authenticator against compromise by the
37 protocol threats for all threats at AAL 1 as well as verifier impersonation attacks. Approved
38 cryptographic techniques are required for all Assertion protocols used at AAL 2 and above.⁹

⁸ 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.

⁹ Approved cryptographic techniques must be FIPS approved, NIST recommended, or otherwise compliant with Commonwealth IT Information Security Standard (SEC501):
http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/HostedEnvironmentInformationSecurityStandardSEC52501.pdf

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

47

48 **Figure 2. Assurance Model Crosswalk**

49

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

50

51 Privacy and Security

52

53 The minimum specifications established in this document for privacy and security in the use of
54 person information for Identity Proofing and verification apply the Fair Information Practice
55 Principles (FIPPs).¹⁰ The FIPPs have been endorsed by the National Strategy for Trusted
56 Identities in Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.¹¹

57

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

61

62 The minimum specifications for Identity Proofing and verification apply the following FIPPs:

- 63 • Transparency: RAs and CSPs should be transparent and provide notice to Applicants
64 regarding collection, use, dissemination, and maintenance of person information required
65 during the Registration, Identity Proofing and verification processes.
- 66 • Individual Participation: RAs and CSPs should involve the Applicant in the process of using
67 person information and, to the extent practicable, seek consent for the collection, use,
68 dissemination, and maintenance of that information. RAs and CSPs also should provide
69 mechanisms for appropriate access, correction, and redress of person information.
- 70 • Purpose Specification: RAs and CSPs should specifically articulate the authority that permits
71 the collection of person information and specifically articulate the purpose or purposes for
72 which the information is intended to be used.
- 73 • Data Minimization: RAs and CSPs should collect only the person information directly
74 relevant and necessary to accomplish the Registration and related processes, and only
75 retain that information for as long as necessary to fulfill the specified purpose.
- 76 • Use Limitation/Minimal Disclosure: RAs and CSPs should use person information solely for
77 the purpose specified in the notice. Disclosure or sharing that information should be limited
78 to the specific purpose for which the information was collected.
- 79 • Data Quality and Integrity: RAs and CSPs should, to the extent practicable, ensure that
80 person information is accurate, relevant, timely, and complete.
- 81 • Security: RAs and CSPs should protect personal information through appropriate security
82 safeguards against risks such as loss, unauthorized access or use, destruction, modification,
83 or unintended or inappropriate disclosure.
- 84 • Accountability and Auditing: RAs and CSPs should be accountable for complying with these
85 principles, providing training to all employees and contractors who use person information,
86 and auditing the actual use of person information to demonstrate compliance with these
87 principles and all applicable privacy protection requirements.

¹⁰ 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.

¹¹ 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>.

88 8 Alignment Comparison

89
90 The minimum specifications for Identity Proofing and verification established in this document
91 have been developed to align with existing national and international standards for e-
92 authentication and Identity management. Specifically, the minimum specifications reflect basic
93 requirements set forth in national standards at the federal and state level, ensuring compliance
94 while accommodating other Identity management standards and protocols. This document
95 assumes that each Digital Identity System and supporting Identity Trust Framework will comply
96 with those governing standards and protocols required by Applicable Law.

97
98 The following section outlines the alignment and disparities between the minimum
99 specifications in this document and core national standards. A crosswalk documenting the
100 alignment and areas of misalignment has been provided in **Appendix 3**.

101

102 NIST SP 800-63-3

103

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

111

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

113

114 The minimum specifications in this document conform with the basic requirements for Identity
115 Proofing and verification set forth by NASCIO in the SICAM Guidance and Roadmap. The
116 NASCIO guidance defines specific requirements for state agencies. Similar to the contrast with
117 the NIST guidance for federal agencies, the minimum specifications in this document provide
118 flexibility for Digital Identity Systems across industries in the private sector and levels of
119 governance.

120

121 IDESG Identity Ecosystem Framework (IDEF) Functional Model

122

123 The minimum specifications in this document conform with the core operations and basic
124 requirements for privacy and security set forth by IDESG in the IDEF Functional Model and
125 Baseline Functional Requirements. The IDESG/IDEF requirements apply the FIPPs but extend
126 them to cover the NSTIC Guiding Principles. The minimum specifications in this document
127 encourage adherence to the IDEF Functional Model, Baseline Functional Requirements, and the
128 NSTIC Guiding Principles.

129

130 Appendix 1. IMSAC Charter

131

132

COMMONWEALTH OF VIRGINIA

133

IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL

134

CHARTER

135

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

137

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

141

142 The Advisory Council recommends to the Secretary of Technology guidance documents relating
143 to (i) nationally recognized technical and data standards regarding the verification and
144 authentication of identity in digital and online transactions; (ii) the minimum specifications and
145 standards that should be included in an Identity Trust Framework, as defined in § 59.1-550, so
146 as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-
147 550 et seq.); and (iii) any other related data standards or specifications concerning reliance by
148 third parties on identity credentials, as defined in § 59.1-550.

149

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

151

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

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

160

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

162

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

165

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

168

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

170

171

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

174

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

177

178 C. Proposed guidance documents and general opportunity for oral or written submittals as to
179 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published
180 in the Virginia Register of Regulations as a general notice following the processes and
181 procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§
182 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written
183 comments following the posting and publication and shall hold at least one meeting dedicated
184 to the receipt of oral comment no less than 15 days after the posting and publication. The
185 Advisory Council shall also develop methods for the identification and notification of interested
186 parties and specific means of seeking input from interested persons and groups. The Advisory
187 Council shall send a copy of such notices, comments, and other background material relative to
188 the development of the recommended guidance documents to the Joint Commission on
189 Administrative Rules.

190

191

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

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

197

198 PRIVACY-1. DATA MINIMIZATION

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

204

205 PRIVACY-2. PURPOSE LIMITATION

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

211

212 PRIVACY-3. ATTRIBUTE MINIMIZATION

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

218

219 PRIVACY-4. CREDENTIAL LIMITATION

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

223

224 PRIVACY-5. DATA AGGREGATION RISK

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

230

231 PRIVACY-6. USAGE NOTICE

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

234

235 PRIVACY-7. USER DATA CONTROL

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

238 PRIVACY-8. THIRD-PARTY LIMITATIONS

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

242

243 PRIVACY-9. USER NOTICE OF CHANGES

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

249

250 PRIVACY-10. USER OPTION TO DECLINE

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

253

254 PRIVACY-11. OPTIONAL INFORMATION

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

257

258 PRIVACY-12. ANONYMITY

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

266

267 PRIVACY-13. CONTROLS PROPORTIONATE TO RISK

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

272

273 PRIVACY-14. DATA RETENTION AND DISPOSAL

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

279

280 PRIVACY-15. ATTRIBUTE SEGREGATION

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

282 SECURE-1. SECURITY PRACTICES

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

285

286 SECURE-2. DATA INTEGRITY

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

291

292 SECURE-3. CREDENTIAL REPRODUCTION

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

295

296 SECURE-4. CREDENTIAL PROTECTION

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

300

301 SECURE-5. CREDENTIAL ISSUANCE

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

307

308 SECURE-6. CREDENTIAL UNIQUENESS

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

311

312 SECURE-7. TOKEN CONTROL

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

315

316 SECURE-8. MULTIFACTOR AUTHENTICATION

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

319

320 SECURE-9. AUTHENTICATION RISK ASSESSMENT

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

323

324

325

326 SECURE-10. UPTIME

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

330

331 SECURE-11. KEY MANAGEMENT

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

334

335 SECURE-12. RECOVERY AND REISSUANCE

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

339

340 SECURE-13. REVOCATION

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

343

344 SECURE-14. SECURITY LOGS

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

349

350 SECURE-15. SECURITY AUDITS

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

355

Appendix 3. Identity Proofing Standards Alignment Comparison Matrix

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