

COMMONWEALTH OF VIRGINIA



IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

GUIDANCE DOCUMENT Identity Trust Frameworks

Table of Contents

1 Publication Version Control 1
2 Reviews 1
3 Purpose and Scope 2
4 Statutory Authority 2
5 Definitions 3
6 Background 15
7 Minimum Specifications 16
8 Alignment Comparison 20

DRAFT

1 Publication Version Control

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

Publication Version	Date	Revision Description
1.0	05/02/2016	Initial Draft of Document
1.0	05/02/2016	Document revised by IMSAC at public workshop
1.0	06/23/2016	Document revised by VITA staff based on comments from IMSAC during May 2, 2016, public workshop
1.0	09/12/2016	Document revised by VITA staff based on public comment received pursuant to § 2.2-437.C, <i>Code of Virginia</i>
1.0	09/30/2016	Document revised by VITA staff based on comments from IMSAC during September 12, 2016, public meeting

2 Reviews

- The initial version of the document was prepared by staff from the Virginia Information Technologies Agency (VITA) for the Secretary of Technology, under the direction from the Identity Management Standards Advisory Council (IMSAC).
- The document was reviewed by IMSAC during a council workshop, May 2, 2016.
- The document was revised based on public comment received in written and verbal form during the 30-day comment period, pursuant to § 2.2-437.C, *Code of Virginia*. The document was posted on the Virginia Regulatory Town Hall and published in the Virginia Register of Regulations as a general notice following the processes and procedures set forth in subsection B of § [2.2-4031](#) of the Virginia Administrative Process Act (§ [2.2-4000](#) et seq.). IMSAC allowed at least 30 days for the submission of written comments following the posting and publication and held a meeting dedicated to the receipt of oral comment on June 30, more than 15 days after the posting and publication.
- The document will be reviewed in a manner compliant with the Commonwealth of Virginia's Administrative Process Act, § 2.2-4000 et seq.

29 3 Purpose and Scope

30
31 Pursuant to § 2.2-436 and § 2.2-437, *Code of Virginia*, this guidance document was developed
32 by the Identity Management Standards Advisory Council (IMSAC), on behalf of the Secretary of
33 Technology, to establish minimum specifications for Digital Identity Systems so as to warrant
34 liability protection pursuant to the Electronic Identity Management Act ("the Act"), Chapter 50
35 of Title 59.1. The guidance document, as defined in § 2.2-4001, was prepared to provide
36 information or guidance of general applicability to the public for interpreting or implementing
37 the Act. The guidance document was not developed as a Commonwealth of Virginia
38 Information Technology Resource Management (ITRM) Policy, Standard, and Guideline,
39 pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive
40 branch agencies of the Commonwealth of Virginia.
41

42 4 Statutory Authority

43
44 The following section documents the statutory authority established in the *Code of Virginia* for
45 the development of minimum specifications and standards for Identity Trust Frameworks.
46 References to statutes below and throughout this document shall be to the *Code of Virginia*,
47 unless otherwise specified.
48

49 Governing Statutes:

50 51 Secretary of Technology

52 § 2.2-225. Position established; agencies for which responsible; additional powers

53 <http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225/>
54

55 Identity Management Standards Advisory Council

56 § 2.2-437. Identity Management Standards Advisory Council

57 <http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/>
58

59 Commonwealth Identity Management Standards

60 § 2.2-436. Approval of electronic identity standards

61 <http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/>
62

63 Electronic Identity Management Act

64 Chapter 50. Electronic Identity Management Act

65 <http://law.lis.virginia.gov/vacode/title59.1/chapter50/>
66
67
68

69 5 Definitions

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

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

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

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

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

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

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

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

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

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

§ 59.1-550, *Code of Virginia*, may be accessed at <http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550/>. The Commonwealth's ITRM Glossary may be accessed at http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/PSG_Sections/COV_ITRM_Glossary.pdf

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

105 Assurance Model: Policies, processes, and protocols that define how Assurance will be
106 established in an Identity Trust Framework.
107

108 Asymmetric Keys: Two related keys, a public key and a private key that are used to perform
109 complementary operations, such as encryption and decryption or signature generation and
110 signature verification.
111

112 Attack: An attempt by an unauthorized individual to fool a verifier or a relying Participant into
113 believing that the unauthorized individual in question is the Subscriber.
114

115 Attacker: A Participant who acts with malicious intent to compromise an Information System.
116

117 Attribute: A claim of a named quality or characteristic inherent in or ascribed to someone or
118 something.
119

120 Authentication: The process of establishing confidence in the identity of users or Information
121 Systems.
122

123 Authentication Protocol: A defined sequence of messages between a claimant and a verifier
124 that demonstrates that the claimant has possession and control of a valid authenticator to
125 establish his/her identity, and optionally, demonstrates to the claimant that he or she is
126 communicating with the intended verifier.
127

128 Authentication Protocol Run: An exchange of messages between a claimant and a verifier that
129 results in authentication (or authentication failure) between the two Participants.
130

131 Authentication Secret: A generic term for any secret value that could be used by an attacker to
132 impersonate the Subscriber in an authentication protocol. These are further divided into short-
133 term authentication secrets, which are only useful to an attacker for a limited period of time,
134 and long-term authentication secrets, which allow an attacker to impersonate the Subscriber
135 until they are manually reset. The authenticator secret is the canonical example of a long term
136 authentication secret, while the authenticator output, if it is different from the authenticator
137 secret, is usually a short term authentication secret.
138

139 Authenticator: Something that the claimant possesses and controls (typically a cryptographic
140 module or password) that is used to authenticate the claimant's identity. In previous versions of
141 this guideline, this was referred to as a token.
142

143 Authenticator Assurance Level (AAL): A metric describing robustness of the authentication
144 process proving that the claimant is in control of a given Subscriber's authenticator(s).
145

146 Authenticator Output: The output value generated by an authenticator. The ability to generate
147 valid authenticator outputs on demand proves that the claimant possesses and controls the

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

150

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

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

153

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

158

159 Bit: A binary digit: 0 or 1.

160

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

164

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

166

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

169

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

178

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

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

185

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

186 Claimed Identity: A declaration by the applicant of their current Personal Name, date of birth
187 and address. [GPG45]⁴
188

189 Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA): An
190 interactive feature added to web-forms to distinguish use of the form by humans as opposed to
191 automated agents. Typically, it requires entering text corresponding to a distorted image or
192 from a sound stream.
193

194 Cookie: A character string, placed in a web browser's memory, which is available to websites
195 within the same Internet domain as the server that placed them in the web browser.
196

197 Credential: An object or data structure that authoritatively binds an identity (and optionally,
198 additional attributes) to an authenticator possessed and controlled by a Subscriber. While
199 common usage often assumes that the credential is maintained by the Subscriber, this
200 document also uses the term to refer to electronic records maintained by the CSP which
201 establish a binding between the Subscriber's authenticator(s) and identity.
202

203 Credential Service Provider (CSP): A trusted entity that issues or registers Subscriber
204 authenticators and issues electronic credentials to Subscribers. The CSP may encompass
205 Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third
206 Participant, or may issue credentials for its own use.
207

208 Cross Site Request Forgery (CSRF): An attack in which a Subscriber who is currently
209 authenticated to an RP and connected through a secure session, browses to an attacker's
210 website which causes the Subscriber to unknowingly invoke unwanted actions at the RP. For
211 example, if a bank website is vulnerable to a CSRF attack, it may be possible for a Subscriber to
212 unintentionally authorize a large money transfer, merely by viewing a malicious link in a
213 webmail message while a connection to the bank is open in another browser window.
214

215 Cross Site Scripting (XSS): A vulnerability that allows attackers to inject malicious code into an
216 otherwise benign website. These scripts acquire the permissions of scripts generated by the
217 target website and can therefore compromise the confidentiality and integrity of data transfers
218 between the website and client. Websites are vulnerable if they display user supplied data from
219 requests or forms without sanitizing the data so that it is not executable.
220

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

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

225
226 Cryptographic Authenticator: An authenticator where the secret is a cryptographic key.
227
228 Data Integrity: The property that data has not been altered by an unauthorized entity.
229
230 Derived Credential: A credential issued based on proof of possession and control of an
231 authenticator associated with a previously issued credential, so as not to duplicate the Identity
232 Proofing process.
233
234 Digital Identity System: An Information System that supports Electronic Authentication and the
235 management of a person's Identity in a digital environment. [Referenced in § 59.1-550, COV]
236
237 Digital Signature: An asymmetric key operation where the private key is used to digitally sign
238 data and the public key is used to verify the signature. Digital signatures provide authenticity
239 protection, integrity protection, and non-repudiation.
240
241 Eavesdropping Attack: An attack in which an attacker listens passively to the authentication
242 protocol to capture information which can be used in a subsequent active attack to
243 masquerade as the claimant.
244
245 Electronic Authentication: The process of establishing confidence in user identities
246 electronically presented to an Information System.
247
248 Entropy: A measure of the amount of uncertainty that an attacker faces to determine the value
249 of a secret. Entropy is usually stated in bits.
250
251 Extensible Mark-up Language (XML): Extensible Markup Language, abbreviated XML, describes
252 a class of data objects called XML documents and partially describes the behavior of computer
253 programs which process them.
254
255 Federal Bridge Certification Authority (FBCA): The FBCA is the entity operated by the Federal
256 Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI
257 Policy Authority to create, sign, and issue public key certificates to Principal CAs.
258
259 Federal Information Security Management Act (FISMA): Title III of the E-Government Act
260 requiring each federal agency to develop, document, and implement an agency-wide program
261 to provide information security for the information and Information Systems that support the
262 operations and assets of the agency, including those provided or managed by another agency,
263 contractor, or other source.
264
265 Federal Information Processing Standard (FIPS): Under the Information Technology
266 Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards
267 and guidelines that are developed by the National Institute of Standards and Technology (NIST)
268 for Federal computer systems. These standards and guidelines are issued by NIST as Federal

269 Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when
270 there are compelling Federal government requirements such as for security and interoperability
271 and there are no acceptable industry standards or solutions.⁵

272

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

276

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

279

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

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

286

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

291

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

293

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

296

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

299

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

303

304 Identity Trust Framework: A Digital Identity System with established identity, security, privacy,
305 technology, and enforcement rules and policies adhered to by certified identity providers that
306 are members of the Identity Trust Framework. Members of an Identity Trust Framework
307 include Identity Trust Framework operators and identity providers. Relying Participants may be,
308 but are not required to be, a member of an Identity Trust Framework in order to accept an

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

309 identity credential issued by a certified identity provider to verify an identity credential holder's
310 identity. [§ 59.1-550, COV]

311

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

315

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

324

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

330

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

334

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

338

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

342

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

348

349 Nonce: A value used in security protocols that is never repeated with the same key. For
350 example, nonces used as challenges in challenge-response authentication protocols must not
351 be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay

352 attack. Using a nonce as a challenge is a different requirement than a random challenge,
353 because a nonce is not necessarily unpredictable.
354

355 Off-line Attack: An attack where the attacker obtains some data (typically by eavesdropping on
356 an authentication protocol run or by penetrating a system and stealing security files) that
357 he/she is able to analyze in a system of his/her own choosing.
358

359 Online Attack: An attack against an authentication protocol where the attacker either assumes
360 the role of a claimant with a genuine verifier or actively alters the authentication channel.
361

362 Online Guessing Attack: An attack in which an attacker performs repeated logon trials by
363 guessing possible values of the authenticator output.
364

365 Operational Authority: Entity responsible for operations, maintenance, management, and
366 related functions of an Identity Trust Framework.
367

368 Participant Requirements: A set of rules and policies in an Identity Trust Framework addressing
369 identity, security, privacy, technology, and enforcement, which are assigned to each member
370 type in a Digital Identity System. Member types include Registration Authorities (RAs), Identity
371 Providers (IdPs), Credential Service Providers (CSPs), Verifiers, and Relying Parties (RPs).
372 [§ 59.1-550, COV]
373

374 Passive Attack: An attack against an authentication protocol where the attacker intercepts data
375 traveling along the network between the claimant and verifier, but does not alter the data (i.e.,
376 eavesdropping).
377

378 Password: A secret that a claimant memorizes and uses to authenticate his or her identity.
379 Passwords are typically character strings.
380

381 Personal Identification Number (PIN): A password consisting only of decimal digits.
382

383 Personal Identity Verification (PIV) Card: Defined by [FIPS 201] as a physical artifact (e.g.,
384 identity card, smart card) issued to federal employees and contractors that contains stored
385 credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that
386 the claimed identity of the cardholder can be verified against the stored credentials by another
387 person (human readable and verifiable) or an automated process (computer readable and
388 verifiable).
389

390 Personally Identifiable Information (PII): As defined by OMB Circular A-130, Personally
391 Identifiable Information means information that can be used to distinguish or trace an
392 individual's identity, either alone or when combined with other information that is linked or
393 linkable to a specific individual.
394

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

399 Phishing: An attack in which the Subscriber is lured (usually through an email) to interact with a
400 counterfeit verifier/RP and tricked into revealing information that can be used to masquerade
401 as that Subscriber to the real verifier/RP.
402

403 Physical In-Person: Method of Identity Proofing in which Applicants are required to physically
404 present themselves and identity evidence to a representative of the Registration Authority or
405 Identity Trust Framework. [NIST SP 800-63-2]
406

407 Possession and control of an authenticator: The ability to activate and use the authenticator in
408 an authentication protocol.
409

410 Practice Statement: A formal statement of the practices followed by the Participants to an
411 authentication process (i.e., RA, CSP, or verifier). It usually describes the policies and practices
412 of the Participants and can become legally binding.
413

414 Private Credentials: Credentials that cannot be disclosed by the CSP because the contents can
415 be used to compromise the authenticator.
416

417 Private Key: The secret part of an asymmetric key pair that is used to digitally sign or decrypt
418 data.
419

420 Protected Session: A session wherein messages between two participants are encrypted and
421 integrity is protected using a set of shared secrets called session keys. A participant is said to be
422 authenticated if, during the session, he, she or it proves possession of a long term authenticator
423 in addition to the session keys, and if the other Participant can verify the identity associated
424 with that authenticator. If both participants are authenticated, the protected session is said to
425 be mutually authenticated.
426

427 Pseudonymous Identifier: A meaningless, but unique number that does not allow the RP to
428 infer the Subscriber but which does permit the RP to associate multiple interactions with the
429 Subscriber's claimed identity.
430

431 Public Credentials: Credentials that describe the binding in a way that does not compromise the
432 authenticator.
433

434 Public Key: The public part of an asymmetric key pair that is used to verify signatures or encrypt
435 data.
436

437 Public Key Certificate: A digital document issued and digitally signed by the private key of a
438 Certificate authority that binds the name of a Subscriber to a public key. The certificate

439 indicates that the Subscriber identified in the certificate has sole control and access to the
440 private key. See also [RFC 5280].
441

442 Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software and
443 workstations used for the purpose of administering certificates and public-private key pairs,
444 including the ability to issue, maintain, and revoke public key certificates.
445

446 Registration: The process through which an applicant applies to become a Subscriber of a CSP
447 and an RA validates the identity of the applicant on behalf of the CSP.
448

449 Registration Authority (RA): A trusted entity that establishes and vouches for the identity or
450 attributes of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be
451 independent of a CSP, but it has a relationship to the CSP(s).
452

453 Relying Party (RP): An entity that relies upon the Subscriber's authenticator(s) and credentials
454 or a verifier's Assertion of a claimant's identity, typically to process a transaction or grant access
455 to information or a system.
456

457 Remote: (As in remote authentication or remote transaction) An information exchange
458 between network-connected devices where the information cannot be reliably protected end-
459 to-end by a single organization's security controls. Note: Any information exchange across the
460 Internet is considered remote.
461

462 Replay Attack: An attack in which the attacker is able to replay previously captured messages
463 (between a legitimate claimant and a verifier) to masquerade as that claimant to the verifier or
464 vice versa.
465

466 Risk Assessment: The process of identifying the risks to system security and determining the
467 probability of occurrence, the resulting impact, and additional safeguards that would mitigate
468 this impact. Part of Risk Management and synonymous with Risk Analysis.
469

470 Salt: A non-secret value that is used in a cryptographic process, usually to ensure that the
471 results of computations for one instance cannot be reused by an attacker.
472

473 Secondary Authenticator: A temporary secret, issued by the verifier to a successfully
474 authenticated Subscriber as part of an Assertion protocol. This secret is subsequently used, by
475 the Subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer
476 Assertions, Assertion references, and Kerberos session keys.
477

478 Secure Sockets Layer (SSL): An authentication and security protocol widely implemented in
479 browsers and web servers. SSL has been superseded by the newer Transport Layer Security
480 (TLS) protocol; TLS 1.0 is effectively SSL version 3.1.
481

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

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

489

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

495

496 Shared Secret: A secret used in authentication that is known to the claimant and the verifier.
497

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

500

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

505

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

508

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

510

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

514

515 Token: See Authenticator.

516

517 Token Authenticator: See Authenticator Output.

518

519 Token Secret: See Authenticator Secret.

520

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

526
527 Trust Anchor: A public or symmetric key that is trusted because it is directly built into hardware
528 or software, or securely provisioned via out-of-band means, rather than because it is vouched
529 for by another trusted entity (e.g. in a public key certificate).
530 Unverified Name: A Subscriber name that is not verified as meaningful by Identity Proofing.
531
532 Valid: In reference to an ID, the quality of not being expired or revoked.
533
534 Verified Name: A Subscriber name that has been verified by Identity Proofing.
535
536 Verifier: An entity that verifies the claimant's identity by verifying the claimant's possession and
537 control of one or two authenticators using an authentication protocol. To do this, the verifier
538 may also need to validate credentials that link the authenticator(s) and identity and check their
539 status.
540
541 Verifier Impersonation Attack: A scenario where the attacker impersonates the verifier in an
542 authentication protocol, usually to capture information that can be used to masquerade as a
543 claimant to the real verifier.
544
545 Virtual In-Person Proofing: A remote identity person proofing process that employs technical
546 and procedural measures that provide sufficient confidence that the remote session can be
547 considered equivalent to a physical, in-person identity proofing encounter. [NIST SP 800-63A]
548
549 Weakly Bound Credentials: Credentials that describe the binding between a user and
550 authenticator in a manner than can be modified without invalidating the credential.
551
552 Zeroize: Overwrite a memory location with data consisting entirely of bits with the value zero
553 so that the data is destroyed and not recoverable. This is often contrasted with deletion
554 methods that merely destroy reference to data within a file system rather than the data itself.
555
556 Zero-knowledge Password Protocol: A password based authentication protocol that allows a
557 claimant to authenticate to a Verifier without revealing the password to the verifier. Examples
558 of such protocols are EKE, SPEKE and SRP.

559 6 Background

560

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

567

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

573

574 The Advisory Council recommends to the Secretary of Technology guidance documents relating
575 to (i) nationally recognized technical and data standards regarding the verification and
576 authentication of Identity in digital and online transactions; (ii) the minimum specifications and
577 standards that should be included in an Identity Trust Framework, as defined in §59.1-550, so
578 as to warrant liability protection pursuant to the Electronic Identity Management Act (§59.1-
579 550 et seq.); and (iii) any other related data standards or specifications concerning reliance by
580 third parties on Identity credentials, as defined in §59.1-550.

581

582 Purpose Statement

583

584 This guidance document, as defined in § 2.2-4001, was developed by the Identity Management
585 Standards Advisory Council (IMSAC), on behalf of the Secretary of Technology, to provide
586 information or guidance of general applicability to the public for interpreting or implementing
587 the Electronic Identity Management Act. Specifically, the document establishes minimum
588 specifications for Identity Trust Frameworks supporting Digital Identity Systems.

589

590 The document defines minimum requirements, components, and related provisions for Identity
591 Trust Frameworks. The document assumes a specific Identity Trust Framework will address the
592 business, legal, and technical requirements for each distinct Digital Identity System; these
593 requirements will be designed based on the specific Assurance Model supported by the system;
594 and the Identity Trust Framework will be compliant with Applicable Law.

595

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

599

600 7 Minimum Specifications

601

602 The Commonwealth of Virginia’s Electronic Identity Management Act defines “Identity Trust
603 Framework” as “a Digital Identity System with established Identity, security, privacy,
604 technology, and enforcement rules and policies adhered to by certified Identity Providers that
605 are members of the Identity Trust Framework” (§ 59.1-550). Identity Trust Frameworks consist
606 of multiparty agreements among members, which enforce requirements and ensure trust in the
607 acceptance of Identity credentials.

608

609 This document establishes minimum specifications for Identity Trust Frameworks. Identity
610 Trust Frameworks should be designed to document the business, legal, and technical
611 components for enterprise architecture, business processes, governance models, operational
612 policies and practices, and member obligations within the system. Identity Trust Frameworks
613 also should contain the requirements for meeting the Assurance Model supported by the
614 system.⁶ Subsequent guidance documents in the IMSAC series have addressed other
615 components of Digital Identity System, pursuant to §2.2-436 and §2.2-437.

616

617 Trust Framework Components

618

619 The following section outlines the minimum specifications for the business, legal and technical
620 components of a standard Identity Trust Framework. These components have been identified
621 through a rigorous assessment of existing Identity Trust Frameworks in the Identity ecosystem
622 and other domains, as outlined in Section 7 of this report. The components also align with the
623 Identity Ecosystem Framework (IDEF), adopted by the Identity Ecosystem Steering Group in
624 October 2015.⁷

625

626 Business Components

627

- 628 • Limitations on Use of Data: Collection, maintenance, and use of a person’s Identity
629 information solely for the purpose for which it was collected.
- 630 • Governance Authority & Change Processes: Governance model for the Identity Trust
631 Framework built on a transparent, clearly defined structure and change-management
632 process.

⁶ The term “Assurance Model” has been used in this document to describe a) the degree of confidence in the vetting process used to establish the Identity of an individual to whom the credential was issued, and b) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.. The term aligns with the Assurance Model established in the Public Review version of NIST SP 800-63-3 but provides for a more general framework to accommodate other Identity management standards and protocols.

⁷ Identity Ecosystem Framework (IDEF) Baseline Functional Requirements (v.1.0), Identity Ecosystem Steering Group (IDESG), may be accessed at: https://workspace.idesg.org/kws/public/download/83/IDEF-Baseline-Requirements-v1.0-FINAL-10152015.pdf&wg_abbrev=idesg_document.

- 633 • Operating Policies & Procedures: Policies and procedures for the operations, maintenance,
634 and business continuity of the Identity Trust Framework's Operational Authority, and across
635 the Digital Identity System.
- 636 • Security, Privacy & Confidentiality (Business): Compliant business processes and
637 documentation for notifying a person of the security, privacy, and confidentiality provisions
638 in the Identity Trust Framework and for gaining consent from the person for using Identity
639 information.
- 640 • Suspension & Termination (Voluntary & Involuntary): Provisions for suspending or
641 terminating a member due to failure to meet the obligations in the agreement, or the
642 member's self-suspension or termination of participation in the Identity Trust Framework.
- 643 • Data Elements & Data Classification: Attribute-level documentation, classification, and
644 labeling of the person Identity information used within the Identity Trust Framework to
645 support compliant handling of the data through the entire data lifecycle.
- 646 • Expectations of Performance: Provisions in the Identity Trust Framework that set the
647 performance and service criteria for all members – IdPs, CSPs, and RPs – including
648 requirements for breach response and resolution, system(s) interruption or failure, and
649 other risk situations.
- 650 • Use Cases (Exchange & Member Types): Documented examples for roles and
651 responsibilities of members of the Identity Trust Framework and data flows across the
652 Digital Identity System.

653

654 Legal Components

655

- 656 • Definition/Identification of Applicable Law: Provisions requiring members of the Identity
657 Trust Framework to comply with all governing laws, statutes, rules, and regulations of the
658 jurisdiction in which each member operates.
- 659 • Legal Agreements for Exchange Structure: Statement of requirements for the architecture,
660 performance, and service specifications, and member obligations for the operation and
661 maintenance of the exchange of person Identity information within the Identity Trust
662 Framework.
- 663 • Security, Privacy & Consent Provisions (Legal): Terms and conditions establishing member
664 obligations for the collection, labeling, operational use, and maintenance of person Identity
665 information and for gaining consent from the person for using Identity information.
- 666 • Assignment of Liability & Risk for Members: Articles that define how liability and risk within
667 the Identity Trust Framework will be distributed among members, with indemnification
668 provisions for violation of the agreement.
- 669 • Representations & Warranties: Statements of factual principles in the Identity Trust
670 Framework upon which members may rely, and assurances of the implied indemnification
671 obligation in the event the principles are violated or proven false.
- 672 • Grant of Authority: Provisions requiring members of the Identity Trust Framework to assign
673 to the Governance Authority decision-making authority over the Identity Trust Framework.

- 674 • Dispute Resolution: Statement of requirements and processes for mediation and the
675 resolution of disputes among members in the Identity Trust Framework in a manner that
676 avoids adjudicative procedures.
- 677 • Authorizations for Data Requests by Members: Articles defining role-based rules,
678 requirements, and processes for members of the Identity Trust Framework to access person
679 Identity information.
- 680 • Open Disclosure & Anti-Circumvention: Provisions requiring transparency in the rules,
681 policies, and practices for operations and governance of the Identity Trust Framework, and
682 prohibiting the circumvention of technical protections within the Digital Identity System for
683 the handling of person Identity information.
- 684 • Confidential Person Information: Statements documenting the business, legal and technical
685 requirements for the classification, labeling and handling of confidential person Identity
686 information.
- 687 • Audit, Accountability & Compliance: Terms of conditions documenting and requiring
688 members of the Identity Trust Framework to comply with audit procedures, and the
689 consequences of members failing to comply with the audit findings and corrective action
690 plan to address deficiencies.
- 691

692 Technical Components

693

- 694 • Performance & Service Specifications: Architecture and infrastructure specifications,
695 protocols, and requirements for all members – IdPs, CSPs, and RPs – covering full end-to-
696 end integration for the Digital Identity System supported by the Identity Trust Framework,
697 including technical, solutions, and information architecture.
- 698 • Security, Privacy & Confidentiality: Architecture and infrastructure specifications, protocols,
699 and requirements within the Digital Identity System supported by the Identity Trust
700 Framework designed for the collection, labeling, operational use, and maintenance of
701 person Identity information and for gaining consent from the person for using Identity
702 information.
- 703 • Breach Notification: Processes, protocols, and requirements compliant with Applicable Law
704 for notifying the appropriate authorities in the event of a breach of person Identity
705 information, and related risk situations, within the Identity Trust Framework.
- 706 • System Access: Standards-based, open architecture processes, protocols, and requirements
707 for member authentication and access to the Digital Identity System supported by the
708 Identity Trust Framework.
- 709 • Provisions for Future Use of Data: Terms and conditions defining limitations on, and
710 permitted purposes for, the use of person Identity information after the information has
711 been used for the Registration event and the issuance of a Credential by a Credential
712 Service Provider.
- 713 • Duty of Response by Members: Terms and conditions requiring Identity Trust Framework
714 member Information Systems to respond to and process messaging requests – inbound and
715 outbound – within the Digital Identity System, normally establishing the time in which the
716 member system must respond and process the request.

- 717 • Onboarding, Testing & Certification Requirements: Documented processes, protocols,
718 specifications, and requirements for onboarding, testing, and certifying prospective
719 member Information Systems in the Identity Trust Framework.
- 720 • Handling of Test Data v. Production Data: Terms and conditions compliant with Applicable
721 Law preventing the use of production data in a test environment.
- 722 • Compliance with Governing Standards: Terms and conditions identifying and stating
723 requirements for member compliance with governing external standards for the Identity
724 Trust Framework, including standards for information processing, Electronic Authentication,
725 and Authorization.
726
727

DRAFT

728 8 Alignment Comparison

729

730 The minimum specifications for Identity Trust Frameworks established in this document have
731 been developed based on a detailed comparison analysis of Identity Trust Frameworks and
732 related governance models currently operational in the Identity management ecosystem.
733 Specifically, the minimum specifications build upon core components of existing Identity Trust
734 Frameworks while adapting or extending them to meet the requirements of IMSAC, pursuant to
735 §2.2-436-§2.2-437. The analysis covered Identity Trust Frameworks on a global scale, including
736 a detailed review of the Open Identity Exchange (OIX) Trust Framework Model (OIX/OITF) and
737 the European Union (EU) standards.

738

739 The following Identity Trust Frameworks were evaluated by IMSAC. Results from the alignment
740 comparison analysis have been compiled into matrix form in **Appendix 2**.

741

- 742 • State Identity, Credential and Access Management (SICAM) Guidance and Roadmap –
743 Strategic framework published by the National Association of State Chief Information
744 Officers (NASCIO) to promote alignment with FICAM within state government.⁸
- 745 • AAMVA DL/ID Security Framework – Set of requirements, recommendations and standards
746 maintained by the American Association of Motor Vehicle Administrators (AAMVA) for use
747 by Motor Vehicle Administrations to ensure driver’s license and identification security.
- 748 • eHealth Exchange Data Use & Reciprocal Support Agreement (DURSA) – Trust framework
749 established to support the exchange health information and messaging within eHealth
750 Exchange, the Nationwide Health Information Network.
- 751 • InCommon Trust Framework – Trust framework designed to facilitate authentication and
752 Identity management for students, faculty, staff and other service providers for institutions
753 of higher education.
- 754 • Kantara Initiative Trust Framework – Trust framework developed on a for-profit,
755 subscription basis to enable secure, Identity-based, online interactions in a secure
756 environment.
- 757 • Open Identity Exchange (OIX)/OITF Model – Set of guidelines and recommended
758 mechanisms (Assurance Model and Level of Protection) for developing and implementing
759 an Identity Trust Framework for secure, confidence-based exchange of information (Global).

760

761

⁸ The Federal Identity, Credential, and Access Management (FICAM) program was created 2008 to address challenges, implementation issues, and design requirements for digital Identity, credential, and access management for federal agencies. For more information, visit:

https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt000000XNYG

762 Appendix 1. IMSAC Charter

763

764

765 **COMMONWEALTH OF VIRGINIA**
766 **IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL**
767 **CHARTER**

768

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

770

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

774

775 The Advisory Council recommends to the Secretary of Technology guidance documents relating
776 to (i) nationally recognized technical and data standards regarding the verification and
777 authentication of identity in digital and online transactions; (ii) the minimum specifications and
778 standards that should be included in an Identity Trust Framework, as defined in § 59.1-550, so
779 as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-
780 550 et seq.); and (iii) any other related data standards or specifications concerning reliance by
781 third parties on identity credentials, as defined in § 59.1-550.

782

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

784

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

786

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

794

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

796

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

799

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

802

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

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

806

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

809

810 C. Proposed guidance documents and general opportunity for oral or written submittals as to
811 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published
812 in the Virginia Register of Regulations as a general notice following the processes and
813 procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§
814 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written
815 comments following the posting and publication and shall hold at least one meeting dedicated
816 to the receipt of oral comment no less than 15 days after the posting and publication. The
817 Advisory Council shall also develop methods for the identification and notification of interested
818 parties and specific means of seeking input from interested persons and groups. The Advisory
819 Council shall send a copy of such notices, comments, and other background material relative to
820 the development of the recommended guidance documents to the Joint Commission on
821 Administrative Rules.

822

823

824 This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the
825 minutes of the meeting and related IMSAC documents, visit:

826 <https://vita.virginia.gov/About/default.aspx?id=6442474173>

Appendix 2. Trust Framework Alignment Comparison Matrix

	Trust Framework (TF) Components for IMSAC			
	Business	Legal	Technical	Other
<p>Trust Framework (TF) Comparison Matrix</p>	<ul style="list-style-type: none"> • Limitations on Use of Data (“Permitted Purpose”) • Governance Authority & Change Processes • Operating Policies & Procedures • Security, Privacy & Confidentiality-Business: Consent/Auth.) • Suspension & Termination (Voluntary & Involuntary) • Data Elements & Data Classification (Attribute Level/Person Identity Information) • Expectations of Performance • Use Cases (Exchange & Member Types) 	<ul style="list-style-type: none"> • Definition/Identification of “Applicable Law” • Legal Agreements for Exchange Structure • Security, Privacy & Consent Provisions • Assignment of Liability & Risk for Members • Representations & Warranties • Grant of Authority • Dispute Resolution • Authorizations for Data Requests by Member • Open Disclosure & Anti-Circumvention • Confidential Person Information • Audit, Accountability & Compliance 	<ul style="list-style-type: none"> • Performance & Service Specifications • Security, Privacy & Confidentiality (Technical: Infrastructure/Architecture) • Breach Notification • System Access (ID/Authentication) • Provisions for Future Use of Data • Duty of Response by Members • Onboarding, Testing & Certification Requirements • Handling of Test Data v. Production Data • Compliance Governing Standards 	<ul style="list-style-type: none"> • Openness & Transparency • TF Lifecycle Management (“Living Agreement”) • Support & Capacity Building (IGs) • Scalability to Support Array of Members (Horizontal/Vertical) • Glossary of TF Terms/Definitions • Component-based Approach for TF Elements

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	Legal	Technical	Other
<p>State Identity, Credential and Access Management (SICAM) Guidance and Roadmap</p>	<ul style="list-style-type: none"> + Limitations on Use of Data (§6.6) + Governance Authority & change processes (§6.6) + Operating policies & procedures (§6.6) + Security, privacy & confidentiality (§6.6) + Suspension & termination (§6.6) + Data elements & data classification (attribute level/PII) (§5.5, §6.5, §6.6) + Expectations of performance (§6.6) 	<ul style="list-style-type: none"> + Compliance w/ applicable law (§6.6) + Legal agreements for exchange structure (§6.6) + Security, privacy & consent (§6.6) + Liability (§6.6) + Representations & warranties (§6.6) + Grant of authority (§6.6) + Dispute resolution (§6.6) + Authorizations for data exchange (§6.6) + Non-exclusivity (§6.6) + Confidential Person Information (§6.6, §6.3) + Audit (§6.6) + Accountability & compliance (§6.9) 	<ul style="list-style-type: none"> + Performance & service specifications (§5, §6.4) + Security, privacy & confidentiality (§5, §6.4) + Breach notification (§5, §6.4; §6.6) + System access (§6.6) + Provisions for future use of data/services (§6) + Expectations of Members (§6.6) + Duty of response by Members (§6.6) + Onboarding, testing & certification (§6.6) + Compliance with governing standards (§5, §6.6) 	<ul style="list-style-type: none"> + Openness & transparency (§6.6) + TF lifecycle management (§6.6) + Scalability to support array of Members (§6.8) + Glossary of TF terms/definitions (§1.4) + Component-based approach for different Member types (§6.6)

NASCIO, State Identity, Credential and Access Management (SICAM) Guidance and Roadmap, Sept. 2012.

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	Legal	Technical	Other
AAMVA DL/ID Security Framework	<ul style="list-style-type: none"> + Data element-level verification and validation (§1.3 #9, §1.4 #10, §1.4 #13, §3.3.4, §7.4, Appdx.) + Data (Name) collection, use and maintenance (§3.3.4, § 7.1, Appdx.) + AAMVA DL/ID Personal ID Card Design Specification (§1.4 #12, §3.3.4, 7.3, Appdx.) + Procedures for initial customer ID and validation (§3.3.3, §6.0) + Record & document use, permitted purpose (§3.3.5, §4.6, §7.1, §8.0) + Benefits/ business drivers (§2.0, §3.1) + Business-driven agreement among MVAs (§3.1, §3.3, §4.5) + Business requirements for P&Ps, document issuing systems, and internal controls, Driver License Agreement (DLA) (§3.3.1, §4.2, §4.5, Appdx.) 	<ul style="list-style-type: none"> + Assumes MVA compliance with applicable law, document use, data sharing (§1.5 All Recs., §3.1, §3.2, §3.3.5, §4.5, §8.3, Appdx.) + Enforcement thru business requirements (§2.0, §3.1, §4.5) + Audit plan (§1.1 #2, §1.2 #5, §3.3.2, §5.1, Appdx.) + Compliance and oversight, internal controls (§3.3.2, §4.4, §5.2) + Risk assessment & management (§1.1 #3, §3.3.5, § 4.2, §4.4, §8.0) + Privacy (§1.1 #4, §4.2, Appdx., §3.3.4, §3.3.5, §4.5, §4.6, §7.1, §7.4, §8.3) + Common set of verifiable resources (§1.3 #8, §3.3.3, §6.2, Appdx.) + Machine-Readable Technology (MRT) (§3.3.5, §8.2, Appdx.) + Restrictions, minimum penalties and sanctions (§3.3.5, §8.1, Appdx.) 	<ul style="list-style-type: none"> + Electronic verification (w/issuing entity) of DL/ID data elements (§1.3 #9, §3.3.3, §6.3) + Standards for MVA system integrity, interoperability & reciprocity (§2.0, §3.1, §3.3.2, §4.2, §4.5) + Compliance with governing standards (§3.3.2, §4.5, §5.2) + System integrity, security & privacy (§4.6) 	<ul style="list-style-type: none"> + Compliance and implementation support thru FDR employee training (§1.1 #1, §3.3.1, §4.1) + Common definition of “residency” (§1.3 #6, §3.3.3) tied to DL/ID verification (§1.3 #7, §3.3.3, §6.1) + “End of stay” on immigration doc. as expiration date for DL/ID - data element derivation (§1.4 #11, §3.3.4, §7.2, Appdx.) + Horizontal scalability thru reciprocity (§3.1) + Openness enforced thru privacy provisions (§4.6, §7.1) + Limits on disclosure enforced thru privacy provisions (§4.6, 7.1) + Glossary of abbreviations/ acronyms (§9.0) + LE Use Case (§1.5 Rec. #8, data sharing §3.3.5, §8.3, Appdx.)

AAMVA. DL/ID Security Framework, Feb. 2004.

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	Legal	Technical	Other
eHealth Exchange Data Use & Reciprocal Support Agreement (DURSA)	<ul style="list-style-type: none"> + Limitations on use of data (§1.jj; §3; §5.01-5.03) + Governance Authority (§4) & change processes (§10.03; §11.03) + Operating policies & procedures (§11; Appdx.; change process in §11.03) + Security, privacy & confidentiality (§7; §8; §14) + Suspension & termination (§19) + Data elements & data classification (attribute level/PII) (§1.v; §1.w; §1.kk) + Expectations of performance (§12) 	<ul style="list-style-type: none"> + Definition/compliance w/ applicable law (§1.a; §15.11; §23.01; Appdx.) + Legal agreements for exchange structure (recitals; §1.ee; §3.01; §23.07) + Security, privacy & consent (§14) + Liability (§18) + Representations & warranties (§15; disclaimers in §17) + Grant of authority (§4.03) + Dispute resolution (§21; Appdx.) + Authorizations for data exchange (§12; §13) + Open disclosure & anti-circumvention (§15; §23.04; §23.07) + Confidential Person information (§16) + Audit (§9) + Accountability & compliance (§10.01; 11.01; §15.03; §15.06) 	<ul style="list-style-type: none"> + Performance & service specifications (§10; Appdx.; change process in §10.03) + Security, privacy & confidentiality (§7; §8; §14) + Breach notification (§14.03) + System access (§6) + Provisions for future use of data (§5.02) + Expectations of Members (§12) + Duty of response by Members (§13) + Onboarding, testing & certification (§10.01) + Handling of test data v. production data (§15.07) 	<ul style="list-style-type: none"> + Openness & transparency (overview; recitals) + TF lifecycle management (“living agreement”) (overview; §4; §10.03; §11.03) + Scalability to support array of Members (horizontal/vertical) (Member types defined in §1; expectations in §12.02; duties in §13) + Glossary of TF terms/definitions (§1) + Component-based approach for different Member types (types defined in §1; expectations in §12.02; duties in §13; warranties in §15)

eHealth Exchange, Data Use and Reciprocal Support Agreement, Sept. 2014.

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	Legal	Technical	Other
InCommon Trust Framework	<ul style="list-style-type: none"> + Limitations on use of data (ICPOP; IAS; limits on use of ID information in PA §9) + Governance Authority & change processes (ICPOP; PA §17) + Operating policies & procedures (ICPOP) + Security, privacy & confidentiality (PA §6, §9; ICPOP) + Suspension & termination (PA §5.b, §5.c) + Data elements & data classification (attribute level/PII) (IAS; PA §6.b) + Expectations of performance (PA §6, §7) + Use cases and examples (InCommon Website; ICBP; Members) 	<ul style="list-style-type: none"> + Definition/compliance w/ applicable law (PA §15) + Legal agreements for exchange structure (ICPP; PA §6, §7.b) + Security, privacy & consent (PA §6, §9) + Liability (PA §11, includes disclaimer & limitations) + Representations & warranties (addressed in PA §7.b) + Grant of authority to executive (PA §18) + Dispute resolution process (PA §10; ICBL §5) + Authorizations for data exchange (PA §18) + Open disclosure & anti-circumvention (PA §14, §16) + Confidential Person information (PA §8, §9) + Audit (ICPOP) + Accountability & compliance (PA §15) 	<ul style="list-style-type: none"> + Performance & service specifications (PA §6, §7) + Security, privacy & confidentiality (ICPOP) + Breach notification (PA and addenda; ICPOP) + System access (ICPOP) + Provisions for future use of data (ICPOP) + Expectations of Members (PA §6, §7) + Duty of response by Members (PA §6, §7) + Onboarding, testing & certification (ICPOP) + Handling of test data v. production data (ICPOP) 	<ul style="list-style-type: none"> + Openness & transparency (ICBP) + TF lifecycle management (“living agreement”) (ICBL; PA §17) + Implementation support (ICPOP) + Scalability to support array of Members (horizontal/vertical) (Member types defined in Join §1, Members) + Glossary of TF terms/definitions (InCommon Website) + Component-based approach for different Member types (Members)

ICPOP=InCommon Member Operational Practices
 PA=InCommon Participation Agreement
 IAS=InCommon Attribute Summary

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	Legal	Technical	Other
Kantara Initiative Trust Framework	<ul style="list-style-type: none"> + Limitations on use of data (KTR MTAU) + Governance Authority (BL §4; OP §2) & change/ amendment processes (BL §12; OP §9; MA §3) + Operating policies & procedures (OP) + Security, privacy & confidentiality (AP; MA) + Suspension & termination (MA §2; BL §8.11; KTR MTAU) + Data elements & data classification (KTR; KIC) + Expectations of performance (AP; KTR MTAU; KIC) + Use cases (Working groups for business cases-trusted federations) 	<ul style="list-style-type: none"> + Definition/identification of applicable law (KTR MTAU; see also “Governing law and jurisdiction” provision in KTR MTAU) + Legal agreement for exchange structure (MA) + Security, privacy & consent provisions + Liability (KTR MTAU) + Warranty (KTR MTAU) + Grant of authority (MA) + Authorizations for data requests by Member + Open disclosure & anti-circumvention (Other agreements in KTR MTAU) + Confidential Person information (Options set in IPRP; IPRP Art. 3) + Accountability & compliance (w/ antitrust laws in BL §17; MA) 	<ul style="list-style-type: none"> + Performance & service specifications (AP; KTR/KTV; KTR MTAU; KIC; Member protection & treatment in IPRP) + Security, privacy & confidentiality (AP; MA) + Technical certification & testing (AP; KIC) + Standards for technical & operational interoperability (KTR; MA goal #3; #7; KIC) 	<ul style="list-style-type: none"> + Open & transparent governance model (MA goals #3, #4; op; BL §3) + TF lifecycle management (MA goals #4, #6) + Support & capacity building (IGs) + Scalability to support array of Members (horizontal/vertical) (member types BL §8) + TF definitions (BL §1; OP §1; IPRP Art. 2)

BL=Bylaws; IPRP=Intellectual Property Rights Policies; MA=Member Agreement; OP=Operating Procedures
 KTR=Kantara Trust Registry; KTV=KTR Trust Validation; KTR MTAU=Metadata Terms of Access & Use; KIC= Kantara Interoperability Cert.-SAML, OATH, etc.
 AP= Assurance Programs; Identity Assurance Accreditation & Approval and Interoperability Certification Programs

Trust Framework Comparison Analysis	Alignment (+) with Core Components for IMSAC			
	Business	Legal	Technical	Other
Open Identity Exchange (OIX)/OITF Model	<ul style="list-style-type: none"> + Limitations on use of data (OITF §III.B, §III.C, §V) + Governance Authority & change processes (OIX; OITF §III.C) + Operating policies & procedures (OIX; OITF §II, §III.B, §III.C) + Security, privacy & confidentiality (OIX; OITF §III.A, §V) + Suspension & termination (OITF §III.C) + Data elements & data classification (attribute level/PII) (OIX; OITF §III.A, §III.B) + Expectations of performance (OIX; OITF §II, §III.C) + Use cases for agreement, transaction & Member types (OITF §I, §III; OIX) 	<ul style="list-style-type: none"> + Compliance w/ applicable law (OIX; OITF §V) + Legal agreements for exchange structure (OIX; OITF §II, §III.C) + Security, privacy & consent (OIX; OITF §III.A) + Liability, representations & warranties (OITF §III.C) + Grant of authority (OIX; OITF §III.C) + Dispute resolution (OITF §II, §III.C, §V) + Authorizations for data exchange (OIX; OITF §III.A) + Anti-circumvention & open disclosure (OITF §V) + Audit (OIX; OITF §II, §III.B, §V) + Accountability & compliance (OIX; OITF §II, §V) 	<ul style="list-style-type: none"> + Performance & service specifications (OIX; OITF §II, §III.A, §III.B) + Security, privacy & confidentiality (OIX; OITF §III.A; §V) + Expectations of Members (OIX; OITF §III.A, §III.B, §III.C) + Onboarding, testing & certification (OIX; OITF §II, §III.B) 	<ul style="list-style-type: none"> + Openness & transparency (OIX; OITF §I; statement in OITF §V, §VI) + TF lifecycle management (OIX; OITF §II) + Scalability to support array of Members (horizontal/vertical) (OITF §II, §III.C, §IV) + High-level definitions (OITF §I) + Component-based approach for different Member types (OIX; OITF §II, §III.C) + Use cases & examples of TFs (OITF §IV)

OITF=The Open Identity Trust Framework (OITF) Model, March 2010

OIX=Open Identity Exchange Trust Framework Requirements and Guidelines v. 1 (Draft 2)