

COMMONWEALTH OF VIRGINIA



Information Technology Resource Management (ITRM)

GUIDANCE DOCUMENT
Identity Trust Frameworks

Virginia Information Technologies Agency (VITA)

Table of Contents

1	Publication Version Control	1
2	Reviews	1
3	Statutory Authority	2
4	Definitions	3
5	Background	14
6	Minimum Specifications	15
7	Alignment Comparison	19

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, Code of Virginia

2 Reviews

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

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

3 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 Trust Frameworks. 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/>

Secretary of Transportation

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

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

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/>

Chief Information Officer (CIO) of the Commonwealth

§ 2.2-2007. Powers of the CIO

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

Virginia Information Technologies Agency

Chapter 20.1. Virginia Information Technologies Agency

<http://law.lis.virginia.gov/vacode/title2.2/chapter20.1/>

70 **4 Definitions**71
72
73
74
75

Terms used in this document adopted definitions in the National Institute of Standards and Technology Special Publication 800-63-2 (NIST SP 800-63-2). Terms used in this document not published in NIST SP 800-63-2 align with industry standard definitions.

Active Attack	An attack on the authentication protocol where the Attacker transmits data to the Claimant, Credential Service Provider, Verifier, or Relying Party. Examples of active attacks include man-in-the-middle, impersonation, and session hijacking.
Address of Record	The official location where an individual can be found. The address of record always includes the residential street address of an individual and may also include the mailing address of the individual.
Approved	Federal Information Processing Standard (FIPS) approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation.
Applicant	A party undergoing the processes of registration and identity proofing.
Assertion	A statement from a Verifier to a Relying Party (RP) that contains identity information about a Subscriber. Assertions may also contain verified attributes.
Assertion Reference	A data object, created in conjunction with an assertion, which identifies the Verifier and includes a pointer to the full assertion held by the Verifier.
Assurance	In the context of OMB M-04-04 and this document, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.
Asymmetric Keys	Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.
Attack	An attempt by an unauthorized individual to fool a Verifier or a Relying Party into believing that the unauthorized individual in question is the Subscriber.
Attacker	A party who acts with malicious intent to compromise an information system.
Attribute	A claim of a named quality or characteristic inherent in or ascribed to someone or something. (See term in [ICAM] for more information.)
Authentication	The process of establishing confidence in the identity of users or information systems.

Authentication Protocol	A defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has possession and control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier.
Authentication Protocol Run	An exchange of messages between a Claimant and a Verifier that results in authentication (or authentication failure) between the two parties.
Authentication Secret	A generic term for any secret value that could be used by an Attacker to impersonate the Subscriber in an authentication protocol. These are further divided into short-term authentication secrets, which are only useful to an Attacker for a limited period of time, and long-term authentication secrets, which allow an Attacker to impersonate the Subscriber until they are manually reset. The token secret is the canonical example of a long-term authentication secret, while the token authenticator, if it is different from the token secret, is usually a short-term authentication secret.
Authenticity	The property that data originated from its purported source.
Bearer Assertion	An assertion that does not provide a mechanism for the Subscriber to prove that he or she is the rightful owner of the assertion. The RP has to assume that the assertion was issued to the Subscriber who presents the assertion or the corresponding assertion reference to the RP.
Bit	A binary digit: 0 or 1.
Biometrics	Automated recognition of individuals based on their behavioral and biological characteristics. Biometrics may be used to unlock authentication tokens and prevent repudiation of registration.
Certificate Authority (CA)	A trusted entity that issues and revokes public key certificates.
Certificate Revocation List (CRL)	A list of revoked public key certificates created and digitally signed by a Certificate Authority. See [RFC 5280].
Challenge-Response Protocol	An authentication protocol where the Verifier sends the Claimant a challenge (usually a random value or a nonce) that the Claimant combines with a secret (such as by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the Verifier. The Verifier can independently verify the response generated by the Claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the Claimant possesses and controls the secret.
Claimant	A party whose identity is to be verified using an authentication

	protocol.
Claimed Address	<p>The physical location asserted by an individual (e.g. an applicant) where he/she can be reached. It includes the residential street address of an individual and may also include the mailing address of the individual.</p> <p>For example, a person with a foreign passport, living in the U.S., will need to give an address when going through the identity proofing process. This address would not be an “address of record” but a “claimed address.”</p>
Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)	An interactive feature added to web forms to distinguish use of the form by humans as opposed to automated agents. Typically, it requires entering text corresponding to a distorted image or from a sound stream.
Cookie	<p>A character string, placed in a web browser’s memory, which is available to websites within the same Internet domain as the server that placed them in the web browser.</p> <p>Cookies are used for many purposes and may be assertions or may contain pointers to assertions.</p>
Credential	<p>An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber.</p> <p>While common usage often assumes that the credential is maintained by the Subscriber, this document also uses the term to refer to electronic records maintained by the CSP which establish a binding between the Subscriber’s token and identity.</p>
Credential Service Provider (CSP)	A trusted entity that issues or registers Subscriber tokens and issues electronic credentials to Subscribers. The CSP may encompass Registration Authorities (RAs) and Verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.
Cross-Site Request Forgery (CSRF)	<p>An attack in which a Subscriber who is currently authenticated to an RP and connected through a secure session, browses to an Attacker’s website which causes the Subscriber to unknowingly invoke unwanted actions at the RP.</p> <p>For example, if a bank website is vulnerable to a CSRF attack, it may be possible for a Subscriber to unintentionally authorize a large money transfer, merely by viewing a malicious link in a webmail message while a connection to the bank is open in another browser window.</p>
Cross-Site Scripting (XSS)	A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of

	scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user-supplied data from requests or forms without sanitizing the data so that it is not executable.
Cryptographic Key	A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, key requirements shall meet the minimum requirements stated in Table 2 of NIST SP 800-57 Part 1. See also Asymmetric keys, Symmetric key.
Cryptographic Token	A token where the secret is a cryptographic key.
Data Integrity	The property that data has not been altered by an unauthorized entity.
Derived Credential	A credential issued based on proof of possession and control of a token associated with a previously issued credential, so as not to duplicate the identity proofing process.
Digital Signature	An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation.
Eavesdropping Attack	An attack in which an Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant.
Electronic Authentication (E-Authentication)	The process of establishing confidence in user identities electronically presented to an information system.
Entropy	A measure of the amount of uncertainty that an Attacker faces to determine the value of a secret. Entropy is usually stated in bits.
Extensible Markup Language (XML)	Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them.
Federal Bridge Certification Authority (FBCA)	The FBCA is the entity operated by the Federal Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI Policy Authority to create, sign, and issue public key certificates to Principal CAs.
Federal Information Security Management Act (FISMA)	Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
Federal Information Processing Standard	Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and

(FIPS)	<p>guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions. See background information for more details.</p> <p>FIPS documents are available online through the FIPS home page: http://www.nist.gov/itl/fips.cfm</p>
Governance	The responsible for providing policy level leadership, oversight, strategic direction and related governance activities within a system.
Guessing Entropy	A measure of the difficulty that an Attacker has to guess the average password used in a system. Entropy is stated in bits. When a password has n-bits of guessing entropy then an Attacker has as much difficulty guessing the average password as in guessing an n-bit random quantity. The Attacker is assumed to know the actual password frequency distribution.
Hash Function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: <ol style="list-style-type: none"> 1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and 2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.
Holder of Key Assertion	An assertion that contains a reference to a symmetric key or a public key (corresponding to a private key) held by the Subscriber. The RP may authenticate the Subscriber by verifying that he or she can indeed prove possession and control of the referenced key.
HTTPS	Protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or Secure Sockets Layer.
Identity	A set of attributes that uniquely describe a person within a given context.
Identity, Access and Credential Management (ICAM)	A comprehensive, strategic framework and architecture adopted by federal and state government for the management of digital identities, credentials, and access control protocols.
Identity Proofing	The process by which a CSP and a Registration Authority (RA) collect and verify information about a person for the purpose of issuing credentials to that person.
In-Person Identity Proofing	Method of identity proofing in which Applicants are required to present themselves and identity evidence to a representative of the

	Registration Authority. (Required for Level of Assurance 4 authentication.)
Kerberos	A widely used authentication protocol developed at MIT. In “classic” Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to-KDC exchange. Longer password length and complexity provide some mitigation to this vulnerability, although sufficiently long passwords tend to be cumbersome for users.
Knowledge Based Authentication (KBA)	Authentication of an individual based on knowledge of information associated with his or her claimed identity in public or private databases. Knowledge of such information is considered to be private rather than secret, because it may be used in contexts other than authentication to a Verifier, thereby reducing the overall assurance associated with the authentication process.
Level of Assurance (LoA)	The continuum for the degree of certainty in the user’s identity established by the Registration Authority during the registration process. The term Level of Assurance in this document aligns with the levels defined for federal agencies in the U.S. Office of Management and Budget Memorandum M04-04 and NIST SP 800-63-2 (i.e., Levels 1-4) but provides for a more general framework to accommodate other identity management standards and protocols.
Man-in-the-Middle Attack (MitM)	An attack on the authentication protocol run in which the Attacker positions himself or herself in between the Claimant and Verifier so that he can intercept and alter data traveling between them.
Message Authentication Code (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection, but not non-repudiation protection.
Min-entropy	A measure of the difficulty that an Attacker has to guess the most commonly chosen password used in a system. Entropy is stated in bits. When a password has n-bits of min-entropy then an Attacker requires as many trials to find a user with that password as is needed to guess an n-bit random quantity. The Attacker is assumed to know the most commonly used password(s).
Multi-Factor	A characteristic of an authentication system or a token that uses more than one authentication factor. The three types of authentication factors are something you know,

	something you have, and something you are.
Network	An open communications medium, typically the Internet, that is used to transport messages between the Claimant and other parties. Unless otherwise stated, no assumptions are made about the security of the network; it is assumed to be open and subject to active (i.e., impersonation, man-in-the-middle, session hijacking) and passive (i.e., eavesdropping) attack at any point between the parties (e.g., Claimant, Verifier, CSP or RP).
Nonce	A value used in security protocols that is never repeated with the same key. For example, nonces used as challenges in challenge-response authentication protocols must not be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable.
Off-line Attack	An attack where the Attacker obtains some data (typically by eavesdropping on an authentication protocol run or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing.
Online Attack	An attack against an authentication protocol where the Attacker either assumes the role of a Claimant with a genuine Verifier or actively alters the authentication channel.
Online-Guessing Attack	An attack in which an Attacker performs repeated logon trials by guessing possible values of the token authenticator.
Operational	The responsible for operations, maintenance, management and related functions within a management system.
Participant	A participating member of a system, including Registration Authorities, Credential Service Providers, and Relying Parties.
Passive Attack	An attack against an authentication protocol where the Attacker intercepts data traveling along the network between the Claimant and Verifier, but does not alter the data (i.e., eavesdropping).
Password	A secret that a Claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings.
Personal Identification Number (PIN)	A password consisting only of decimal digits.
Personal Identity Verification (PIV) Card	Defined by [FIPS 201] as a physical artifact (e.g., identity card, smart card) issued to federal employees and contractors that contains stored credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

Personally Identifiable Information (PII)	Defined by GAO Report 08-536 as “Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.”
Pharming	An attack in which an Attacker corrupts an infrastructure service such as DNS (Domain Name Service) causing the Subscriber to be misdirected to a forged Verifier/RP, which could cause the Subscriber to reveal sensitive information, download harmful software or contribute to a fraudulent act.
Phishing	An attack in which the Subscriber is lured (usually through an email) to interact with a counterfeit Verifier/RP and tricked into revealing information that can be used to masquerade as that Subscriber to the real Verifier/RP.
Possession and control of a token	The ability to activate and use the token in an authentication protocol.
Practice Statement	A formal statement of the practices followed by the parties to an authentication process (i.e., RA, CSP, or Verifier). It usually describes the policies and practices of the parties and can become legally binding.
Private Credentials	Credentials that cannot be disclosed by the CSP because the contents can be used to compromise the token.
Private Key	The secret part of an asymmetric key pair that is used to digitally sign or decrypt data.
Protected Session	A session wherein messages between two Participants are encrypted and integrity is protected using a set of shared secrets called session keys. A Participant is said to be authenticated if, during the session, he, she or it proves possession of a long term token in addition to the session keys, and if the other party can verify the identity associated with that token. If both Participants are authenticated, the protected session is said to be mutually authenticated.
Pseudonym	A false name. All unverified names are assumed to be pseudonyms.
Public Credentials	Credentials that describe the binding in a way that does not compromise the token.
Public Key	The public part of an asymmetric key pair that is used to verify signatures or encrypt data.
Public Key Certificate	A digital document issued and digitally signed by the private key of a Certificate authority that binds the name of a Subscriber to a public key. The certificate indicates that the Subscriber identified in the certificate has sole control and access to the private key.

Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration	The process through which an Applicant applies to become a Subscriber of a CSP and an RA validates the identity of the Applicant on behalf of the CSP.
Registration Authority (RA)	A trusted entity that establishes and vouches for the identity or attributes of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).
Relying Party (RP)	An entity that relies upon the Subscriber's token and credentials or a Verifier's assertion of a Claimant's identity, typically to process a transaction or grant access to information or a system.
Remote	(As in remote authentication or remote transaction) An information exchange between network connected devices where the information cannot be reliably protected end-to-end by a single organization's security controls. Note: Any information exchange across the Internet is considered remote.
Replay Attack	An attack in which the Attacker is able to replay previously captured messages (between a legitimate Claimant and a Verifier) to masquerade as that Claimant to the Verifier or vice versa.
Risk Assessment	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.
Salt	A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an Attacker.
Secondary Authenticator	A temporary secret, issued by the Verifier to a successfully authenticated Subscriber as part of an assertion protocol. This secret is subsequently used, by the Subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer assertions, assertion references, and Kerberos session keys.
Secure Sockets Layer (SSL)	An authentication and security protocol widely implemented in browsers and web servers. SSL has been superseded by the newer Transport Layer Security (TLS) protocol; TLS 1.0 is effectively SSL version 3.1.
Security Assertion Mark-up Language (SAML)	An XML-based security specification developed by the Organization for the Advancement of Structured Information Standards (OASIS) for exchanging authentication (and authorization) information between trusted entities over the Internet. See [SAML].

SAML Authentication Assertion	A SAML assertion that conveys information from a Verifier to an RP about a successful act of authentication that took place between the Verifier and a Subscriber.
Session Hijack Attack	An attack in which the Attacker is able to insert himself or herself between a Claimant and a Verifier subsequent to a successful authentication exchange between the latter two parties. The Attacker is able to pose as a Subscriber to the Verifier or vice versa to control session data exchange. Sessions between the Claimant and the Relying Party can also be similarly compromised.
Shared Secret	A secret used in authentication that is known to the Claimant and the Verifier.
Social Engineering	he ability to collect publically available information on individuals and engineering it in a way that enables discovery of passwords, PINs, and other identity secrets.
Special Publication (SP)	A type of publication issued by NIST. Specifically, the Special Publication 800-series reports on the Information Technology Laboratory's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.
Strongly Bound Credentials	Credentials that describe the binding between a user and token in a tamper-evident fashion.
Subscriber	A party who has received a credential or token from a CSP.
Symmetric Key	A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.
Token	Something that the Claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the Claimant's identity.
Token Authenticator	The output value generated by a token. The ability to generate valid token authenticators on demand proves that the Claimant possesses and controls the token. Protocol messages sent to the Verifier are dependent upon the token authenticator, but they may or may not explicitly contain it.
Token Secret	The secret value, contained within a token, which is used to derive token authenticators.
Transport Layer Security (TLS)	An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by [RFC 2246], [RFC 3546], and [RFC 5246]. TLS is similar to the older Secure Sockets Layer (SSL) protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations specifies how TLS is to be used in government applications.

Trust Anchor	A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g. in a public key certificate).
Trust Framework	A “digital identity system with established identity, security, privacy, technology, and enforcement rules and policies adhered to by certified identity providers that are members of the identity Trust Framework.” Trust frameworks consist of multiparty agreements among Participants in a system, which enforce requirements and ensure trust in the acceptance of identity credentials.
Unverified Name	An applicant name that is not verified as meaningful by identity proofing.
Valid	In reference to an ID, the quality of not being expired or revoked.
Verified Name	An applicant name that has been verified by identity proofing.
Verifier	An entity that verifies the Claimant’s identity by verifying the Claimant’s possession and control of a token using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the token and identity and check their status.
Verifier Impersonation Attack	A scenario where the Attacker impersonates the Verifier in an authentication protocol, usually to capture information that can be used to masquerade as a Claimant to the real Verifier.
Weakly Bound Credentials	Credentials that describe the binding between a user and token in a manner that can be modified without invalidating the credential.
Zeroize	Overwrite a memory location with data consisting entirely of bits with the value zero so that the data is destroyed and not recoverable. This is often contrasted with deletion methods that merely destroy reference to data within a file system rather than the data itself.
Zero-knowledge Password Protocol	A password based authentication protocol that allows a claimant to authenticate to a Verifier without revealing the password to the Verifier. Examples of such protocols are EKE, SPEKE and SRP.

76 Terms used in this document comply with definitions in the Public Review version of the
 77 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3),
 78 and align with adopted definitions in § 59.1-550, Code of Virginia (COV), and the
 79 Commonwealth of Virginia’s ITRM Glossary (ITRM Glossary).¹
 80

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

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

84

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

90

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

94

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

97

98 Applicant: A party undergoing the processes of registration and identity proofing.

99

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

102

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

105

106

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

111
112 Assurance Model: Policies, processes, and protocols that define how Assurance will be
113 established in an Identity Trust Framework.

114
115 Asymmetric Keys: Two related keys, a public key and a private key that are used to perform
116 complementary operations, such as encryption and decryption or signature generation and
117 signature verification.

118
119 Attack: An attempt by an unauthorized individual to fool a verifier or a relying party into
120 believing that the unauthorized individual in question is the subscriber.

121
122 Attacker: A party who acts with malicious intent to compromise an Information System.

123
124 Attribute: A claim of a named quality or characteristic inherent in or ascribed to someone or
125 something.

126
127 Authentication: The process of establishing confidence in the identity of users or Information
128 Systems.

129
130 Authentication Protocol: A defined sequence of messages between a claimant and a verifier
131 that demonstrates that the claimant has possession and control of a valid authenticator to
132 establish his/her identity, and optionally, demonstrates to the claimant that he or she is
133 communicating with the intended verifier.

134
135 Authentication Protocol Run: An exchange of messages between a claimant and a verifier that
136 results in authentication (or authentication failure) between the two parties.

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

145

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>.

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

149
150 Authenticator Assurance Level (AAL): A metric describing robustness of the authentication
151 process proving that the claimant is in control of a given subscriber's authenticator(s).

152
153 Authenticator Output: The output value generated by an authenticator. The ability to generate
154 valid authenticator outputs on demand proves that the claimant possesses and controls the
155 authenticator. Protocol messages sent to the verifier are dependent upon the authenticator
156 output, but they may or may not explicitly contain it.

157
158 Authenticator Secret: The secret value contained within an authenticator.

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

160
161 Bearer Assertion: An assertion that does not provide a mechanism for the subscriber to prove
162 that he or she is the rightful owner of the assertion. The RP has to assume that the assertion
163 was issued to the subscriber who presents the assertion or the corresponding assertion
164 reference to the RP.

165
166 Bit: A binary digit: 0 or 1.

167
168 Biometrics: Automated recognition of individuals based on their behavioral and biological
169 characteristics. In this document, biometrics may be used to unlock authenticators and prevent
170 repudiation of registration.

171
172 Certificate Authority (CA): A trusted entity that issues and revokes public key certificates.

173
174 Certificate Revocation List (CRL): A list of revoked public key certificates created and digitally
175 signed by a Certificate Authority. [RFC 5280]³

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

185
186 Claimant: A party whose identity is to be verified using an authentication protocol.

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

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

192
193 Claimed Identity: A declaration by the applicant of their current Personal Name, date of birth
194 and address. [GPG45]⁴

195
196 Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA): An
197 interactive feature added to web-forms to distinguish use of the form by humans as opposed to
198 automated agents. Typically, it requires entering text corresponding to a distorted image or
199 from a sound stream.

200
201 Cookie: A character string, placed in a web browser’s memory, which is available to websites
202 within the same Internet domain as the server that placed them in the web browser.

203
204 Credential: An object or data structure that authoritatively binds an identity (and optionally,
205 additional attributes) to an authenticator possessed and controlled by a subscriber. While
206 common usage often assumes that the credential is maintained by the subscriber, this
207 document also uses the term to refer to electronic records maintained by the CSP which
208 establish a binding between the subscriber’s authenticator(s) and identity.

209
210 Credential Service Provider (CSP): A trusted entity that issues or registers subscriber
211 authenticators and issues electronic credentials to subscribers. The CSP may encompass
212 Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third
213 party, or may issue credentials for its own use.

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

221
222 Cross Site Scripting (XSS): A vulnerability that allows attackers to inject malicious code into an
223 otherwise benign website. These scripts acquire the permissions of scripts generated by the
224 target website and can therefore compromise the confidentiality and integrity of data transfers

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

225 between the website and client. Websites are vulnerable if they display user supplied data from
226 requests or forms without sanitizing the data so that it is not executable.
227

228 Cryptographic Key: A value used to control cryptographic operations, such as decryption,
229 encryption, signature generation or signature verification. For the purposes of this document,
230 key requirements shall meet the minimum requirements stated in Table 2 of NIST SP 800-57
231 Part 1. See also Asymmetric keys, Symmetric key.
232

233 Cryptographic Authenticator: An authenticator where the secret is a cryptographic key.
234

235 Data Integrity: The property that data has not been altered by an unauthorized entity.
236

237 Derived Credential: A credential issued based on proof of possession and control of an
238 authenticator associated with a previously issued credential, so as not to duplicate the identity
239 proofing process.
240

241 Digital Identity System: An Information System that supports Electronic Authentication and the
242 management of a person’s Identity in a digital environment. [Referenced in § 59.1-550, COV]
243

244 Digital Signature: An asymmetric key operation where the private key is used to digitally sign
245 data and the public key is used to verify the signature. Digital signatures provide authenticity
246 protection, integrity protection, and non-repudiation.
247

248 Eavesdropping Attack: An attack in which an attacker listens passively to the authentication
249 protocol to capture information which can be used in a subsequent active attack to
250 masquerade as the claimant.
251

252 Electronic Authentication: The process of establishing confidence in user identities
253 electronically presented to an Information System.
254

255 Entropy: A measure of the amount of uncertainty that an attacker faces to determine the value
256 of a secret. Entropy is usually stated in bits.
257

258 Extensible Mark-up Language (XML): Extensible Markup Language, abbreviated XML, describes
259 a class of data objects called XML documents and partially describes the behavior of computer
260 programs which process them.
261

262 Federal Bridge Certification Authority (FBCA): The FBCA is the entity operated by the Federal
263 Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI
264 Policy Authority to create, sign, and issue public key certificates to Principal CAs.
265

266 Federal Information Security Management Act (FISMA): Title III of the E-Government Act
267 requiring each federal agency to develop, document, and implement an agency-wide program
268 to provide information security for the information and Information Systems that support the

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

271

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

279

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

282

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

285

- 286 • (One-way) It is computationally infeasible to find any input that maps to any pre-
287 specified output, and
- 288 • (Collision resistant) It is computationally infeasible to find any two distinct inputs that
289 map to the same output.

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

294

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

296

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

299

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

302

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

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

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

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

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

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

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

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

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

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

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

356
357 Online Attack: An attack against an authentication protocol where the attacker either assumes
358 the role of a claimant with a genuine verifier or actively alters the authentication channel.

359
360 Online Guessing Attack: An attack in which an attacker performs repeated logon trials by
361 guessing possible values of the authenticator output.

362
363 Operational Authority: Entity responsible for operations, maintenance, management, and
364 related functions of an Identity Trust Framework.

365
366 Passive Attack: An attack against an authentication protocol where the attacker intercepts data
367 traveling along the network between the claimant and verifier, but does not alter the data (i.e.,
368 eavesdropping).

369
370 Password: A secret that a claimant memorizes and uses to authenticate his or her identity.
371 Passwords are typically character strings.

372
373 Personal Identification Number (PIN): A password consisting only of decimal digits.

374
375 Personal Identity Verification (PIV) Card: Defined by [FIPS 201] as a physical artifact (e.g.,
376 identity card, smart card) issued to federal employees and contractors that contains stored
377 credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that
378 the claimed identity of the cardholder can be verified against the stored credentials by another
379 person (human readable and verifiable) or an automated process (computer readable and
380 verifiable).

381
382 Personally Identifiable Information (PII): As defined by OMB Circular A-130, Personally
383 Identifiable Information means information that can be used to distinguish or trace an
384 individual's identity, either alone or when combined with other information that is linked or
385 linkable to a specific individual.

386
387 Pharming: An attack in which an attacker corrupts an infrastructure service such as DNS
388 (Domain Name Service) causing the subscriber to be misdirected to a forged verifier/RP, which
389 could cause the subscriber to reveal sensitive information, download harmful software or
390 contribute to a fraudulent act.

391
392 Phishing: An attack in which the subscriber is lured (usually through an email) to interact with a
393 counterfeit verifier/RP and tricked into revealing information that can be used to masquerade
394 as that subscriber to the real verifier/RP.

395

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

398

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

402

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

405

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

408

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

415

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

419

420 Public Credentials: Credentials that describe the binding in a way that does not compromise the
421 authenticator.

422

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

425

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

430

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

434

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

437

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

441

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

445

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

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

453

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

457

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

460

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

465

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

469

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

474

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

478

479 Session Hijack Attack: An attack in which the attacker is able to insert himself or herself
480 between a claimant and a verifier subsequent to a successful authentication exchange between
481 the latter two parties. The attacker is able to pose as a subscriber to the verifier or vice versa to

482 control session data exchange. Sessions between the claimant and the relying party can also be
483 similarly compromised.

484

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

486

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

489

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

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

496

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

498

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

502

503 Token: See Authenticator.

504

505 Token Authenticator: See Authenticator Output.

506

507 Token Secret: See Authenticator Secret.

508

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

514

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

518

519 Unverified Name: A subscriber name that is not verified as meaningful by identity proofing.

520

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

522

523 Verified Name: A subscriber name that has been verified by identity proofing.

524

525 Verifier: An entity that verifies the claimant’s identity by verifying the claimant’s possession and
526 control of one or two authenticators using an authentication protocol. To do this, the verifier
527 may also need to validate credentials that link the authenticator(s) and identity and check their
528 status.

529
530 Verifier Impersonation Attack: A scenario where the attacker impersonates the verifier in an
531 authentication protocol, usually to capture information that can be used to masquerade as a
532 claimant to the real verifier.

533
534 Virtual In-Person Proofing: A remote identity person proofing process that employs technical
535 and procedural measures that provide sufficient confidence that the remote session can be
536 considered equivalent to a physical, in-person identity proofing encounter. [NIST SP 800-63A]

537
538 Weakly Bound Credentials: Credentials that describe the binding between a user and
539 authenticator in a manner than can be modified without invalidating the credential.

540
541 Zeroize: Overwrite a memory location with data consisting entirely of bits with the value zero
542 so that the data is destroyed and not recoverable. This is often contrasted with deletion
543 methods that merely destroy reference to data within a file system rather than the data itself.

544
545 Zero-knowledge Password Protocol: A password based authentication protocol that allows a
546 claimant to authenticate to a Verifier without revealing the password to the verifier. Examples
547 of such protocols are EKE, SPEKE and SRP.

548 5 Background

549

550 In 2015, Virginia’s General Assembly passed the Electronic Identity Management Act (Chapter
551 50, Code of Virginia) to address demand in the state’s digital economy for secure, privacy
552 enhancing electronic authentication and identity management. Growing numbers of
553 “communities of interest” have advocated for stronger, scalable and interoperable identity
554 solutions to increase consumer protection and reduce liability for principal actors in the identity
555 ecosystem – Identity Providers, Credential Service Providers and Relying Parties.

556

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

563

564 The Advisory Council recommends to the Secretary of Technology guidance documents relating
565 to (i) nationally recognized technical and data standards regarding the verification and
566 authentication of identity in digital and online transactions; (ii) the minimum specifications and
567 standards that should be included in an Identity Trust Framework, as defined in §59.1-550, so
568 as to warrant liability protection pursuant to the Electronic Identity Management Act (§59.1-
569 550 et seq.); and (iii) any other related data standards or specifications concerning reliance by
570 third parties on identity credentials, as defined in §59.1-550. The following guidance document
571 has been developed by the Virginia Information Technologies Agency (VITA), acting on behalf of
572 the Secretary of Technology and Chief Information Officer of the Commonwealth, at the
573 direction of IMSAC. IMSAC was created by the General Assembly and advises the Secretary of
574 Technology on the adoption of identity management standards and the creation of guidance
575 documents pursuant to §2.2-436. A copy of the IMSAC Charter has been provided in **Appendix**
576 **1.** IMSAC recommends to the Secretary of Technology guidance documents relating to (i)
577 nationally recognized technical and data standards regarding the verification and
578 authentication of identity in digital and online transactions; (ii) the minimum specifications and
579 standards that should be included in an identity, as defined in §59.1-550, so as to warrant
580 liability protection pursuant to the Electronic Identity Management Act (§59.1-550 et seq.); and
581 (iii) any other related data standards or specifications concerning reliance by third parties on
582 identity credentials, as defined in §59.1-550.

583

584 Purpose Statement

585

586 The purpose of this document is to establish minimum specifications for Identity Trust
 587 Frameworks. The document assumes that the Identity Trust Framework will be compliant with
 588 Applicable Law.⁶

589
 590 The document defines minimum requirements, components, and related provisions for Identity
 591 Trust Frameworks. The document assumes that specific Identity Trust Frameworks will address
 592 the business, legal and technical requirements for each distinct identity management
 593 systemDigital Identity System, and that these requirements will be designed based on the
 594 specific Assurance Model supported by the system.

595
 596 The document limits its focus to Identity Trust Frameworks. Minimum specifications for other
 597 components of an identity management systemDigital Identity System have been defined in
 598 separate IMSAC guidance documents in this series, pursuant to §2.2-436 and §2.2-437.

599 6 Minimum Specifications

600
 601 The Commonwealth of Virginia’s Electronic Identity Management Act defines “Identity Trust
 602 Framework” as “a digital identity systemDigital Identity System with established identity,
 603 security, privacy, technology, and enforcement rules and policies adhered to by certified
 604 identity providers that are members of the Identity Trust Framework” (§ 59.1-550). Identity
 605 Trust Frameworks consist of multiparty agreements among members, which enforce
 606 requirements and ensure trust in the acceptance of identity credentials.

607
 608 This document establishes minimum specifications for Identity Trust Frameworks. Identity
 609 Trust Frameworks should be designed to document the business, legal, and technical
 610 components for enterprise architecture, business processes, governance models, operational
 611 policies and practices, and Participant member obligations within the system. Identity Trust
 612 Frameworks also should contain the requirements for meeting the Levels of
 613 AssuranceAssurance Model supported by the system.⁷ Subsequent guidance documents in the
 614 IMSAC series have addressed other components of an identity management systemDigital
 615 Identity System, pursuant to §2.2-436 and §2.2-437.

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

⁷ The term “Level of AssuranceAssurance 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 continuum for the degree of certainty in the user’s identity established within the identity management system. The term aligns with the Assurance Model established in the with the levels defined for federal agencies in the U.S. Office of Management and Budget Memorandum M04-04 and Public Review version of NIST SP 800-63-2-3 (i.e., Levels 1-4) but provides for a more general framework to accommodate other identity management standards and protocols.

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 2015.⁸

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.
- 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 **Identity** information.
- 640 • Suspension & Termination (Voluntary & Involuntary): Provisions for suspending or
 641 terminating a **Participant member** due to failure to meet the obligations in the agreement,
 642 or the **Participant’s member’s** self-suspension or termination of participation in the **identity**
 643 **management system Identity Trust Framework.**
- 644 • Data Elements & Data Classification: Attribute-level documentation, **classification, and**
 645 **labeling of the** person **identity-Identity** information used within the **identity management**
 646 **system Identity Trust Framework** to **support compliant handling of the data through the**
 647 **entire data lifecycle.**
- 648 • **Expectations of Performance**: Provisions in the **Identity Trust Framework** that **set** the
 649 performance and service criteria for all **Participants members – IdPs, CSPs, and RPs –**
 650 **including requirements for breach response and resolution, system(s) interruption or**
 651 **failure, and other risk situations.**
- 652 • Use Cases (Exchange & **Participant Member** Types): Documented examples for roles and
 653 responsibilities **of members of the Identity Trust Framework** and data flows across the
 654 **identity management system Digital Identity System.**

Comment [JG2]: Add a statement re business continuity, as ID systems must support business continuity requirements. (D. Burhop)

Comment [JG3]: Data labeling and handling requirements. (T. Moran)

Comment [JG4]: Add language covering what happens when “things go wrong” and disclosure. (K. Crepps and J. Grant)

Comment [JG5]: Incorporate role-based provisions, IdPs RPs, etc. (J. Grant)

⁸ 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.

655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696

Legal Components

- Definition/Identification of “Applicable Law”: Provisions requiring Participants-members of the Identity Trust Framework to comply with all governing laws, statutes, rules, and regulations of the jurisdiction in which each Participant-member operates.
- Legal Agreements for Exchange Structure: Statement of requirements for the architecture, performance, and service specifications, and Participant-member obligations for the operation and maintenance of the exchange of person identity-Identity information within the Identity Trust Framework.
- Security, Privacy & Consent Provisions (Legal): Terms and conditions establishing Participant-member obligations for the collection, labeling, operational use, and maintenance of person identity-Identity information and for gaining consent from the person for using identity-Identity information.
- Assignment of Liability & Risk for ParticipantsMembers: Articles that define how liability and risk within the identity-management-systemIdentity Trust Framework will be distributed among Participantsmembers, with indemnification provisions for violation of the agreement.
- Representations & Warranties: Statements of factual principles in the Identity Trust Framework upon which Participants-members may rely, and assurances of the implied indemnification obligation in the event the principles are violated or proven false.
- Grant of Authority: Provisions requiring Participants-members of the Identity Trust Framework to assign to the Governance Authority decision-making authority over the identity-management-systemIdentity Trust Framework.
- Dispute Resolution: Statement of requirements and processes for mediation and the resolution of disputes among Participants-members in the identity-management-systemIdentity Trust Framework in a manner that avoids adjudicative procedures.
- Authorizations for Data Requests by ParticipantMembers: Articles defining role-based rules, requirements, and processes for Participants-members of the Identity Trust Framework in the identity-management-system to access person identity information.
- Open Disclosure & Anti-Circumvention: Provisions requiring transparency in the rules, policies, and practices for operations and governance of the Identity Trust Framework, and prohibiting the circumvention of technical protections within the identity-management-systemDigital Identity System for the handling of person identity-Identity information.
- Confidential Participant Person Information: Statements documenting the business, legal and technical requirements for the classification, labeling and handling of confidential person identity-Identity information.
- Audit, Accountability & Compliance: Terms of conditions documenting and requiring Participants-members of the Identity Trust Framework to comply with audit procedures, and the consequences of Participants-members failing to comply with the audit findings and corrective action plan to address deficiencies.

Comment [JG6]: Data labeling and handling requirements. (T. Moran)

697 Technical Components

698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737

- Performance & Service Specifications: Architecture and infrastructure specifications, protocols, and requirements ~~for all members – IdPs, CSPs, and RPs –~~ covering full end-to-end integration for the ~~Digital Identity System supported by the identity management system~~ Identity Trust Framework, including technical, solutions, and information architecture.
- Security, Privacy & Confidentiality: Architecture and infrastructure specifications, protocols, and requirements within the ~~Digital Identity System supported by the identity management system~~ Identity Trust Framework designed for the collection, labeling, operational use, and maintenance of person ~~identity-Identity~~ information and for gaining consent from the person for using ~~identity-Identity~~ information.
- Breach Notification: Processes, protocols, and requirements compliant with Applicable Law for notifying the appropriate authorities in the event of a breach of person ~~identity-Identity~~ information, and related risk situations, within the ~~identity management system~~ Identity Trust Framework.
- System Access (ID/Authentication): Standards-based, open architecture processes, protocols, and requirements for Participant-member authentication and access to the ~~identity management system~~ Digital Identity System supported by the Identity Trust Framework.
- Provisions for Future Use of Data: Terms and conditions defining limitations on, and permitted purposes for, the use of person ~~identity-Identity~~ information after the information has been used for the Registration event and the issuance of a ~~credential~~ Credential by a Credential Service Provider.
- Duty of Response by ~~Participants~~ Members: Terms and conditions requiring Identity Trust Framework ~~Participant-member information system~~ Information Systems to respond to and process messaging requests – inbound and outbound – within the ~~identity management system~~ Digital Identity System, normally establishing the time in which the ~~Participant member~~ system must respond and process the request.
- Onboarding, Testing & Certification Requirements: Documented processes, protocols, specifications, and requirements for onboarding, testing, and certifying prospective ~~Participants-member~~ Information Systems in the ~~identity management system~~ Identity Trust Framework.
- Handling of Test Data v. Production Data: Terms and conditions compliant with Applicable Law preventing the use of production data in a test environment.
- Compliance with Governing Standards: Terms and conditions identifying and stating requirements for ~~Participant-member~~ compliance with governing external standards for the ~~identity management system~~ Identity Trust Framework, including standards for information processing, ~~e-Electronic A~~ authentication, and ~~authorization~~ Authorization.

Comment [JG7]: Incorporate role-based provisions, IdPs RPs, etc. (J. Grant)

Comment [JG8]: Data labeling and handling. (T. Moran)

738 7 Alignment Comparison

739 The minimum specifications for Identity Trust Frameworks established in this document have
 740 been developed based on a detailed comparison analysis of Identity Trust Frameworks and
 741 related governance models currently operational in the identity management ecosystem.
 742 Specifically, the minimum specifications build upon core components of existing Identity Trust
 743 Frameworks while adapting or extending them to meet the requirements of IMSAC, pursuant to
 744 §2.2-436-§2.2-437. The analysis covered Identity Trust Frameworks on a global scale, including
 745 a detailed review of the Open Identity Exchange (OIX) Trust Framework Model (OIX/OITF) and
 746 the European Union (EU) standards.

747
 748
 749 The following operational Identity Trust Frameworks were evaluated by IMSAC. Results from
 750 the alignment comparison analysis have been compiled into matrix form in **Appendix 2**.

- 751 • State Identity, Credential and Access Management (SICAM) Guidance and Roadmap –
 752 Strategic framework published by the National Association of State Chief Information
 753 Officers (NASCIO) to promote alignment with FICAM within state government.⁹
- 754 • AAMVA DL/ID Security Framework – Set of requirements, recommendations and standards
 755 maintained by the American Association of Motor Vehicle Administrators (AAMVA) for use
 756 by Motor Vehicle Administrations to ensure driver’s license and identification security.
- 757 • eHealth Exchange Data Use & Reciprocal Support Agreement (DURSA) – Trust framework
 758 established to support the exchange health information and messaging within eHealth
 759 Exchange, the Nationwide Health Information Network.
- 760 • InCommon Trust Framework – Trust framework designed to facilitate authentication and
 761 identity management for students, faculty, staff and other service providers for institutions
 762 of higher education.
- 763 • Kantara Initiative Trust Framework – Trust framework developed on a for-profit,
 764 subscription basis to enable secure, identity-based, online interactions in a secure
 765 environment.
- 766 • Open Identity Exchange (OIX)/OITF Model – Set of guidelines and recommended
 767 mechanisms (Level of Assurance Assurance Model and Level of Protection) for developing
 768 and implementing an Identity Trust Framework for secure, confidence-based exchange of
 769 information (Global).

Comment [JG9]: Reference the fact that IMSAC explored global models via OIX and IDESG. (N. Moe) Reference EU standards. (D. Burhop)

⁹ 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=a0Gt0000000XNYG

773 Appendix 1. IMSAC Charter

774
775
776
777
778

COMMONWEALTH OF VIRGINIA
IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL
CHARTER

779 **Advisory Council Responsibilities (§ 2.2-437.A; § 2.2-436.A)**780
781
782
783
784

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

785
786
787
788
789
790
791

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

792
793**Membership and Governance Structure (§ 2.2-437.B)**

794

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

795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812

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

813
814

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

817
818 The statutory authority and requirements for public notice and comment periods for guidance
819 documents have been established pursuant to § 2.2-437.C, as follows:

820
821 C. Proposed guidance documents and general opportunity for oral or written submittals as to
822 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published
823 in the Virginia Register of Regulations as a general notice following the processes and
824 procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§
825 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written
826 comments following the posting and publication and shall hold at least one meeting dedicated
827 to the receipt of oral comment no less than 15 days after the posting and publication. The
828 Advisory Council shall also develop methods for the identification and notification of interested
829 parties and specific means of seeking input from interested persons and groups. The Advisory
830 Council shall send a copy of such notices, comments, and other background material relative to
831 the development of the recommended guidance documents to the Joint Commission on
832 Administrative Rules.

833
834
835 This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the
836 minutes of the meeting and related IMSAC documents, visit:
837 <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
Trust Framework (TF) Comparison Matrix	<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 & ParticipantMember 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 ParticipantMembers • Representations & Warranties • Grant of Authority • Dispute Resolution • Authorizations for Data Requests by ParticipantMember • Open Disclosure & Anti-Circumvention • Confidential ParticipantPerson 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 ParticipantMembers • 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 ParticipantMembers (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) + <u>Governance Authority</u> & 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 <u>Participant Person</u> 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 <u>ParticipantMembers</u> (\$6.6) + Duty of response by <u>ParticipantMembers</u> (\$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 <u>ParticipantMembers</u> (\$6.8) + Glossary of TF terms/definitions (\$1.4) + Component-based approach for different <u>ParticipantMember</u> types (\$6.6)

Comment [JG10]: Add subsection references (J. Grubbs)

Comment [JG11]: SICAM references remain at the section level since most provisions covered across subsections.

Comment [JG12]: Does NASCIO offer SICAM certification? (D. Burhop; N. Moe)

Comment [JG13]: Confirm with N. Moe following NASCIO conference

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 ParticipantPerson 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 ParticipantMembers (§12) + Duty of response by ParticipantMembers (§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 ParticipantMember (horizontal/vertical) (ParticipantMember types defined in §1; expectations in §12.02; duties in §13) + Glossary of TF terms/definitions (§1) + Component-based approach for different ParticipantMember 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; ParticipantMembers) 	<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 Participant 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 ParticipantMembers (PA §6, §7) + Duty of response by ParticipantMembers (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 ParticipantMembers (horizontal/vertical) (ParticipantMember types defined in Join §1, ParticipantMembers) + Glossary of TF terms/definitions (InCommon Website) + Component-based approach for different ParticipantMember types (ParticipantMembers)

ICPOP=InCommon **ParticipantMember** 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 ParticipantMember + Open disclosure & anti-circumvention (Other agreements in KTR MTAU) + Confidential Participant 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 ParticipantMembers (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 & ParticipantMember 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 ParticipantMembers (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 ParticipantMembers (horizontal/vertical) (OITF §II, §III.C, §IV) + High-level definitions (OITF §I) + Component-based approach for different ParticipantMember 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)