

## COMMONWEALTH OF VIRGINIA



~~Information Technology Resource  
Management~~**IDENTITY MANAGEMENT STANDARDS  
ADVISORY COUNCIL (ITRMIMSAC)**

**GUIDANCE DOCUMENT  
Identity Management of Non-Person Entities**

~~Virginia Information Technologies Agency (VITA)~~

### Table of Contents

1	Publication Version Control .....	1
2	Reviews .....	1
<del>3</del>	<del>Purpose and Scope .....</del>	<del>1</del>
<del>3-4</del>	<del>Statutory Authority .....</del>	<del>1</del>
	<del>.....</del>	<del>2</del>
<del>4-5</del>	<del>Definitions .....</del>	<del>3</del>
<del>5-6</del>	<del>Background .....</del>	<del>1415</del>
<del>6-7</del>	<del>Minimum Specifications .....</del>	<del>1516</del>
8	IdM of NPE Use Case: Public Health Emergency Response .....	1526
<del>7</del>	<del>Alignment Comparison .....</del>	<del>26</del>

Formatted: Font: 5 pt

DRAFT

# 1 Publication Version Control

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

Publication Version	Date	Revision Description
1.0	<del>07/20</del> 01/04/2017	Initial Draft of Document

Formatted Table

# 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 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.~~

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

• ~~The document will be reviewed in a manner compliant with the Commonwealth of Virginia's Administrative Process Act, § 2.2-4000 et seq. 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: Normal, No bullets or numbering

• ~~Proposed guidance documents and general opportunity for oral or written submittals as to those guidance documents shall be posted on the Virginia Regulatory Town Hall and published in the Virginia Register of Regulations as a general notice following the processes and procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§2.2-4000 et seq.). The Advisory Council [IMSAC] shall allow at least 30 days for the submission of written comments following the posting and publication and shall hold at least one meeting dedicated to the receipt of oral comment no less than 15 days after the posting and publication. The Advisory Council shall also develop methods for the identification and notification of interested parties and specific means of seeking input from interested persons and groups. The Advisory Council shall send a copy of such notices,~~

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

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49

*comments, and other background material relative to the development of the recommended guidance documents to the Joint Commission on Administrative Rules.*

Formatted: Font: Italic  
Formatted: Indent: Left: 0"

### 3 Purpose and Scope

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

Formatted: Indent: Left: 0"

DRAFT

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

## 34 Statutory Authority

The following section documents the statutory authority established in the *Code of Virginia* for the development of minimum specifications and standards for Identity Management of Non-Person Entities. References to statutes below and throughout this document shall be to the *Code of Virginia*, unless otherwise specified.

### Governing Statutes:

#### Secretary of Technology

§ 2.2-225. Position established; agencies for which responsible; additional powers  
<http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225/>

#### Identity Management Standards Advisory Council

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

#### Commonwealth Identity Management Standards

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

#### Electronic Identity Management Act

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

The following section documents the statutory authority established in the *Code of Virginia* for the development of minimum specifications and standards for electronic authentication. References to statutes below and throughout this document shall be to the *Code of Virginia*, unless otherwise specified.

### Governing Statutes:

#### Secretary of Technology

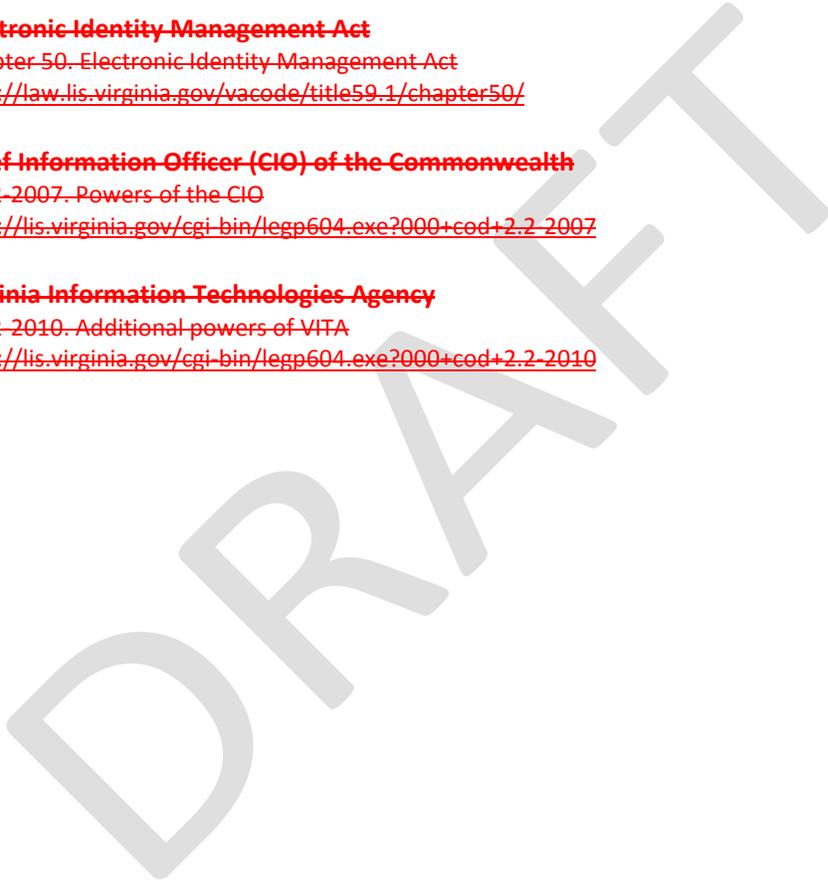
§ 2.2-225. Position established; agencies for which responsible; additional powers  
<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-225>

#### Secretary of Transportation

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

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

- 90 **Identity Management Standards Advisory Council**
- 91 § 2.2-437. Identity Management Standards Advisory Council
- 92 <http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/>
- 93
- 94 **Commonwealth Identity Management Standards**
- 95 § 2.2-436. Approval of electronic identity standards
- 96 <http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/>
- 97
- 98 **Electronic Identity Management Act**
- 99 Chapter 50. Electronic Identity Management Act
- 100 <http://law.lis.virginia.gov/vacode/title59.1/chapter50/>
- 101
- 102 **Chief Information Officer (CIO) of the Commonwealth**
- 103 § 2.2-2007. Powers of the CIO
- 104 <http://lis.virginia.gov/cgi-bin/legp604.exe?000+cod+2.2-2007>
- 105
- 106 **Virginia Information Technologies Agency**
- 107 § 2.2-2010. Additional powers of VITA
- 108 <http://lis.virginia.gov/cgi-bin/legp604.exe?000+cod+2.2-2010>
- 109
- 110
- 111
- 112
- 113
- 114



Formatted: Position: Vertical: -0.04", Relative to: Paragraph

## 115 45 Definitions

116 Terms used in this document comply with definitions in the Public Review version of the  
 117 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3),  
 118 and align with adopted definitions in § 59.1-550, Code of Virginia (COV), and the  
 119 Commonwealth of Virginia’s ITRM Glossary (ITRM Glossary).<sup>1</sup>  
 120  
 121 Active Attack: An online attack where the attacker transmits data to the claimant, credential  
 122 service provider, verifier, or relying Participant. Examples of active attacks include man-in-the-  
 123 middle, impersonation, and session hijacking.  
 124  
 125 Address of Record: The official location where an individual can be found. The address of record  
 126 always includes the residential street address of an individual and may also include the mailing  
 127 address of the individual. In very limited circumstances, an Army Post Office box number, Fleet  
 128 Post Office box number or the street address of next of kin or of another contact individual can  
 129 be used when a residential street address for the individual is not available.  
 130  
 131 Approved: Federal Information Processing Standard (FIPS) approved or NIST recommended. An  
 132 algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2)  
 133 adopted in a FIPS or NIST Recommendation.  
 134  
 135 Applicable Law: Laws, statutes, regulations, and rules of the jurisdiction in which the members  
 136 of an Identity Trust Framework operates.  
 137  
 138 Applicant: A Participant undergoing the processes of Registration and Identity Proofing.  
 139  
 140 Assertion: A statement from a verifier to a relying Participant (RP) that contains identity  
 141 information about a Subscriber. Assertions may also contain verified attributes.  
 142  
 143 Assertion Reference: A data object, created in conjunction with an Assertion, which identifies  
 144 the verifier and includes a pointer to the full Assertion held by the verifier.  
 145  
 146 Assurance: In the context of [OMB M-04-04]<sup>2</sup> and this document, assurance is defined as 1) the  
 147 degree of confidence in the vetting process used to establish the identity of an individual to  
 148 whom the credential was issued, and 2) the degree of confidence that the individual who uses  
 149 the credential is the individual to whom the credential was issued.  
 150

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

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

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

Formatted: Font: 9 pt

Formatted: Default Paragraph Font, Font: 9 pt

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

- 151 Assurance Model: Policies, processes, and protocols that define how Assurance will be  
152 established in an Identity Trust Framework.
- 153
- 154 Asymmetric Keys: Two related keys, a public key and a private key that are used to perform  
155 complementary operations, such as encryption and decryption or signature generation and  
156 signature verification.
- 157
- 158 Attack: An attempt by an unauthorized individual to fool a verifier or a relying Participant into  
159 believing that the unauthorized individual in question is the Subscriber.
- 160
- 161 Attacker: A Participant who acts with malicious intent to compromise an Information System.
- 162
- 163 Attribute: A claim of a named quality or characteristic inherent in or ascribed to someone or  
164 something.
- 165
- 166 Authentication: The process of establishing confidence in the identity of users or Information  
167 Systems.
- 168
- 169 Authentication Protocol: A defined sequence of messages between a claimant and a verifier  
170 that demonstrates that the claimant has possession and control of a valid authenticator to  
171 establish his/her identity, and optionally, demonstrates to the claimant that he or she is  
172 communicating with the intended verifier.
- 173
- 174 Authentication Protocol Run: An exchange of messages between a claimant and a verifier that  
175 results in authentication (or authentication failure) between the two Participants.
- 176
- 177 Authentication Secret: A generic term for any secret value that could be used by an attacker to  
178 impersonate the Subscriber in an authentication protocol. These are further divided into short-  
179 term authentication secrets, which are only useful to an attacker for a limited period of time,  
180 and long-term authentication secrets, which allow an attacker to impersonate the Subscriber  
181 until they are manually reset. The authenticator secret is the canonical example of a long term  
182 authentication secret, while the authenticator output, if it is different from the authenticator  
183 secret, is usually a short term authentication secret.
- 184
- 185 Authenticator: Something that the claimant possesses and controls (typically a cryptographic  
186 module or password) that is used to authenticate the claimant's identity. In previous versions of  
187 this guideline, this was referred to as a token.
- 188
- 189 Authenticator Assurance Level (AAL): A metric describing robustness of the authentication  
190 process proving that the claimant is in control of a given Subscriber's authenticator(s).
- 191
- 192 Authenticator Output: The output value generated by an authenticator. The ability to generate  
193 valid authenticator outputs on demand proves that the claimant possesses and controls the

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

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

196

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

198

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

200

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

205

206 Bit: A binary digit: 0 or 1.

207

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

211

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

213

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

216

217 Challenge-Response Protocol: An authentication protocol where the verifier sends the claimant  
218 a challenge (usually a random value or a nonce) that the claimant combines with a secret (such  
219 as by hashing the challenge and a shared secret together, or by applying a private key operation  
220 to the challenge) to generate a response that is sent to the verifier. The verifier can  
221 independently verify the response generated by the claimant (such as by re-computing the hash  
222 of the challenge and the shared secret and comparing to the response, or performing a public  
223 key operation on the response) and establish that the claimant possesses and controls the  
224 secret.

225

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

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

232

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

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

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

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

239  
240 Cookie: A character string, placed in a web browser's memory, which is available to websites  
241 within the same Internet domain as the server that placed them in the web browser.

242  
243 Credential: An object or data structure that authoritatively binds an identity (and optionally,  
244 additional attributes) to an authenticator possessed and controlled by a Subscriber. While  
245 common usage often assumes that the credential is maintained by the Subscriber, this  
246 document also uses the term to refer to electronic records maintained by the CSP which  
247 establish a binding between the Subscriber's authenticator(s) and identity.

248  
249 Credential Service Provider (CSP): A trusted entity that issues or registers Subscriber  
250 authenticators and issues electronic credentials to Subscribers. The CSP may encompass  
251 Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third  
252 Participant, or may issue credentials for its own use.

253  
254 Cross Site Request Forgery (CSRF): An attack in which a Subscriber who is currently  
255 authenticated to an RP and connected through a secure session, browses to an attacker's  
256 website which causes the Subscriber to unknowingly invoke unwanted actions at the RP. For  
257 example, if a bank website is vulnerable to a CSRF attack, it may be possible for a Subscriber to  
258 unintentionally authorize a large money transfer, merely by viewing a malicious link in a  
259 webmail message while a connection to the bank is open in another browser window.

260  
261 Cross Site Scripting (XSS): A vulnerability that allows attackers to inject malicious code into an  
262 otherwise benign website. These scripts acquire the permissions of scripts generated by the  
263 target website and can therefore compromise the confidentiality and integrity of data transfers  
264 between the website and client. Websites are vulnerable if they display user supplied data from  
265 requests or forms without sanitizing the data so that it is not executable.

266  
267 Cryptographic Key: A value used to control cryptographic operations, such as decryption,  
268 encryption, signature generation or signature verification. For the purposes of this document,  
269 key requirements must meet the minimum requirements stated in Table 2 of NIST SP 800-57  
270 Part 1. See also Asymmetric keys, Symmetric key.

271  
272 Cryptographic Authenticator: An authenticator where the secret is a cryptographic key.  
273

---

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

274 Data Integrity: The property that data has not been altered by an unauthorized entity.  
275  
276 Derived Credential: A credential issued based on proof of possession and control of an  
277 authenticator associated with a previously issued credential, so as not to duplicate the Identity  
278 Proofing process.  
279  
280 Digital Identity System: An Information System that supports Electronic Authentication and the  
281 management of a person's Identity in a digital environment. [Referenced in § 59.1-550, COV]  
282  
283 Digital Signature: An asymmetric key operation where the private key is used to digitally sign  
284 data and the public key is used to verify the signature. Digital signatures provide authenticity  
285 protection, integrity protection, and non-repudiation.  
286  
287 Eavesdropping Attack: An attack in which an attacker listens passively to the authentication  
288 protocol to capture information which can be used in a subsequent active attack to  
289 masquerade as the claimant.  
290  
291 Electronic Authentication: The process of establishing confidence in user identities  
292 electronically presented to an Information System.  
293  
294 Entropy: A measure of the amount of uncertainty that an attacker faces to determine the value  
295 of a secret. Entropy is usually stated in bits.  
296  
297 Extensible Mark-up Language (XML): Extensible Markup Language, abbreviated XML, describes  
298 a class of data objects called XML documents and partially describes the behavior of computer  
299 programs which process them.  
300  
301 Federal Bridge Certification Authority (FBCA): The FBCA is the entity operated by the Federal  
302 Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI  
303 Policy Authority to create, sign, and issue public key certificates to Principal CAs.  
304  
305 Federal Information Security Management Act (FISMA): Title III of the E-Government Act  
306 requiring each federal agency to develop, document, and implement an agency-wide program  
307 to provide information security for the information and Information Systems that support the  
308 operations and assets of the agency, including those provided or managed by another agency,  
309 contractor, or other source.  
310  
311 Federal Information Processing Standard (FIPS): Under the Information Technology  
312 Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards  
313 and guidelines that are developed by the National Institute of Standards and Technology (NIST)  
314 for Federal computer systems. These standards and guidelines are issued by NIST as Federal  
315 Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

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

318  
319 Federation: A process that allows for the conveyance of identity and authentication information  
320 across a set of networked systems. These systems are often run and controlled by disparate  
321 Participants in different network and security domains. [NIST SP 800-63C]

322  
323 Governance Authority: Entity responsible for providing policy level leadership, oversight,  
324 strategic direction, and related governance activities within an Identity Trust Framework.

325  
326 Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string.  
327 Approved hash functions satisfy the following properties:

- 328 • (One-way) It is computationally infeasible to find any input that maps to any pre-  
329 specified output, and
- 330 • (Collision resistant) It is computationally infeasible to find any two distinct inputs that  
331 map to the same output.

332  
333 Holder-of-Key Assertion: An Assertion that contains a reference to a symmetric key or a public  
334 key (corresponding to a private key) held by the Subscriber. The RP may authenticate the  
335 Subscriber by verifying that he or she can indeed prove possession and control of the  
336 referenced key.

337  
338 Identity: A set of attributes that uniquely describe a person within a given context.

339  
340 Identity Assurance Level (IAL): A metric describing degree of confidence that the applicant's  
341 claimed identity is their real identity.

342  
343 Identity Proofing: The process by which a CSP and a Registration Authority (RA) collect and  
344 verify information about a person for the purpose of issuing credentials to that person.

345  
346 Identity Provider (IdP): The party that manages the subscriber's primary authentication  
347 credentials and issues Assertions derived from those credentials generally to the credential  
348 service provider (CSP).

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

357

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

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

361

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

370

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

376

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

380

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

384

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

388

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

394

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

400

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

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

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

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

411 Operational Authority: Entity responsible for operations, maintenance, management, and  
412 related functions of an Identity Trust Framework.

414 Participant Requirements: A set of rules and policies in an Identity Trust Framework addressing  
415 identity, security, privacy, technology, and enforcement, which are assigned to each member  
416 type in a Digital Identity System. Member types include Registration Authorities (RAs), Identity  
417 Providers (IdPs), Credential Service Providers (CSPs), Verifiers, and Relying Parties (RPs).  
418 [§ 59.1-550, COV]

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

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

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

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

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

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

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

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

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

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

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

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

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

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

469 Public Credentials: Credentials that describe the binding in a way that does not compromise the  
470 authenticator.

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

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

487

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

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

491

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

494

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

498

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

502

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

507

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

511

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

515

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

518

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

523

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

527

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

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

532 SAML Authentication Assertion: A SAML Assertion that conveys information from a verifier to  
533 an RP about a successful act of authentication that took place between the verifier and a  
534 Subscriber.

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

541  
542 Shared Secret: A secret used in authentication that is known to the claimant and the verifier.

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

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

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

554  
555 Subscriber: A Participant who has received a credential or authenticator from a CSP.

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

560  
561 Token: See Authenticator.

562  
563 Token Authenticator: See Authenticator Output.

564  
565 Token Secret: See Authenticator Secret.

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

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

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

576 Unverified Name: A Subscriber name that is not verified as meaningful by Identity Proofing.

577

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

579

580 Verified Name: A Subscriber name that has been verified by Identity Proofing.

581

582 Verifier: An entity that verifies the claimant’s identity by verifying the claimant’s possession and

583 control of one or two authenticators using an authentication protocol. To do this, the verifier

584 may also need to validate credentials that link the authenticator(s) and identity and check their

585 status.

586

587 Verifier Impersonation Attack: A scenario where the attacker impersonates the verifier in an

588 authentication protocol, usually to capture information that can be used to masquerade as a

589 claimant to the real verifier.

590

591 Virtual In-Person Proofing: A remote identity person proofing process that employs technical

592 and procedural measures that provide sufficient confidence that the remote session can be

593 considered equivalent to a physical, in-person identity proofing encounter. [NIST SP 800-63A]

594

595 Weakly Bound Credentials: Credentials that describe the binding between a user and

596 authenticator in a manner than can be modified without invalidating the credential.

597

598 Zeroize: Overwrite a memory location with data consisting entirely of bits with the value zero

599 so that the data is destroyed and not recoverable. This is often contrasted with deletion

600 methods that merely destroy reference to data within a file system rather than the data itself.

601

602 Zero-knowledge Password Protocol: A password based authentication protocol that allows a

603 claimant to authenticate to a Verifier without revealing the password to the verifier. Examples

604 of such protocols are EKE, SPEKE and SRP. Terms used in this document comply with definitions

605 in the Public Review version of the National Institute of Standards and Technology Special

606 Publication 800-63-3 (NIST SP 800-63-3), and align with adopted definitions in § 59.1-550, *Code*

607 *of Virginia*, and the Commonwealth of Virginia’s ITRM Glossary (ITRM Glossary).<sup>6</sup>

608

609 Active Attack: An online attack where the attacker transmits data to the claimant, credential

610 service provider, verifier, or relying party. Examples of active attacks include man-in-the-

611 middle, impersonation, and session hijacking.

612

<sup>6</sup> NIST SP 800-63-3 may be accessed at <https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3>. At the time of the publication of this document, NIST SP 800-63-3 was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3. § 59.1-550, *Code of Virginia*, may be accessed at <http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550/>. The Commonwealth’s ITRM Glossary may be accessed at [http://www.vita.virginia.gov/uploadedFiles/VITA\\_Main\\_Public/Library/PSGs/PSG\\_Sections/COV-ITRM-Glossary.pdf](http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/PSG_Sections/COV-ITRM-Glossary.pdf)

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

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

618  
619 ~~Approved: Federal Information Processing Standard (FIPS) approved or NIST recommended. An~~  
620 ~~algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2)~~  
621 ~~adopted in a FIPS or NIST Recommendation.~~

622  
623 ~~Applicant: A party undergoing the processes of registration and identity proofing.~~

624  
625 ~~Assertion: A statement from a verifier to a relying party (RP) that contains identity information~~  
626 ~~about a subscriber. Assertions may also contain verified attributes.~~

627  
628 ~~Assertion Reference: A data object, created in conjunction with an assertion, which identifies~~  
629 ~~the verifier and includes a pointer to the full assertion held by the verifier.~~

630  
631 ~~Assurance: In the context of [OMB M-04-04]<sup>7</sup> and this document, assurance is defined as 1) the~~  
632 ~~degree of confidence in the vetting process used to establish the identity of an individual to~~  
633 ~~whom the credential was issued, and 2) the degree of confidence that the individual who uses~~  
634 ~~the credential is the individual to whom the credential was issued.~~

635  
636 ~~Asymmetric Keys: Two related keys, a public key and a private key that are used to perform~~  
637 ~~complementary operations, such as encryption and decryption or signature generation and~~  
638 ~~signature verification.~~

639  
640 ~~Attack: An attempt by an unauthorized individual to fool a verifier or a relying party into~~  
641 ~~believing that the unauthorized individual in question is the subscriber.~~

642  
643 ~~Attacker: A party who acts with malicious intent to compromise an information system.~~

644  
645 ~~Attribute: A claim of a named quality or characteristic inherent in or ascribed to someone or~~  
646 ~~something.~~

647  
648 ~~Authentication: The process of establishing confidence in the identity of users or information~~  
649 ~~systems.~~

650  
651 ~~Authentication Protocol: A defined sequence of messages between a claimant and a verifier~~  
652 ~~that demonstrates that the claimant has possession and control of a valid authenticator to~~

<sup>7</sup> [OMB M-04-04] Office of Management and Budget, Memorandum 04-04: E-Authentication Guidance for Federal Agencies, accessible at <https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>.

653 ~~establish his/her identity, and optionally, demonstrates to the claimant that he or she is~~  
654 ~~communicating with the intended verifier.~~  
655  
656 ~~Authentication Protocol Run: An exchange of messages between a claimant and a verifier that~~  
657 ~~results in authentication (or authentication failure) between the two parties.~~  
658  
659 ~~Authentication Secret: A generic term for any secret value that could be used by an attacker to~~  
660 ~~impersonate the subscriber in an authentication protocol. These are further divided into short-~~  
661 ~~term authentication secrets, which are only useful to an attacker for a limited period of time,~~  
662 ~~and long-term authentication secrets, which allow an attacker to impersonate the subscriber~~  
663 ~~until they are manually reset. The authenticator secret is the canonical example of a long-term~~  
664 ~~authentication secret, while the authenticator output, if it is different from the authenticator~~  
665 ~~secret, is usually a short-term authentication secret.~~  
666  
667 ~~Authenticator: Something that the claimant possesses and controls (typically a cryptographic~~  
668 ~~module or password) that is used to authenticate the claimant's identity. In previous versions of~~  
669 ~~this guideline, this was referred to as a token.~~  
670  
671 ~~Authenticator Assurance Level (AAL): A metric describing robustness of the authentication~~  
672 ~~process proving that the claimant is in control of a given subscriber's authenticator(s).~~  
673  
674 ~~Authenticator Output: The output value generated by an authenticator. The ability to generate~~  
675 ~~valid authenticator outputs on demand proves that the claimant possesses and controls the~~  
676 ~~authenticator. Protocol messages sent to the verifier are dependent upon the authenticator~~  
677 ~~output, but they may or may not explicitly contain it.~~  
678  
679 ~~Authenticator Secret: The secret value contained within an authenticator.~~  
680 ~~Authenticity: The property that data originated from its purported source.~~  
681  
682 ~~Bearer Assertion: An assertion that does not provide a mechanism for the subscriber to prove~~  
683 ~~that he or she is the rightful owner of the assertion. The RP has to assume that the assertion~~  
684 ~~was issued to the subscriber who presents the assertion or the corresponding assertion~~  
685 ~~reference to the RP.~~  
686  
687 ~~Bit: A binary digit: 0 or 1.~~  
688  
689 ~~Biometrics: Automated recognition of individuals based on their behavioral and biological~~  
690 ~~characteristics. In this document, biometrics may be used to unlock authenticators and prevent~~  
691 ~~repudiation of registration.~~  
692  
693 ~~Certificate Authority (CA): A trusted entity that issues and revokes public key certificates.~~  
694

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

695 ~~Certificate Revocation List (CRL): A list of revoked public key certificates created and digitally~~  
696 ~~signed by a Certificate Authority. [RFC 5280]<sup>8</sup>~~

697  
698 ~~Challenge Response Protocol: An authentication protocol where the verifier sends the claimant~~  
699 ~~a challenge (usually a random value or a nonce) that the claimant combines with a secret (such~~  
700 ~~as by hashing the challenge and a shared secret together, or by applying a private key operation~~  
701 ~~to the challenge) to generate a response that is sent to the verifier. The verifier can~~  
702 ~~independently verify the response generated by the claimant (such as by re-computing the hash~~  
703 ~~of the challenge and the shared secret and comparing to the response, or performing a public~~  
704 ~~key operation on the response) and establish that the claimant possesses and controls the~~  
705 ~~secret.~~

706  
707 ~~Claimant: A party whose identity is to be verified using an authentication protocol.~~

708  
709 ~~Claimed Address: The physical location asserted by an individual (e.g. an applicant) where~~  
710 ~~he/she can be reached. It includes the residential street address of an individual and may also~~  
711 ~~include the mailing address of the individual. For example, a person with a foreign passport,~~  
712 ~~living in the U.S., will need to give an address when going through the identity proofing process.~~  
713 ~~This address would not be an “address of record” but a “claimed address.”~~

714  
715 ~~Claimed Identity: A declaration by the applicant of their current Personal Name, date of birth~~  
716 ~~and address. [GPG45]<sup>9</sup>~~

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

721  
722 ~~Cookie: A character string, placed in a web browser’s memory, which is available to websites~~  
723 ~~within the same Internet domain as the server that placed them in the web browser.~~

724  
725 ~~Credential: An object or data structure that authoritatively binds an identity (and optionally,~~  
726 ~~additional attributes) to an authenticator possessed and controlled by a subscriber. While~~  
727 ~~common usage often assumes that the credential is maintained by the subscriber, this~~  
728 ~~document also uses the term to refer to electronic records maintained by the CSP which~~  
729 ~~establish a binding between the subscriber’s authenticator(s) and identity.~~

730  
731 ~~Credential Service Provider (CSP): A trusted entity that issues or registers subscriber~~  
732 ~~authenticators and issues electronic credentials to subscribers. The CSP may encompass~~

<sup>8</sup> [RFC 5280] Official Internet Protocol Standards, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008, accessible at <http://www.rfc-editor.org/info/rfc5280>.

<sup>9</sup> [GPG 45] UK Cabinet Office, Good Practice Guide 45, Identity proofing and verification of an individual, November 3, 2014, accessible at <https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual>.

733 Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third  
734 party, or may issue credentials for its own use.

735  
736 Cross-Site Request Forgery (CSRF): An attack in which a subscriber who is currently  
737 authenticated to an RP and connected through a secure session, browses to an attacker's  
738 website which causes the subscriber to unknowingly invoke unwanted actions at the RP. For  
739 example, if a bank website is vulnerable to a CSRF attack, it may be possible for a subscriber to  
740 unintentionally authorize a large money transfer, merely by viewing a malicious link in a  
741 webmail message while a connection to the bank is open in another browser window.

742  
743 Cross-Site Scripting (XSS): A vulnerability that allows attackers to inject malicious code into an  
744 otherwise benign website. These scripts acquire the permissions of scripts generated by the  
745 target website and can therefore compromise the confidentiality and integrity of data transfers  
746 between the website and client. Websites are vulnerable if they display user-supplied data from  
747 requests or forms without sanitizing the data so that it is not executable.

748  
749 Cryptographic Key: A value used to control cryptographic operations, such as decryption,  
750 encryption, signature generation or signature verification. For the purposes of this document,  
751 key requirements shall meet the minimum requirements stated in Table 2 of NIST SP 800-57  
752 Part 1. See also Asymmetric keys, Symmetric key.

753  
754 Cryptographic Authenticator: An authenticator where the secret is a cryptographic key.

755  
756 Data Integrity: The property that data has not been altered by an unauthorized entity.

757  
758 Derived Credential: A credential issued based on proof of possession and control of an  
759 authenticator associated with a previously issued credential, so as not to duplicate the identity  
760 proofing process.

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

764  
765 Eavesdropping Attack: An attack in which an attacker listens passively to the authentication  
766 protocol to capture information which can be used in a subsequent active attack to  
767 masquerade as the claimant.

768  
769 Electronic Authentication: The process of establishing confidence in user identities  
770 electronically presented to an information system.

771  
772 Entropy: A measure of the amount of uncertainty that an attacker faces to determine the value  
773 of a secret. Entropy is usually stated in bits.

774

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

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

778  
 779 Federal Bridge Certification Authority (FBCA): The FBCA is the entity operated by the Federal  
 780 Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI  
 781 Policy Authority to create, sign, and issue public key certificates to Principal CAs.

782  
 783 Federal Information Security Management Act (FISMA): Title III of the E-Government Act  
 784 requiring each federal agency to develop, document, and implement an agency-wide program  
 785 to provide information security for the information and information systems that support the  
 786 operations and assets of the agency, including those provided or managed by another agency,  
 787 contractor, or other source.

788  
 789 Federal Information Processing Standard (FIPS): Under the Information Technology  
 790 Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards  
 791 and guidelines that are developed by the National Institute of Standards and Technology (NIST)  
 792 for Federal computer systems. These standards and guidelines are issued by NIST as Federal  
 793 Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when  
 794 there are compelling Federal government requirements such as for security and interoperability  
 795 and there are no acceptable industry standards or solutions.<sup>40</sup>

796  
 797 Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string.  
 798 Approved hash functions satisfy the following properties:

- 799 • (One-way) It is computationally infeasible to find any input that maps to any pre-
- 800 specified output, and
- 801 • (Collision resistant) It is computationally infeasible to find any two distinct inputs that
- 802 map to the same output.

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

807  
 808 Identity: A set of attributes that uniquely describe a person within a given context.

809  
 810 Identity Assurance Level (IAL): A metric describing degree of confidence that the applicant's  
 811 claimed identity is their real identity.

812  
 813 Identity Proofing: The process by which a CSP and a Registration Authority (RA) collect and  
 814 verify information about a person for the purpose of issuing credentials to that person.

815

<sup>40</sup> Federal Information Processing Standard (FIPS), accessible at <http://www.nist.gov/itl/fips.cfm>.

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

824  
825 Knowledge-Based Authentication: Authentication of an individual based on knowledge of  
826 information associated with his or her claimed identity in public databases. Knowledge of such  
827 information is considered to be private rather than secret, because it may be used in contexts  
828 other than authentication to a verifier, thereby reducing the overall assurance associated with  
829 the authentication process.

830  
831 Man-in-the-Middle Attack (MitM): An attack on the authentication protocol run in which the  
832 attacker positions himself or herself in between the claimant and verifier so that he can  
833 intercept and alter data traveling between them.

834  
835 Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric  
836 key to detect both accidental and intentional modifications of the data. MACs provide  
837 authenticity and integrity protection, but not non-repudiation protection.

838  
839 Multi-Factor: A characteristic of an authentication system or an authenticator that uses more  
840 than one authentication factor. The three types of authentication factors are something you  
841 know, something you have, and something you are.

842  
843

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

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

849  
850 ~~Nonce: A value used in security protocols that is never repeated with the same key. For~~  
851 ~~example, nonces used as challenges in challenge-response authentication protocols must not~~  
852 ~~be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay~~  
853 ~~attack. Using a nonce as a challenge is a different requirement than a random challenge,~~  
854 ~~because a nonce is not necessarily unpredictable.~~

855  
856 ~~Off-line Attack: An attack where the attacker obtains some data (typically by eavesdropping on~~  
857 ~~an authentication protocol run or by penetrating a system and stealing security files) that~~  
858 ~~he/she is able to analyze in a system of his/her own choosing.~~

859  
860 ~~Online Attack: An attack against an authentication protocol where the attacker either assumes~~  
861 ~~the role of a claimant with a genuine verifier or actively alters the authentication channel.~~

862  
863 ~~Online Guessing Attack: An attack in which an attacker performs repeated logon trials by~~  
864 ~~guessing possible values of the authenticator output.~~

865  
866 ~~Passive Attack: An attack against an authentication protocol where the attacker intercepts data~~  
867 ~~traveling along the network between the claimant and verifier, but does not alter the data (i.e.,~~  
868 ~~eavesdropping).~~

869  
870 ~~Password: A secret that a claimant memorizes and uses to authenticate his or her identity.~~  
871 ~~Passwords are typically character strings.~~

872  
873 ~~Personal Identification Number (PIN): A password consisting only of decimal digits.~~

874  
875 ~~Personal Identity Verification (PIV) Card: Defined by [FIPS 201] as a physical artifact (e.g.,~~  
876 ~~identity card, smart card) issued to federal employees and contractors that contains stored~~  
877 ~~credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that~~  
878 ~~the claimed identity of the cardholder can be verified against the stored credentials by another~~  
879 ~~person (human readable and verifiable) or an automated process (computer readable and~~  
880 ~~verifiable).~~

881  
882 ~~Personally Identifiable Information (PII): As defined by OMB Circular A-130, Personally~~  
883 ~~Identifiable Information means information that can be used to distinguish or trace an~~  
884 ~~individual's identity, either alone or when combined with other information that is linked or~~  
885 ~~linkable to a specific individual.~~

886

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

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

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

894 ~~Possession and control of an authenticator: The ability to activate and use the authenticator in~~  
895 ~~an authentication protocol.~~

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

899 ~~Private Credentials: Credentials that cannot be disclosed by the CSP because the contents can~~  
900 ~~be used to compromise the authenticator.~~

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

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

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

912 ~~Public Credentials: Credentials that describe the binding in a way that does not compromise the~~  
913 ~~authenticator.~~

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

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

920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

931 ~~Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software and~~  
932 ~~workstations used for the purpose of administering certificates and public-private key pairs,~~  
933 ~~including the ability to issue, maintain, and revoke public key certificates.~~  
934  
935 ~~Registration: The process through which an applicant applies to become a subscriber of a CSP~~  
936 ~~and an RA validates the identity of the applicant on behalf of the CSP.~~  
937  
938 ~~Registration Authority (RA): A trusted entity that establishes and vouches for the identity or~~  
939 ~~attributes of a subscriber to a CSP. The RA may be an integral part of a CSP, or it may be~~  
940 ~~independent of a CSP, but it has a relationship to the CSP(s).~~  
941  
942 ~~Relying Party (RP): An entity that relies upon the subscriber's authenticator(s) and credentials~~  
943 ~~or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access~~  
944 ~~to information or a system.~~  
945  
946 ~~Remote: (As in remote authentication or remote transaction) An information exchange~~  
947 ~~between network-connected devices where the information cannot be reliably protected end-~~  
948 ~~to-end by a single organization's security controls. Note: Any information exchange across the~~  
949 ~~Internet is considered remote.~~  
950  
951 ~~Replay Attack: An attack in which the attacker is able to replay previously captured messages~~  
952 ~~(between a legitimate claimant and a verifier) to masquerade as that claimant to the verifier or~~  
953 ~~vice-versa.~~  
954  
955 ~~Risk Assessment: The process of identifying the risks to system security and determining the~~  
956 ~~probability of occurrence, the resulting impact, and additional safeguards that would mitigate~~  
957 ~~this impact. Part of Risk Management and synonymous with Risk Analysis.~~  
958  
959 ~~Salt: A non-secret value that is used in a cryptographic process, usually to ensure that the~~  
960 ~~results of computations for one instance cannot be reused by an attacker.~~  
961  
962 ~~Secondary Authenticator: A temporary secret, issued by the verifier to a successfully~~  
963 ~~authenticated subscriber as part of an assertion protocol. This secret is subsequently used, by~~  
964 ~~the subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer~~  
965 ~~assertions, assertion references, and Kerberos session keys.~~  
966  
967 ~~Secure Sockets Layer (SSL): An authentication and security protocol widely implemented in~~  
968 ~~browsers and web servers. SSL has been superseded by the newer Transport Layer Security~~  
969 ~~(TLS) protocol; TLS 1.0 is effectively SSL version 3.1.~~  
970  
971 ~~Security Assertion Mark-up Language (SAML): An XML-based security specification developed~~  
972 ~~by the Organization for the Advancement of Structured Information Standards (OASIS) for~~  
973 ~~exchanging authentication (and authorization) information between trusted entities over the~~  
974 ~~Internet.~~

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

975 ~~SAML Authentication Assertion: A SAML assertion that conveys information from a verifier to~~  
976 ~~an RP about a successful act of authentication that took place between the verifier and a~~  
977 ~~subscriber.~~

978  
979 ~~Session Hijack Attack: An attack in which the attacker is able to insert himself or herself~~  
980 ~~between a claimant and a verifier subsequent to a successful authentication exchange between~~  
981 ~~the latter two parties. The attacker is able to pose as a subscriber to the verifier or vice versa to~~  
982 ~~control session data exchange. Sessions between the claimant and the relying party can also be~~  
983 ~~similarly compromised.~~

984  
985 ~~Shared Secret: A secret used in authentication that is known to the claimant and the verifier.~~

986  
987 ~~Social Engineering: The act of deceiving an individual into revealing sensitive information by~~  
988 ~~associating with the individual to gain confidence and trust.~~

989  
990 ~~Special Publication (SP): A type of publication issued by NIST. Specifically, the Special~~  
991 ~~Publication 800-series reports on the Information Technology Laboratory's research, guidelines,~~  
992 ~~and outreach efforts in computer security, and its collaborative activities with industry,~~  
993 ~~government, and academic organizations.~~

994  
995 ~~Strongly Bound Credentials: Credentials that describe the binding between a user and~~  
996 ~~authenticator in a tamper-evident fashion.~~

997  
998 ~~Subscriber: A party who has received a credential or authenticator from a CSP.~~

999  
1000 ~~Symmetric Key: A cryptographic key that is used to perform both the cryptographic operation~~  
1001 ~~and its inverse, for example to encrypt and decrypt, or create a message authentication code~~  
1002 ~~and to verify the code.~~

1003  
1004 ~~Token: See Authenticator.~~

1005  
1006 ~~Token Authenticator: See Authenticator Output.~~

1007  
1008 ~~Token Secret: See Authenticator Secret.~~

1009  
1010 ~~Transport Layer Security (TLS): An authentication and security protocol widely implemented in~~  
1011 ~~browsers and web servers. TLS is defined by [RFC 5246]. TLS is similar to the older Secure~~  
1012 ~~Sockets Layer (SSL) protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52,~~  
1013 ~~Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations specifies~~  
1014 ~~how TLS is to be used in government applications.~~

1015  
1016 ~~Trust Anchor: A public or symmetric key that is trusted because it is directly built into hardware~~  
1017 ~~or software, or securely provisioned via out-of-band means, rather than because it is vouched~~  
1018 ~~for by another trusted entity (e.g. in a public key certificate).~~

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1019 ~~Trust Framework: In identity management, means a digital identity system with established~~  
1020 ~~identity, security, privacy, technology, and enforcement rules and policies adhered to by~~  
1021 ~~certified identity providers that are members of the identity trust framework. Members of an~~  
1022 ~~identity trust framework include identity trust framework operators and identity providers.~~  
1023 ~~Relying parties may be, but are not required to be, a member of an identity trust framework in~~  
1024 ~~order to accept an identity credential issued by a certified identity provider to verify an identity~~  
1025 ~~credential holder's identity. [§ 59.1-550, Code of Virginia]~~  
1026  
1027 ~~Unverified Name: A subscriber name that is not verified as meaningful by identity proofing.~~  
1028  
1029 ~~Valid: In reference to an ID, the quality of not being expired or revoked.~~  
1030  
1031 ~~Verified Name: A subscriber name that has been verified by identity proofing.~~  
1032  
1033 ~~Verifier: An entity that verifies the claimant's identity by verifying the claimant's possession and~~  
1034 ~~control of one or two authenticators using an authentication protocol. To do this, the verifier~~  
1035 ~~may also need to validate credentials that link the authenticator(s) and identity and check their~~  
1036 ~~status.~~  
1037  
1038 ~~Verifier Impersonation Attack: A scenario where the attacker impersonates the verifier in an~~  
1039 ~~authentication protocol, usually to capture information that can be used to masquerade as a~~  
1040 ~~claimant to the real verifier.~~  
1041  
1042 ~~Weakly Bound Credentials: Credentials that describe the binding between a user and~~  
1043 ~~authenticator in a manner that can be modified without invalidating the credential.~~  
1044  
1045 ~~Zeroize: Overwrite a memory location with data consisting entirely of bits with the value zero~~  
1046 ~~so that the data is destroyed and not recoverable. This is often contrasted with deletion~~  
1047 ~~methods that merely destroy reference to data within a file system rather than the data itself.~~  
1048  
1049 ~~Zero-knowledge Password Protocol: A password-based authentication protocol that allows a~~  
1050 ~~claimant to authenticate to a Verifier without revealing the password to the verifier. Examples~~  
1051 ~~of such protocols are EKE, SPEKE and SRP.~~

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

## 1052 **56 Background**

1053  
1054 In 2015, Virginia’s General Assembly passed the Electronic Identity Management Act (Chapter  
1055 of Title 59.1, Code of Virginia) to address demand in the state’s digital economy for secure,  
1056 privacy enhancing ~~electronic authentication~~Electronic Authentication and identity  
1057 management. Growing numbers of “communities of interest” have advocated for stronger,  
1058 scalable and interoperable identity solutions to increase consumer protection and reduce  
1059 liability for principal actors in the identity ecosystem – Identity Providers, Credential Service  
1060 Providers and Relying Parties.

1062 To address the demand contemplated by the Electronic Identity Management Act, the General  
1063 Assembly also created the Identity Management Standards Advisory Council (IMSAC) to advise  
1064 the Secretary of Technology on the adoption of identity management standards and the  
1065 creation of guidance documents, pursuant to §2.2-436. A copy of the IMSAC Charter has been  
1066 provided in Appendix 1. ~~The following guidance document has been developed by the Virginia~~  
1067 ~~Information Technologies Agency (VITA), acting on behalf of the Secretary of Technology and~~  
1068 ~~Chief Information Officer of the Commonwealth, at the direction of IMSAC. IMSAC was created~~  
1069 ~~by the General Assembly as part of the Act and advises the Secretary of Technology on the~~  
1070 ~~adoption of identity management standards and the creation of guidance documents pursuant~~  
1071 ~~to §2.2-436. A copy of the IMSAC Charter has been provided in Appendix 1.~~

1073 The Advisory Council recommends to the Secretary of Technology guidance documents relating  
1074 to (i) nationally recognized technical and data standards regarding the verification and  
1075 authentication of identity in digital and online transactions; (ii) the minimum specifications and  
1076 standards that should be included in an ~~identity~~Identity Trust Framework, as defined in §59.1-  
1077 550, so as to warrant liability protection pursuant to the Electronic Identity Management Act  
1078 (§59.1-550 et seq.); and (iii) any other related data standards or specifications concerning  
1079 reliance by third parties on identity credentials, as defined in §59.1-550.

### 1081 **Purpose Statement**

1082  
1083 This guidance document, as defined in § 2.2-4001, was developed by the Identity Management  
1084 Standards Advisory Council (IMSAC), on behalf of the Secretary of Technology, to provide  
1085 information or guidance of general applicability to the public for interpreting or implementing  
1086 the Electronic Identity Management Act. Specifically, the document establishes ~~The purpose of~~  
1087 ~~this document is to establish~~ minimum specifications for ~~electronic~~ identity management of  
1088 Non-Person Entities (NPEs) in a Digital Identity System. ~~The document assumes that the~~  
1089 ~~identity management system will be supported by a trust framework, compliant with Applicable~~  
1090 ~~Law.~~<sup>††</sup> ~~The minimum specifications also outline a data model for interoperability and discovery~~  
1091 ~~of identity information on NPEs.~~

<sup>††</sup> ~~For the purpose of this guidance document, the term “Applicable Law” shall mean laws, statutes, regulations, and rules of the jurisdiction in which each participant in an identity management system member of an Identity Trust Framework operates.~~

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1093 The document assumes that specific business, legal, and technical requirements for ~~electronic~~  
 1094 ~~authentication~~ NPEs will be established in the ~~Trust Framework~~ Identity Trust Framework for  
 1095 each distinct ~~identity management system~~ Digital Identity System, and that these requirements  
 1096 will be designed based on the ~~Electronic Authentication model~~, Identity Assurance Level (IAL),  
 1097 and Authenticator Assurance Level (AAL) requirements for the system. The document limits its  
 1098 focus to ~~electronic authentication~~ identity management for NPEs. Minimum specifications for  
 1099 other components of ~~an identity management system~~ a Digital Identity System ~~will behave been~~  
 1100 defined in separate IMSAC guidance documents in this series, pursuant to §2.2-436 and §2.2-  
 1101 437.  
 1102

## 1103 67 Minimum Specifications

1104  
 1105 Identity management (IdM) of Non-Person Entities (NPEs) has become a critical issue with the  
 1106 growth in number and level of interconnectedness of “smart” devices, particularly as these  
 1107 devices increasingly become targets of malware and cyber attacks. Despite a substantial focus  
 1108 worldwide on IdM of person entities, the parallel effort on IdM of NPEs has not achieved a  
 1109 similar level of maturity.  
 1110

1111 The National Institute of Standards and Technology (NIST) in Special Publication (SP) 800-63-3,  
 1112 and through the National Program Office of the National Strategy for Trusted Identities in  
 1113 Cyberspace (NSTIC), has established processes, protocols, and related guidance for IdM on  
 1114 persons but has not offered the same level of treatment for NPEs. Federal and State Identity  
 1115 Credential Access Management (FICAM/SICAM) Guidelines reference NPEs but do not define  
 1116 specific protocols for NPE management.  
 1117

1118 In recent years, international organizations have made substantial contributions to the  
 1119 knowledge-base relating to IdM of NPEs. Much of this effort stems from analysis on the  
 1120 “Internet of Things” (IoT), defined by the International Telecommunication Union (ITU) as a  
 1121 “global infrastructure for the information society, enabling advanced services by  
 1122 interconnecting (physical and virtual) things based on existing and evolving interoperable  
 1123 information and communication technologies.”<sup>12</sup>  
 1124

1125 The European Commission IoT Expert Group’s Subgroup on Identification, in its current-state  
 1126 analysis of the IoT, noted the following issues associated with IdM of NPEs:

- 1127 • Object Identifiers and Protocols: The question of whether to adopt a global, standardized  
 1128 scheme of unique identifiers for NPEs or continue to maintain an array of distinct identity  
 1129 spaces for NPEs with fluctuating degrees of interoperability.
- 1130 • Identifiers vs. Network Addresses: The importance of distinguishing between an NPE’s  
 1131 identifier, which establishes a unique handle for the entity, and its network address, which  
 1132 may change based on the NPE’s physical location.

<sup>12</sup> International Telecommunications Union. 2012. *Recommendation Y.2060: Overview of the Internet of Things*.  
<https://www.itu.int/rec/T-REC-Y.2060-201206-I>

- 1133 • Resolution and Discovery Functions: The need to build upon existing knowledge and  
 1134 experience with identification, naming, and addressing systems to resolve disparate  
 1135 identifiers for an NPE and enable discovery across disparate Digital Identity Systems.<sup>13</sup>  
 1136

1137 The European Commission, and other groups such as the Cloud Security Alliance, Kantara  
 1138 Initiative, and Internet Society have published guidance on how to address these and related  
 1139 issues for IdM of NPEs.<sup>14</sup> Also, the ITU has released recommendations to promote  
 1140 interoperability, resolution, and discovery of identity information on NPEs.<sup>15</sup>  
 1141 The minimum specifications defined in this document leverage the guidance and  
 1142 recommendations issued by these international organizations. First, the minimum  
 1143 specifications set general guidelines for IdM of NPEs based on the guidance from the Cloud  
 1144 Security Alliance and Kantara Initiative. Second, the minimum specifications outline a standard  
 1145 data model for NPE identity information conformant with ITU recommendations ~~for electronic~~  
 1146 ~~authentication~~.<sup>16</sup> Third, the minimum specifications present a comprehensive use case  
 1147 illustrating the complexity of issues associated with IdM of NPEs and strategies for addressing  
 1148 these issues through a standards-based reference architecture and communications protocols,  
 1149 such as those established by the European Commission and Internet Society.  
 1150

## 1151 General Guidelines

1152  
 1153 The following general guidelines have been adapted from the CSA's *Identity and Access*  
 1154 *Management for the Internet of Things – Summary Guidance*.  
 1155

- 1156 1. Integrate IdM-NPE implementation into existing IdM and IT governance frameworks.  
 1157 Considerations should include the following steps:  
 1158 a. Define a common namespace for NPEs.  
 1159 b. Establish an extensible identity lifecycle that can be applied to NPEs, designed based on  
 1160 the lifetime of the NPE and required identifier.  
 1161 c. Within the identify lifecycle, establish clear registration processes for NPEs. The rigor of  
 1162 the registration process should be dictated by the sensitivity of the data handled by a  
 1163 particular NPE.  
 1164 d. Determine the level of security protections (confidentiality, authentication,  
 1165 authorization) to be applied to unique data flows from NPE components.

<sup>13</sup> European Commission. 2012. IoT Factsheet – Identification. Report from the Internet of Things Expert Group (IoT-EG),  
 Subgroup on Identification. <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=7663&no=12>

<sup>14</sup> Cloud Security Alliance. 2016. *Identity and Access Management for the Internet of Things – Summary Guidance*.  
<https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identity-and-access-management-for-the-iot.pdf>  
 Kantara Initiative. *Identity Relationship Management: Pillars of IRM*. <https://kantarainitiative.org/irmpillars/>  
 European Commission. 2012. IoT Factsheet – Identification. Report from the Internet of Things Expert Group (IoT-EG),  
 Subgroup on Identification. <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=7663&no=12>

Internet Society. 2015. *The Internet of Things: An Overview*. <https://www.internetsociety.org/doc/iot-overview>

<sup>15</sup> The term “non-person entity” shall be used in this document in place of comparable terms currently in practice, such as “IoT  
 devices,” “digital entities,” “digital objects,” etc., in order to standardize reference terminology and remain consistent with  
 FICAM/SICAM.

<sup>16</sup> International Telecommunications Union. 2013. *Recommendation X. 1255: Framework for Discovery of Identity Management*  
*Information*. <http://www.itu.int/ITU-T/recommendations/rec.aspx?id=11951&lang=en>

Formatted: Position: Vertical: -0.04", Relative  
 to: Paragraph

- 1166 e. Establish clear authentication and authorization procedures for local access to NPEs.  
 1167 f. Define privacy protections required for different data categories. (Note: Establishing a  
 1168 framework reference definition for establishing privacy protections of Personally-  
 1169 Identifiable Information (PII) will aid in these definitions.)  
 1170 g. Determine and document whether outside organizations have access to certain  
 1171 categories of data.  
 1172 h. Define how to perform authentication and authorization for NPEs that are only  
 1173 intermittently connected to the network.  
 1174 i. Establish access control requirements that apply to NPEs according to the access control  
 1175 policies defined in the Identity Trust Framework.  
 1176  
 1177 2. Do not deploy NPE assets without changing default passwords for administrative access. If  
 1178 possible, do not deploy NPEs with only local access capabilities. Instead, attempt to  
 1179 integrate all NPE assets into the enterprise IdM system. (Note: This guidance does not apply  
 1180 to consumer-based NPEs that are attached to the enterprise network. New concepts similar  
 1181 to those required for bring-your-own-device (BYOD) registration of devices would need to  
 1182 be applied to that segment of NPE assets.  
 1183  
 1184 3. Evaluate a move to Identity Relationship Management (IRM) in place of traditional IAM, as  
 1185 recommended by the Kantara Initiative.<sup>17</sup> IRM is more suitable to NPEs than traditional IAM  
 1186 and is based on a set of pillars that include a focus on consumers and things over  
 1187 employees, Internet-scale over Enterprise-scale, and Borderless over perimeter. Identify  
 1188 and evaluate IRM vendor solutions as a possible fit for NPE identity requirements.  
 1189  
 1190 4. Design authentication and authorization schemes based on system-level threat models.  
 1191 Evaluate each individual NPE asset's implementation and choose vendors that have adhered  
 1192 to applicable standards and/or sought guidance or followed best practices from industry  
 1193 security groups. Take into account system vulnerabilities.  
 1194  
 1195 5. Smartphones for authentication on IoT. Mobile Devices and Telecommunication networks  
 1196 play a major role in the IoT. Smartphones will potentially be used as one means of  
 1197 authentication step to access things surrounding us. The features that makes the  
 1198 smartphone a powerful authentication factor needs to be tightly integrated with other  
 1199 devices. The next generation smartphones would drive different types of authentication  
 1200 mechanisms like facial recognition using the front-facing camera, voice recognition, gesture  
 1201 dynamics and handling dynamics in addition to traditional biometrics such as fingerprints.  
 1202 These smart phones could be used for enterprise level local authentication to IoT devices.  
 1203  
 1204 6. Create reference architectures for your NPE assets using *ITU-T Y.2060: Overview of the*  
 1205 *Internet of Things* as a starting point. NPE reference architectures enable consistent  
 1206 implementation of authentication, authorization, and accounting (AAA) services across all  
 1207 NPE assets in the infrastructure and can be used to test the overall access of systems at

<sup>17</sup> For more information in the Kantara Initiative's guidance on IRM, visit <https://kantarainitiative.org/irmpillars/>

- 1208 every level, from the individual machine to networks of machines at various layers in the  
1209 technology stack. Identify the most vulnerable devices within the enterprise and apply MFA  
1210 whenever possible.  
1211
- 1212 7. Plan for the introduction of IPv6. Organizations have not fully moved to IPv6 as the industry  
1213 is still in a state of prolonged transition. There are many NPEs that are designed to use IPv4,  
1214 so planning now for how an NPE asset designed to use IPv4 will talk to an NPE asset  
1215 designed to use IPv6, in a M2M implementation scenario, is needed. To make this feasible,  
1216 consider a Software Defined Networking (SDN) mechanism that can allow these devices to  
1217 talk to each other to provide the intended service.  
1218
- 1219 8. Consider design updates to Public Key Infrastructure (PKI) environment to support  
1220 provisioning of certificates to NPE assets. Use certificates whenever possible for NPE  
1221 authentication and confidentiality during Transport Layer Security (TLS) and other protocol  
1222 negotiations, as well as to support various other identity bindings when integrating with  
1223 other access control mechanisms. Ensure that the PKI architecture supports standard  
1224 services such as revocation checking, trust management, enrollment and registration  
1225 procedures, and compromise recovery. Evaluate alternative certificate types that are  
1226 optimized for NPEs, such as the smaller IEEE 1609.2 credential format. Evaluate additional  
1227 services such as Online Certificate Status Protocol (OCSP)- stapling or the Domain Name  
1228 System (DNS) Authentication of Named Entities (DANE) means of supporting an enhanced  
1229 NPE ecosystem. These technologies can improve security and reduce the burden on the  
1230 network and sensors as they are not required to communicate with an OCSP server. Ensure  
1231 that the PKI can scale to issue certificates to the larger quantities of NPE assets.  
1232
- 1233 9. Establish a plan for sharing NPE-related data with device manufacturers. Device  
1234 manufacturers will continue to want to have device data access in order to monitor device  
1235 health, track statistics, and be able to provide support to their customers. This data is  
1236 collected and stored within various types of databases. Make sure to implement an  
1237 authorization model for these back-end data stores such that 1) is compliant with relevant  
1238 privacy regulations and 2) allows the minimal access required by manufacturers and other  
1239 third parties.  
1240
- 1241 10. Implement an AAA server that allow consumers to define preferences and provide services'  
1242 consent for access to consumer profile data. An NPE implementation is one such service.  
1243 This requires management of external identities such as consumers and patients, who are  
1244 allowed to give their consent preferences for which attributes of their profile information  
1245 can be shared and to whom. In many cases, this requires the integration of AAA services  
1246 with third party services that manage consumer and business partner preferences for  
1247 handling of data.  
1248
- 1249 11. Consider integrating the identity management system with a building's Physical Access  
1250 Control System (PACS) to enable additional security measures, such as selectively

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

- 1251 provisioning what doors and entrances a person's badge can access. These security  
 1252 enhancements will provide improved physical protection to NPE assets.  
 1253
- 1254 12. Implement restrictive logic in identity management workflows to proactively restrict access  
 1255 to NPE-related systems and devices if a person has not had the necessary prerequisites as  
 1256 specified by the access governance framework. Examples of prerequisites include training  
 1257 and background checks.  
 1258
- 1259 13. Implement a privileged user management system to ensure that administrators can access  
 1260 and monitor NPE systems and devices. This includes session monitoring of privileged  
 1261 sessions, protection of passwords to service accounts, and frequent password rotation.  
 1262
- 1263 14. Extend where possible the use of current asset management to inventory and document  
 1264 NPE assets. Categorize them based on risk and assign owners. Modify access records to  
 1265 support asset ownership, asset deployment, and any required revocation or asset lifecycle  
 1266 workflows. Integrate a service desk system that audits and automates the opening of tickets  
 1267 so that revocation of physical assets occurs in a system of record.  
 1268
- 1269 15. Invest in a well-documented plan for how to respond to failures and breaches when they  
 1270 occur. One example is an Incident Handling or an Incident Response plan. Note that this  
 1271 plan should be made a part of the incident management process and workflows.  
 1272
- 1273 16. Establish relationship mappings between people and NPE assets. This includes establishing  
 1274 explicit authorizations for people's authorized behavior on specific data sets. Enforce access  
 1275 management by both users and things. Implement MFA where possible for user access to  
 1276 NPE-centric data.  
 1277
- 1278 17. Develop effective AAA mechanisms for sensor nodes based on the context and service  
 1279 security requirements. Wireless sensor nodes can be a key element for NPE asset  
 1280 implementations; however, AAA of the sensor nodes in a wireless mesh network is not yet  
 1281 fool proof due to limitations in energy and computing power. Consider context as a way to  
 1282 determine the rigor of the authentication required based on risk introduced by a particular  
 1283 sensor node. Examples include location/coordinates, time-of-day, end-device/system being  
 1284 accessed, or data types being transmitted/received. Note: In some attack scenarios,  
 1285 context information is easily stolen, forged, or proxied. Also, evaluate the risk associated  
 1286 with context false-negatives and the potential risk that may result when legitimate users are  
 1287 incorrectly blocked (e.g., bad device clocks, upgraded endpoints, unexpected but legitimate  
 1288 locations, loss of GPS signal, etc). Perform threat modeling to determine the most  
 1289 appropriate AAA mechanisms for sensor nodes.  
 1290
- 1291 18. Leverage security controls built into standards-based NPE protocols such as CoAP, DDS, and  
 1292 REST to allow for interoperable authentication and authorization transactions between  
 1293 different manufacturers' NPE assets. A list of common NPE communication protocols and  
 1294 assertions has been provided in **Table 1**.

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1295  
1296

DRAFT

**Formatted:** Position: Vertical: -0.04", Relative to: Paragraph

1297  
1298**Table 1. Common NPE Communication Protocols and Assertions**

Protocol	M2M Authentication Options	Description
MQTT	Username/Password	MQTT allows for sending a username and password, although recommends that the password be no longer than 12 characters. Username and password are sent in the clear, and as such it is critical that TLS be employed when using MQTT.
CoAP	Pre-Shared Key Raw-Shared Key Certificate	CoAP supports multiple authentication options for device-to-device communication. Pair with Datagram TLS (D-TLS) for higher level confidentiality services.
XMPP	Multiple Options Available Depending on Protocol	XMPP supports a variety of authentication patterns via the Simple Authentication and Security Layer (SASL – RFC4422). Mechanisms include one-way anonymous as well as mutual authentication with encrypted passwords, certificates and other means implemented through the SASL abstraction layer.
DDS	X.509 Certificates (PKI) using RSA and DSA Algorithms (Tokens)	The Object Management Groups Data Distribution Standard (DDS) Security Specification provides endpoint authentication and key establishment to perform subsequent message data origin authentication (i.e., HMAC). Both digital certificates and various identity/authorization token types are supported.
Zigbee	Pre-Shared Key	Zigbee provides both network and application level authentication (and encryption) through the use of Master key (optional), Network (mandatory) and Application Link keys (optional)
HTTP/REST	Basic Authentication (cleartext) (TLS Methods) OAUTH2	HTTP/REST typically requires the support of the TLS protocol for authentication and confidentiality services. Although Basic Authentication (where credentials are passed in the clear) can be used under the cover of TLS, this is not a recommended practice. Instead attempt to stand up a token-based authentication approach such as OAUTH 2

1299

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

Protocol	M2M Authentication Options	Description
Bluetooth	Shared Key	Bluetooth provides authentication services through two different device pairing options, Standard and Simple Pairing. The Standard Pairing method is automatic; the Simple Pairing method includes a human-in-loop to verify (following a simple Diffie-Hellman exchange) that the two devices display the same hash of the established key. Bluetooth offers both one-way as well as mutual authentication options. Bluetooth secure simple pairing offers 'Just works', 'Passkey entry' and 'Out of Box' options for device-device authentication
Bluetooth-LE	Unencrypted data authenticated using Connection Signature Resolving Key (CSRK) Device Identity/Privacy is via an Identity Resolving Key (IRK)	Bluetooth-LE introduces a two-factor authentication system, the LE Secure Connections pairing model which combines – based on device capability – several of the available association models available. In addition, Elliptic-Curve Diffie Hellman is used for key exchange.

Source: CSA Identity and Access Management for the Internet of Things – Summary Guidance, pp 10-11.

1300  
1301

DRAFT

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1302 Data Model for NPE Identity Information

1303

1304 The following data model for NPE identity information has been adapted from ITU  
1305 *Recommendation X. 1255: Framework for Discovery of Identity Management Information.*

1306

1307 The data model for NPE identity information described in this section provides a uniform means  
1308 to represent metadata records as NPEs, and can also be used to represent other types of  
1309 information as NPEs. It is a logical model that allows for multiple forms of encoding and  
1310 storage, and enables a single point of reference (i.e., the identifier) for many types of  
1311 information that may be available in digital form.

1312

1313 Each NPE has an intrinsic set of attributes, a user-defined set of attributes, embodied in one or  
1314 more elements and zero or more additional elements containing information such as text,  
1315 video or images represented in digital form. All of these elements can be made available  
1316 through a precisely defined NPE specification, which incorporates the capability for  
1317 authentication using public key security, and perhaps other means of authentication using  
1318 higher-level APIs, as might be implemented by NPE repositories. This provides access with  
1319 privacy and security to NPEs.

1320

1321 The essential fixed attribute of a NPE is its associated unique persistent identifier, which can be  
1322 resolved to current state information about the NPE, including its location(s), access controls,  
1323 and validation, by submitting a resolution request to the resolution system. Examples of other  
1324 intrinsic NPE element attributes are: date last modified, date created, and size. User extensible  
1325 attributes may be set by the users with appropriate permissions.

1326

1327 Attributes that are not specifically addressed by the basic NPE data model include ownership,  
1328 authentication and access terms and conditions. These attributes will be an important part of  
1329 most NPE implementations; however, a single solution seems unlikely. Ownership and access  
1330 control information will likely be contained in user extensible NPE attributes or in separate data  
1331 elements. This provides a common way to deal with various ownership and information  
1332 management schemes, as well as multiple authentication and authorization schemes, without  
1333 making the assumption that a single approach will be used across all domains and user  
1334 communities.

1335

1336 The combination of a standard data model, a defined protocol for interacting with that data  
1337 model, and an identifier/resolution system, provides a key ingredient for the coherent long-  
1338 term management of information in a digital context. The resolution system should be a  
1339 distributed, secure, high-performance resolution system designed to enable persistent  
1340 reference to digital entities over long periods of time and over changes in location, access  
1341 methods, ownership and other mutable attributes.

1342

1343

1344

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1345 The core capability for discovery of IdM information results from the use of the registry  
 1346 component, which includes the repository. The function of an individual registry is to federate  
 1347 across collections of NPEs, enabling end users and applications to search through and navigate  
 1348 the universe of registered entities.

1349  
 1350 Repositories that contain collections of NPEs can contribute metadata about the NPEs for which  
 1351 they are responsible to one or more registries. A single registry can collect metadata from  
 1352 multiple repositories, and a single repository can send metadata to multiple registries. The  
 1353 registries can provide search and reporting functions over the represented entities and provide  
 1354 an entry point into the structured world of NPEs and repositories.

1355  
 1356 There may be situations in which the registries are not, strictly speaking, needed, e.g., in the  
 1357 case where a direct reference to a NPE, in the form of its identifier, is embedded in another NPE  
 1358 or in a message or other document. In many cases, however, the end user, or automated  
 1359 process acting on behalf of a user, will not know the identifier to begin with, and will have to  
 1360 use some variety of search or sorting process to discover the needed reference. Even if a user  
 1361 knows the identifier, the user may not know how to resolve it, or how to interpret the  
 1362 resolution results. Recording the existence of NPEs in registries can help to solve that problem  
 1363 in a very general way.

1364  
 1365 By defining operations that interact with a specified data model, digital entities can be  
 1366 constructed and used to represent most types of structured information. A standard NPE data  
 1367 model has been illustrated in **Figure 1**. Representation of the entities in a form that is  
 1368 independent of the implementation details of the relevant storage system is an essential  
 1369 interoperability feature, as it allows multiple storage formats and approaches to be normalized  
 1370 to a single logical model.

1371  
 1372 **Figure 1. Standard Data Model for NPE Identity Information**  
 1373

	NON-PERSON ENTITY	
	ATTRIBUTE	EXAMPLE
<b>Intrinsic Attributes</b>	Unique Identifier (ID)	84321/ab5
	Date Created	2016/02/10
	Date Modified	2016/10/30
<b>User-Defined Attributes</b>	Object Type	89754/123
	Permission Scheme A	84321/ab5
	More...	...
<b>Additional Elements (1-N)</b>	<b>ELEMENT 1</b>	
	Intrinsic Attributes	
	User-Defined Attributes	
	Data	

Source: ITU Recommendation X.1255, p. 9.

1374  
 1375

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1376 Except for the persistent identifier at the top, all data shown in Figure 1 is conceptual only. Each  
1377 element of a digital entity can take different forms, i.e., digital entity references by identifier, an  
1378 actual digital entity, plain local data suitably typed.

1379  
1380 Registries may use or incorporate repositories to store metadata records; and repositories are  
1381 information management systems that provide access to collections of NPEs via the digital  
1382 entity interface protocol. Repositories may generally be thought to incorporate the digital  
1383 entities to which they provide access. A more detailed view however, would show them as  
1384 portals into various storage and information systems, mapping the raw data into digital entities  
1385 that may be stored locally or remotely. This could be as simple as a file system holding the data  
1386 for a given NPE in one or more files that are not known or visible to the user.

1387  
1388 Alternatively, especially for complex digital entities, data may be spread across multiple  
1389 locations and systems and brought together in NPE form only on demand, with one storage  
1390 component holding the “map” of the entity and the bulk of the data held in other systems. This  
1391 technique of interacting with existing systems is key to federation, as the information in an  
1392 arbitrarily complex information system can be logically divided into NPEs, and those NPEs made  
1393 available in a standardized fashion, using an instance of a NPE within user-centric applications.

1394  
1395 A NPE client can locate one or more repositories for a given NPE by resolving its identifier. The  
1396 resolution request will return the location of one or more relevant repositories with which the  
1397 client can initiate a NPE transaction.

1398  
1399 The NPE repository software normally provides multiple network interfaces for performing  
1400 operations on digital entities, namely, the digital entity interface protocol for interacting with  
1401 the NPE itself, as well as locally desirable interfaces as determined by current technology  
1402 options. The various interfaces each have their own benefits in terms of security, compatibility  
1403 with proxy servers and the use of ubiquitous client software. Redundancy is built into the digital  
1404 entity interface protocol, along with strong individual and group authentication. Redundancy is  
1405 supported by a mirroring system in which each NPE repository communicates with the others  
1406 to ensure that replicated entities are kept in sync. Authentication is based on either secret or  
1407 public/private keys or other authentication mechanisms.

1408  
1409 Other notable features include replication, allowing easy mirroring across repositories and  
1410 extensibility through a plug-in mechanism. Plug-ins could be built to manage both entity type  
1411 specific activities, e.g., parsing a video format and dispensing a requested section, or activities  
1412 oriented to network services, e.g., contributing metadata to a NPE registry.

1413  
1414  
1415  
1416  
1417  
1418

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

## 1419 **7.8 IdM of NPE Use Case: Public Health Emergency Response**

1420 Purpose: To illustrate the complex challenges associated with IdM of NPEs across jurisdictions  
 1421 and domains of governance. An architecture model outlining the IdM and communications  
 1422 protocols required for the use case has been provided in **Figure 2**.  
 1423

1424 Use Case Scenario: Emergency response involving a biological hazard event within a populated  
 1425 urban area. Public health officials/NPEs must communicate with emergency management  
 1426 personnel/NPEs and hospital personnel/NPEs to address the public health impacts resulting  
 1427 from the biological hazard.  
 1428

### 1429 NPE Settings:

- 1431 Human – NPEs attached to or inside the human body for vital signs
- 1432 Hazard Site – NPEs for remote sensing of conditions in urban hazard zone
- 1433 Vehicles – NPEs and applications/components within drone units
- 1434 Supplies – NPEs delivered by drones, such as medications, and their tracking devices
- 1435 Built Environment – NPEs for monitoring conditions in residential/commercial structures<sup>18</sup>

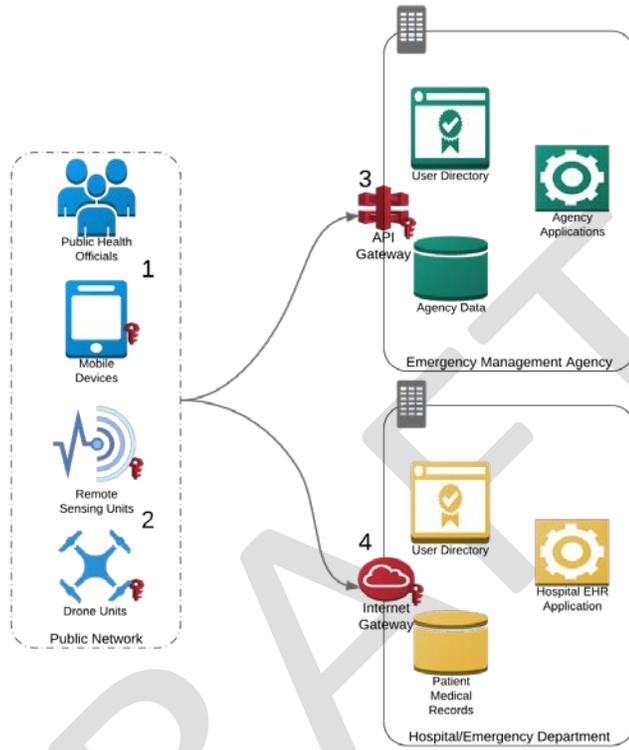
### 1436 Runtime Flows (Figure 2):

- 1437 1. Public health officials rely on authenticated NPEs for mobile communications and to  
 1438 monitor real-time feeds from remote sensing units to evaluate air, soil, and water  
 1439 conditions within the hazard zone – both in the outside and in the built environment  
 1440 (machine-to-machine).  
 1441
- 1442 2. Public health officials use authenticated drone technology to deliver medical supplies  
 1443 and measure vital signs of affected persons onsite (human-machine); IdM and data  
 1444 management must be compliant with the Health Insurance Portability and  
 1445 Accountability Act (HIPAA, P.L. 104-191) Security and Privacy Rules.  
 1446
- 1447 3. Public health officials authenticate to the emergency management agency’s applications  
 1448 to submit data from monitoring activity (application/API).  
 1449
- 1450 4. Public health officials authenticate to a hospital’s electronic health record system to  
 1451 submit patient-level data collected from persons within hazard zone in advance of  
 1452 transport to the emergency department (application/API); IdM and data management  
 1453 must be compliant with the Health Insurance Portability and Accountability Act (HIPAA,  
 1454 P.L. 104-191) Security and Privacy Rules.

<sup>18</sup> Internet Society. 2015. *The Internet of Things: An Overview*. <https://www.internetsociety.org/doc/iot-overview>  
 Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. 2015. *The Internet of Things: Mapping the Value Beyond the Hype*. McKinsey Global Institute. p.3.  
<http://www.mckinsey.com/insights/business-technology/the-internet-of-things-the-value-of-digitizing-the-physical-world>

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1455 **Figure 2. IdM of NPEs Use Case Architecture Model**



1456  
1457  
1458

DRAFT

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1459 In addition, certain registration, identity proofing, and issuance processes performed by the  
1460 credential service provider (CSP) may be delegated to an entity known as the registration  
1461 authority (RA) or identity manager (IM). A close relationship between the RA/IM and CSP is  
1462 typical, and the nature of this relationship may differ among RAs, IMs, and CSPs. The minimum  
1463 specifications defined in this document assume that relationships between participants and  
1464 their requirements are established in the trust framework for the identity management system.

1465  
1466 Electronic authentication begins with registration (also referred to as enrollment). The usual  
1467 sequence for registration proceeds as follows. An applicant applies to a CSP. If approved, the  
1468 CSP creates a credential and binds it to one or more authenticators. The credential includes an  
1469 identifier, which can be pseudonymous, and one or more attributes that the CSP has verified.  
1470 The authenticators may be issued by the CSP, generated/provided directly by the subscriber, or  
1471 provided by a third party. The authenticator and credential may be used in subsequent  
1472 authentication events.

1473  
1474 The process used to verify an applicant's association with their real world identity is called  
1475 identity proofing. The strength of identity proofing is described by a categorization called the  
1476 identity assurance level (IAL, see subsection on Assurance Level Model below in this document).  
1477 Minimum specifications for identity proofing and verification during the registration process  
1478 have been established in *ITRM Guidance Document: Identity Proofing and Verification*.

1479  
1480 At IAL 1, identity proofing is not required, therefore any attribute information provided by the  
1481 subscriber is self-asserted and not verified. At IAL 2 and 3, identity proofing is required, but the  
1482 CSP may assert verified attribute values, verified attribute claims, pseudonymous identifiers, or  
1483 nothing. This information assists Relying Parties (RPs) in making access control or authorization  
1484 decisions. RPs may decide that their required IAL is 2 or 3, but may only need specific  
1485 attributes, and perhaps attributes that retain an individual's pseudonymity. A relying party may  
1486 also employ a federated identity approach where the RP outsources all identity proofing,  
1487 attribute collection, and attribute storage to a CSP.

1488  
1489 In these minimum specifications, the party to be authenticated is called a claimant and the  
1490 party verifying that identity is called a verifier. When a claimant successfully demonstrates  
1491 possession and control of one or more authenticators to a verifier through an authentication  
1492 protocol, the verifier can verify that the claimant is a valid subscriber. The verifier passes on an  
1493 assertion about the subscriber, who may be either pseudonymous or non-pseudonymous, to  
1494 the RP. That assertion includes an identifier, and may include identity information about the  
1495 subscriber, such as the name, or other attributes that were verified in the enrollment process  
1496 (subject to the policies of the CSP and the trust framework for the system). When the verifier is  
1497 also the RP, the assertion may be implicit. The RP can use the authenticated information  
1498 provided by the verifier to make access control or authorization decisions.

1499  
1500 Authentication establishes confidence in the claimant's identity, and in some cases in the  
1501 claimant's attributes. Authentication does not determine the claimant's authorizations or  
1502 access privileges; this is a separate decision. RPs will use a subscriber's authenticated identity

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1503 ~~and attributes with other factors to make access control or authorization decisions. Nothing in~~  
1504 ~~this document precludes RPs from requesting additional information from a subscriber that has~~  
1505 ~~successfully authenticated.~~

1506  
1507 ~~The strength of the authentication process is described by a categorization called the~~  
1508 ~~authenticator assurance level (AAL). AAL 1 requires single factor authentication and is~~  
1509 ~~permitted with a variety of different authenticator types. At AAL 2, authentication requires two~~  
1510 ~~authentication factors for additional security. Authentication at the highest level, AAL 3,~~  
1511 ~~requires the use of a hardware-based authenticator and one other factor.~~

1512  
1513 ~~As part of authentication, mechanisms such as device identity or geo-location may be used to~~  
1514 ~~identify or prevent possible authentication false positives. While these mechanisms do not~~  
1515 ~~directly increase the authenticator assurance level, they can enforce security policies and~~  
1516 ~~mitigate risks. In many cases, the authentication process and services will be shared by many~~  
1517 ~~applications and agencies. However, it is the individual agency or application acting as the RP~~  
1518 ~~that shall make the decision to grant access or process a transaction based on the specific~~  
1519 ~~application requirements.~~

#### 1520 1521 ~~Authentication Components and Process Flows~~

1522  
1523 ~~The various entities and interactions that comprise the electronic authentication model defined~~  
1524 ~~in these minimum specifications have been illustrated below in **Figure 1**. The left shows the~~  
1525 ~~enrollment, credential issuance, lifecycle management activities, and the stages an individual~~  
1526 ~~transitions, based on the specific phase of the identity proofing and authentication process.~~

1527  
1528 ~~The authentication process begins with the claimant demonstrating to the verifier possession~~  
1529 ~~and control of an authenticator that is bound to the asserted identity through an authentication~~  
1530 ~~protocol. Once possession and control have been demonstrated, the verifier confirms that the~~  
1531 ~~credential remains valid, usually by interacting with the CSP.~~

1532  
1533 ~~The exact nature of the interaction between the verifier and the claimant during the~~  
1534 ~~authentication protocol contributes to the overall security of the system. Well-designed~~  
1535 ~~protocols can protect the integrity and confidentiality of traffic between the claimant and the~~  
1536 ~~verifier both during and after the authentication exchange, and it can help limit the damage~~  
1537 ~~that can be done by an attacker masquerading as a legitimate verifier.~~

1538  
1539 ~~Additionally, mechanisms located at the verifier can mitigate online guessing attacks against~~  
1540 ~~lower entropy secrets like passwords and PINs by limiting the rate at which an attacker can~~  
1541 ~~make authentication attempts or otherwise delaying incorrect attempts. Generally, this is done~~  
1542 ~~by keeping track of and limiting the number of unsuccessful attempts, since the premise of an~~  
1543 ~~online guessing attack is that most attempts will fail.~~

1544  
1545 ~~The verifier is a functional role, but is frequently implemented in combination with the CSP~~  
1546 ~~and/or the RP. If the verifier is a separate entity from the CSP, it is often desirable to ensure~~

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1547 ~~that the verifier does not learn the subscriber's authenticator secret in the process of~~  
1548 ~~authentication, or at least to ensure that the verifier does not have unrestricted access to~~  
1549 ~~secrets stored by the CSP.~~

1550 ~~The usual sequence of interactions in the authentication process is as follows:~~

- 1551 ~~1. An applicant applies to a CSP through a registration process.~~
- 1552 ~~2. The CSP identity proofs that applicant. Upon successful proofing, the applicant becomes~~  
1553 ~~a subscriber.~~
- 1554 ~~3. An authenticator and a corresponding credential are established between the CSP and~~  
1555 ~~the new subscriber.~~
- 1556 ~~4. The CSP maintains the credential, its status, and the enrollment data collected for the~~  
1557 ~~lifetime of the credential. The subscriber maintains his or her authenticator.~~

1560 ~~Other sequences are less common, but could also achieve the same functional requirements.~~

1561 ~~The right side of Figure 1 shows the entities and the interactions related to using an~~  
1562 ~~authenticator to perform electronic authentication. When the subscriber needs to authenticate~~  
1563 ~~to perform a transaction, he or she becomes a claimant to a verifier. The interactions are as~~  
1564 ~~follows:~~

- 1565 ~~1. The claimant proves to the verifier that he or she possesses and controls the~~  
1566 ~~authenticator through an authentication protocol.~~
- 1567 ~~2. The verifier interacts with the CSP to validate the credential that binds the subscriber's~~  
1568 ~~identity to his or her authenticator and to optionally obtain claimant attributes.~~
- 1569 ~~3. If the verifier is separate from the RP (application), the verifier provides an assertion~~  
1570 ~~about the subscriber to the RP, which may use the information in the assertion to make~~  
1571 ~~an access control or authorization decision.~~
- 1572 ~~4. An authenticated session is established between the subscriber and the RP.~~

1574 ~~In all cases, the RP should request the attributes it requires from a CSP prior to authentication~~  
1575 ~~of the claimant. In addition, the claimant should be requested to consent to the release of~~  
1576 ~~those attributes prior to generation and release of an assertion.~~

1578 ~~In some cases, the verifier does not need to communicate in real time with the CSP to complete~~  
1579 ~~the authentication activity (e.g., some uses of digital certificates). Therefore, the dashed line~~  
1580 ~~between the verifier and the CSP represents a logical link between the two entities rather than~~  
1581 ~~a physical link. In some implementations, the verifier, RP and the CSP functions may be~~  
1582 ~~distributed and separated as shown in Figure 1; however, if these functions reside on the same~~  
1583 ~~platform, the interactions between the components are local messages between applications~~  
1584 ~~running on the same system rather than protocols over shared untrusted networks.~~

1586 ~~As noted above, CSPs maintain status information about issued credentials. CSPs may assign a~~  
1587 ~~finite lifetime to a credential in order to limit the maintenance period. When the status~~  
1588 ~~changes, or when the credentials near expiration, credentials may be renewed or re-issued; or,~~  
1589 ~~the credential may be revoked or destroyed. Typically, the subscriber authenticates to the CSP~~  
1590 ~~using his or her existing, unexpired authenticator and credential in order to request issuance of~~

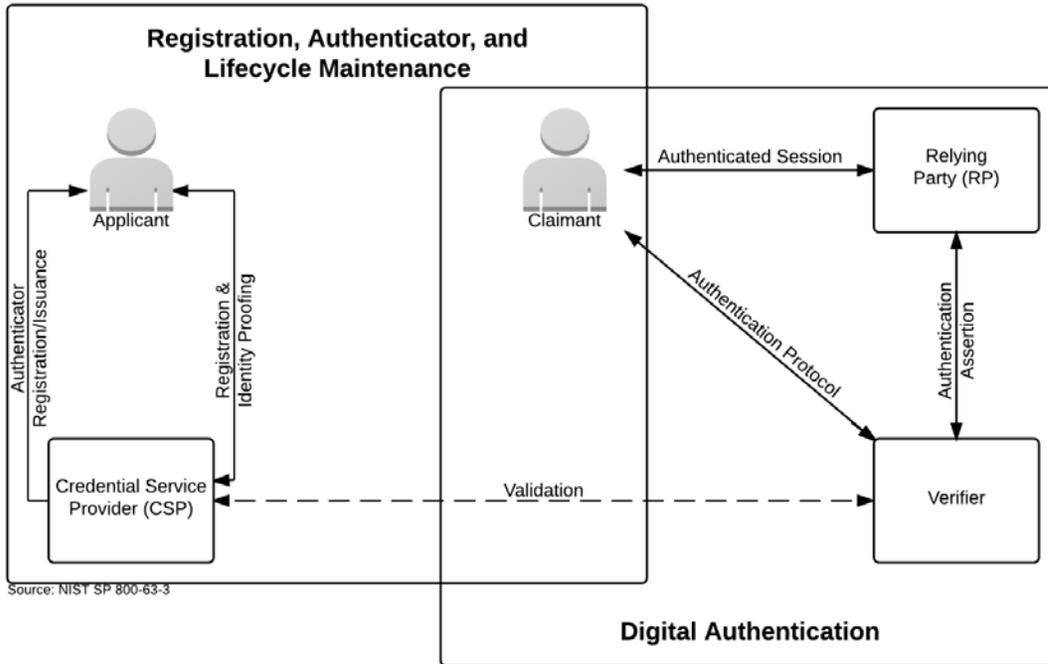
Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1591 ~~a new authenticator and credential. If the subscriber fails to request authenticator and~~  
1592 ~~credential re-issuance prior to their expiration or revocation, he or she may be required to~~  
1593 ~~repeat the enrollment process to obtain a new authenticator and credential. Alternatively, the~~  
1594 ~~CSP may choose to accept a request during a grace period after expiration.~~

DRAFT

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1595 **Figure 1. Electronic Authentication Model**



1596  
1597  
1598 Source: NIST SP 800-63-3, accessible at <https://pages.nist.gov/800-63-3/sp800-63-3.html>  
1599 Note: Figure 1 illustrates the model for electronic authentication in an identity management system, as documented in NIST SP 800-63-3  
1600 (Public Review), containing all components, requirements, and specifications recommended by IMSAC. However, the minimum  
1601 specifications defined in this document have been developed to accommodate requirements for electronic authentication established  
1602 under other national and international standards.  
1603

1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643

~~Authentication Protocols and Lifecycle Management~~

~~Authenticators~~

~~The established paradigm for electronic authentication identifies three factors as the cornerstone of authentication:~~

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

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

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

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

~~Shared secrets stored on authenticators may be either symmetric keys or passwords. While they can be used in similar protocols, one important difference between the two is how they relate to the subscriber. While symmetric keys are generally stored in hardware or software that the subscriber controls, passwords are intended to be memorized by the subscriber. As such, keys are something the subscriber has, while passwords are something he or she knows. Since passwords are committed to memory,~~

Formatted: Width: 8.5", Height: 11",  
Numbering: Continuous

Formatted: Font: 13 pt

1644 they usually do not have as many possible values as cryptographic keys, and, in many  
1645 protocols, are severely vulnerable to network attacks that are more restricted for keys.

1646  
1647 Moreover, the entry of passwords into systems (usually through a keyboard) presents  
1648 the opportunity for very simple keyboard logging attacks, and may also allow those  
1649 nearby to learn the password by watching it being entered. Therefore, keys and  
1650 passwords demonstrate somewhat separate authentication properties (something you  
1651 have rather than something you know). When using either public key pairs or shared  
1652 secrets, the subscriber has a duty to maintain exclusive control of his or her  
1653 authenticator, since possession and control of the authenticator is used to authenticate  
1654 the claimant's identity.

1655  
1656 The minimum specifications defined in this document assume that authenticators  
1657 always contain a secret. Authentication factors classified as something you know are not  
1658 necessarily secrets. Knowledge based authentication, where the claimant is prompted  
1659 to answer questions that can be confirmed from public databases, also does not  
1660 constitute an acceptable secret for electronic authentication. More generally,  
1661 something you are does not generally constitute a secret. However, the requirements  
1662 for some identity management systems may allow the use of biometrics as an  
1663 authenticator.

1664  
1665 Biometric characteristics are unique personal attributes that can be used to verify the  
1666 identity of a person who is physically present at the point of verification. They include  
1667 facial features, fingerprints, iris patterns, voiceprints, and many other characteristics.  
1668 NIST recommends that biometrics be used in the enrollment process for higher levels of  
1669 assurance to later help prevent a subscriber who is registered from repudiating the  
1670 enrollment, to help identify those who commit enrollment fraud, and to unlock  
1671 authenticators. The specific requirements for the use of biometrics must be defined in  
1672 the trust framework for the system.

1673  
1674 The minimum specifications in this document encourage identity management systems  
1675 to use authentication processes and protocols that incorporate all three factors, as a  
1676 means of enhancing system security. An electronic authentication system may  
1677 incorporate multiple factors in either of two ways. The system may be implemented so  
1678 that multiple factors are presented to the verifier, or some factors may be used to  
1679 protect a secret presented to the verifier. If multiple factors are presented to the  
1680 verifier, each will need to be an authenticator (and therefore contain a secret). If a  
1681 single factor is presented to the verifier, the additional factors are used to protect the  
1682 authenticator and need not themselves be authenticators.

1683

1684 **Credentials**

1685 ~~As described in the preceding sections, credentials bind an authenticator to the~~  
1686 ~~subscriber as part of the issuance process. Credentials are stored and maintained by the~~  
1687 ~~CSP. The claimant possesses an authenticator, but is not necessarily in possession of the~~  
1688 ~~electronic credentials. For example, database entries containing the user attributes are~~  
1689 ~~considered to be credentials for the purpose of this document but are possessed by the~~  
1690 ~~verifier.~~

1691  
1692 **Assertions**

1693 ~~Upon completion of the electronic authentication process, the verifier generates an~~  
1694 ~~assertion containing the result of the authentication and provides it to the RP. If the~~  
1695 ~~verifier is implemented in combination with the RP, the assertion is implicit. If the~~  
1696 ~~verifier is a separate entity from the RP, as in typical federated identity models, the~~  
1697 ~~assertion is used to communicate the result of the authentication process, and~~  
1698 ~~optionally information about the subscriber, from the verifier to the RP.~~  
1699 ~~Assertions may be communicated directly to the RP, or can be forwarded through the~~  
1700 ~~subscriber, which has further implications for system design. An RP trusts an assertion~~  
1701 ~~based on the source, the time of creation, and the corresponding trust framework that~~  
1702 ~~governs the policies and process of CSPs and RPs. The verifier is responsible for~~  
1703 ~~providing a mechanism by which the integrity of the assertion can be confirmed.~~

1704  
1705 ~~The RP is responsible for authenticating the source (e.g., the verifier) and for confirming~~  
1706 ~~the integrity of the assertion. When the verifier passes the assertion through the~~  
1707 ~~subscriber, the verifier must protect the integrity of the assertion in such a way that it~~  
1708 ~~cannot be modified by the subscriber. However, if the verifier and the RP communicate~~  
1709 ~~directly, a protected session may be used to provide the integrity protection. When~~  
1710 ~~sending assertions across a network, the verifier is responsible for ensuring that any~~  
1711 ~~sensitive subscriber information contained in the assertion can only be extracted by an~~  
1712 ~~RP that it trusts to maintain the information's confidentiality.~~

1713  
1714 **Examples of assertions include:**

- 1715 ~~• SAML Assertions — SAML assertions are specified using a mark-up language~~  
1716 ~~intended for describing security assertions. They can be used by a verifier to~~  
1717 ~~make a statement to an RP about the identity of a claimant. SAML assertions may~~  
1718 ~~be digitally signed.~~
- 1719 ~~• OpenID Connect Claims — OpenID Connect are specified using JavaScript Object~~  
1720 ~~Notation (JSON) for describing security, and optionally, user claims. JSON user~~  
1721 ~~info claims may be digitally signed.~~

1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737

• ~~Kerberos Tickets – Kerberos Tickets allow a ticket granting authority to issue session keys to two authenticated parties using symmetric key based encapsulation schemes.~~

~~Relying Parties~~

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

- Formatted: Font: Not Bold
- Formatted: Font: 13 pt, Not Bold
- Formatted: Font: Not Bold

DRAFT

1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775

Assurance Model

The minimum specifications defined in this document for electronic authentication assume that the trust framework for an identity management system will define a specific assurance model for that system.<sup>19</sup> 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.<sup>20</sup>

<sup>19</sup> Trust Framework Identity Trust Frameworks for identity management system Digital Identity Systems also should set requirements for how the assurance for each credential will be documented in the metadata for the credential to support audit and compliance.

<sup>20</sup> Approved cryptographic techniques shall must be FIPS approved, NIST recommended, or otherwise compliant with Commonwealth IT Information Security Standard (SEC501):

Formatted: Font: 13 pt, Not Bold

Formatted: Normal

Formatted: Font: Not Bold

IMSAC Guidance Document: Identity Management of Non-Person Entities/IRM Guidance Document – Electronic Authentication  
 Draft Date: July 20/January 4, 2017

1776 Authenticator Assurance Level 3 – AAL 3 is intended to provide the highest practical electronic  
 1777 authentication assurance. Authentication at AAL 3 is based on proof of possession of a key  
 1778 through a cryptographic protocol. AAL 3 is similar to AAL 2 except that only “hard”  
 1779 cryptographic authenticators are allowed. The authenticator is required to be a hardware  
 1780 cryptographic module validated at Federal Information Processing Standard (FIPS) 140 Level 2  
 1781 or higher overall with at least FIPS 140 Level 3 physical security. AAL 3 authenticator  
 1782 requirements can be met by using the PIV authentication key of a FIPS 201 compliant Personal  
 1783 Identity Verification (PIV) Card.

1784 **Figure 2. Assurance Model Crosswalk**

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

1787 **8 Alignment Comparison**

1788 The minimum specifications for electronic authentication defined in this document have been  
 1789 developed to align with existing national and international standards for electronic  
 1790 authentication and identity management. Specifically, the minimum specifications reflect basic  
 1791 requirements set forth in national standards at the federal and state level, ensuring compliance  
 1792 while accommodating other identity management standards and protocols. This document  
 1793 assumes that each identity management system will comply with those governing standards  
 1794 and protocols required by Applicable Law.

1795 The following section outlines the alignment and disparities between the minimum  
 1796 specifications in this document and core national standards. A crosswalk documenting the  
 1797 alignment and areas of misalignment has been provided in Appendix 3.

1800 **NIST SP 800-63-3**

1801 The minimum specifications in this document conform with the basic requirements for  
 1802 electronic authentication set forth in NIST SP 800-63-3 (Public Review version). However, as  
 1803 the NIST guidance defines specific requirements for federal agencies, the minimum  
 1804 specifications in this document provide flexibility for identity management systems across  
 1805  
 1806

[http://www.vita.virginia.gov/uploadedFiles/VITA\\_Main\\_Public/Library/PSGs/HostedEnvironmentInformationSecurityStandards/SEC52501.pdf](http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/HostedEnvironmentInformationSecurityStandards/SEC52501.pdf)

Formatted: Font: Bold, Font color: Text 1  
 Formatted: Normal, No bullets or numbering  
 Formatted: Font: 13 pt, Bold, Font color: Text 1

Formatted: Normal

~~IMSAC Guidance Document: Identity Management of Non-Person Entities/IRM Guidance Document – Electronic Authentication~~  
~~Draft Date: July 20 January 4, 2017~~

1807 industries in the private sector and levels of governance. This flexibility enables identity  
1808 management systems to adhere to the specifications but do so in a manner appropriate and  
1809 compliant with their governing trust frameworks.

1810  
1811 ~~State Identity and Access Management Credential (SICAM) Guidance and Roadmap~~

Formatted: Normal

1812  
1813 The minimum specifications in this document conform with the basic requirements for  
1814 electronic authentication set forth by NASCIO in the SICAM Guidance and Roadmap. The  
1815 NASCIO guidance defines specific requirements for state agencies. Similar to the contrast with  
1816 the NIST guidance for federal agencies, the minimum specifications in this document provide  
1817 flexibility for identity management systems across industries in the private sector and levels of  
1818 governance.

Formatted: Normal

1819  
1820 ~~IDESG Identity Ecosystem Framework (IDEF) Functional Model~~

1821  
1822 The minimum specifications in this document conform with the core operations and basic  
1823 requirements for privacy and security set forth by IDESG in the IDEF Functional Model and  
1824 Baseline Functional Requirements. The IDESG/IDEF requirements apply the FIPPs but extend  
1825 them to cover the Guiding Principles of the National Strategy for Trusted Identities in  
1826 Cyberspace (NSTIC). The minimum specifications in this document encourage adherence to the  
1827 IDEF Functional Model, Baseline Functional Requirements and the NSTIC Guiding Principles.

1828 **Appendix 1. IMSAC Charter**

1829  
1830 **COMMONWEALTH OF VIRGINIA**  
1831 **IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL**  
1832 **CHARTER**

1833  
1834 **Advisory Council Responsibilities (§ 2.2-437.A; § 2.2-436.A)**

1835  
1836 The Identity Management Standards Advisory Council (the Advisory Council) advises the  
1837 Secretary of Technology on the adoption of identity management standards and the creation of  
1838 guidance documents pursuant to § 2.2-436.

1839  
1840 The Advisory Council recommends to the Secretary of Technology guidance documents relating  
1841 to (i) nationally recognized technical and data standards regarding the verification and  
1842 authentication of identity in digital and online transactions; (ii) the minimum specifications and  
1843 standards that should be included in an identity-Identity Trust Framework, as defined in § 59.1-  
1844 550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§  
1845 59.1-550 et seq.); and (iii) any other related data standards or specifications concerning reliance  
1846 by third parties on identity credentials, as defined in § 59.1-550.

1847  
1848 **Membership and Governance Structure (§ 2.2-437.B)**

1849

- 1850 The Advisory Council’s membership and governance structure is as follows:  
1851 1. The Advisory Council consists of seven members, to be appointed by the Governor, with  
1852 expertise in electronic identity management and information technology. Members include  
1853 a representative of the Department of Motor Vehicles, a representative of the Virginia  
1854 Information Technologies Agency, and five representatives of the business community with  
1855 appropriate experience and expertise. In addition to the seven appointed members, the  
1856 Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex  
1857 officio member of the Advisory Council.  
1858  
1859 2. The Advisory Council designates one of its members as chairman.  
1860  
1861 3. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure  
1862 of the Governor, and may be reappointed.  
1863  
1864 4. Members serve without compensation but may be reimbursed for all reasonable and  
1865 necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.  
1866  
1867 5. Staff to the Advisory Council is provided by the Office of the Secretary of Technology.  
1868  
1869

IMSAC Guidance Document: Identity Management of Non-Person Entities~~IRM Guidance Document – Electronic Authentication~~  
Draft Date: ~~July 20~~January 4, 2017

1870 The formation, membership and governance structure for the Advisory Council has been  
1871 codified pursuant to § 2.2-437.A, § 2.2-437.B, as cited above in this charter.

1872  
1873 The statutory authority and requirements for public notice and comment periods for guidance  
1874 documents have been established pursuant to § 2.2-437.C, as follows:

1875  
1876 C. Proposed guidance documents and general opportunity for oral or written submittals as to  
1877 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published  
1878 in the Virginia Register of Regulations as a general notice following the processes and  
1879 procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§  
1880 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written  
1881 comments following the posting and publication and shall hold at least one meeting dedicated  
1882 to the receipt of oral comment no less than 15 days after the posting and publication. The  
1883 Advisory Council shall also develop methods for the identification and notification of interested  
1884 parties and specific means of seeking input from interested persons and groups. The Advisory  
1885 Council shall send a copy of such notices, comments, and other background material relative to  
1886 the development of the recommended guidance documents to the Joint Commission on  
1887 Administrative Rules.

1888  
1889  
1890 This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the  
1891 minutes of the meeting and related IMSAC documents, visit:  
1892 <https://vita.virginia.gov/About/default.aspx?id=6442474173>