# COMMONWEALTH OF VIRGINIA


## Information Technology Resource Management (ITRM)

### GUIDANCE DOCUMENT
### Trust Frameworks

### Virginia Information Technologies Agency (VITA)

# Table of Contents

# 1 Publication Version Control

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

| Version | Date | Revision Description |
|---|---|---|
| 1.0 | 05/02/2016 | Initial Draft of Document |
| | | |
| | | |
| | | |

# 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 will be reviewed by IMSAC during a council workshop, May 2, 2016.

- The document will be reviewed in a manner compliant with §2.2-437.C, *Code of Virginia*:

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

# 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 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://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-225

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

### 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://lis.virginia.gov/cgi-bin/legp604.exe?000+cod+2.2-2007

### Virginia Information Technologies Agency
§ 2.2-2010. Additional powers of VITA
http://lis.virginia.gov/cgi-bin/legp604.exe?000+cod+2.2-2010

# 4 Definitions

Terms used in this document align with adopted definitions in the National Institute of Standards and Technology Special Publication 800-63-2 (NIST SP 800-63-2), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf. 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. In very limited circumstances, an Army Post Office box number, Fleet Post Office box number or the street address of next of kin or of another contact individual can be used when a residential street address for the individual is not available. |
| 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.<br>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.<br>In this document, 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 | 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.<br>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.” |
| 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 | 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.<br>Cookies are used for many purposes and may be assertions or may contain pointers to assertions. See Section 9.1.1 for more information. |
| Credential | An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber.<br>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. |
| 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) | 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.<br>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. |
| 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. See Appendix A. |
| Extensible Mark-up 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 | Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to |

| | |
|---|---|
| Management Act (FISMA) | 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 (FIPS) | Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and 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.<br>FIPS documents are available online through the FIPS home page: http://www.nist.gov/itl/fips.cfm |
| Federated Identity | The means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems. |
| Governance Entity | The legal entity responsible for providing policy level leadership, oversight, strategic direction and related governance activities within a trust-based identity management system. |
| Guessing Entropy | A measure of the difficulty that an Attacker has to guess the average password used in a system. In this document, 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. See Appendix A. |
| 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:<br>1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and<br>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 or 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.<br>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.<br><br>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. In this document, 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). See Appendix A. |
| Multi-Factor | A characteristic of an authentication system or a token that uses more than one authentication factor.<br>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 Entity | The legal entity responsible for operations, maintenance, management and related functions within a trust-based identity management system. |
| Participant | A participating member of a trust framework for a trust-based identity management 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. (For more discussion, see Section 7.1.1.) |
| 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.<br>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.<br>In this document, all unverified names are assumed to be pseudonyms. |
| Public Credentials | Credentials that describe the binding in a way that does not compromise the token. (For more discussion, see Section 7.1.1.) |
| 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. See also [RFC 5280]. |
| 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.<br>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 | The ability to collect publically available information on individuals and engineering it in a way that enables discovery of passwords, PINs, and other identity secrets. Also, the act of deceiving an individual into revealing sensitive information by associating with the individual to gain confidence and trust. |
| 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. (For more discussion, see Section 7.1.1.) |
| 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" (§ 59.1-550). Trust frameworks consist of multiparty agreements among Participants in an identity management system, which enforce requirements and ensure trust in the acceptance of identity credentials. |
| Unverified Name | A Subscriber 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 | A Subscriber 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 than can be modified without invalidating the credential. (For more discussion, see Section 7.1.1.) |
| 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. |

# 5 Background

The following guidance document has been developed by the Virginia Information Technologies Agency (VITA), acting on behalf of the Secretary of Technology and Chief Information Officer of the Commonwealth, at the direction of the Identity Management Standards Advisory Council (IMSAC). IMSAC was created by the General Assembly of the Commonwealth of Virginia in 2015 and advises the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to §2.2-436. A copy of the IMSAC Charter has been provided in **Appendix 1**.

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 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.

## Purpose Statement

The purpose of this document is to establish minimum specifications for operational trust frameworks to enable and support a trust-based identity management system. The document assumes that the identity management system's trust framework will be compliant with Applicable Law.[1]

The document limits its focus to operational trust frameworks for identity management systems. Minimum specifications for other components of an identity management system will be defined in separate IMSAC guidance documents in this series, pursuant to §2.2-436 and §2.2-437.

The document defines minimum requirements, components, and related provisions for operational trust frameworks. The document assumes that specific trust frameworks will address the business, legal and technical requirements for each distinct identity management system, and that these requirements will be designed based on the specific level of assurance model supported by the system.



[1] For the purpose of this guidance document, the term "Applicable Law" shall mean laws, statutes, regulations and rules of the jurisdiction in which the Participants of a trust-based identity management system operates.

# 6 Minimum Specifications

The Commonwealth of Virginia's Electronic Identity Management Act defines "trust framework" as "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" (§ 59.1-550). Trust frameworks consist of multiparty agreements among Participants in an identity management system, which enforce requirements and ensure trust in the acceptance of identity credentials.

This document establishes minimum specifications for trust frameworks for identity management systems. Trust frameworks should be designed to document the business, legal, and technical components for enterprise architecture, business processes, governance models, operational policies and practices, and Participant obligations within the system. Trust frameworks also should contain the requirements for meeting the Levels of Assurance supported by the system.[2] Subsequent guidance documents in the IMSAC series will address other components of an identity management system, pursuant to §2.2-436 and §2.2-437.

## Trust Framework Components

The following section outlines the minimum specifications for the business, legal and technical components of a standard trust framework for an identity management system. These components have been identified through a rigorous assessment of existing operational trust frameworks in the identity ecosystem and other domains, as outlined in Section 7 of this report. The components also align with the Identity Ecosystem Framework (IDEF), adopted by the Identity Ecosystem Steering Group in October 2015.[3]

## Business Components

- Limitations on Use of Data: Collection, maintenance, and use of a person's identity information solely for the purpose for which it was collected.
- Governing Body & Change Processes: Governance model for the trust framework built on a transparent, clearly defined structure and change-management process.
- Operating Policies & Procedures: Policies and procedures for the operations and maintenance of the trust framework's operational entity.

[2] The term "Level of Assurance" has been used in this document to describe the continuum for the degree of certainty in the user's identity established within the identity management system. The term aligns with the levels defined for federal agencies in the U.S. Office of Management and Budget Memorandum M04-04 and NIST SP 800-63-2 (i.e., Levels 1-4) but provides for a more general framework to accommodate other identity management standards and protocols.

[3] 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.

- Security, Privacy & Confidentiality (Business): Compliant business processes and documentation for notifying a person of the security, privacy, and confidentiality provisions in the trust framework and for gaining consent from the person for using identity information.
- Suspension & Termination (Voluntary & Involuntary): Provisions for suspending or terminating a Participant due to failure to meet the obligations in the agreement, or the Participant's self-suspension or termination of participation in the identity management system.
- Data Elements & Data Classification: Attribute-level documentation and classification for person identity information used within the identity management system to assess the level of sensitivity in the data.
- Expectations of Performance: Provisions in the trust framework that clearly state the performance and service criteria for all Participants.
- Use Cases (Exchange & Participant Types): Documented examples for Participant roles and responsibilities and data flows across the identity management system.

## Legal Components

- Definition/Identification of "Applicable Law": Provisions requiring Participants to comply with all governing laws, statutes, rules, and regulations of the jurisdiction in which each Participant operates.
- Legal Agreements for Exchange Structure: Statement of requirements for the architecture, performance, and service specifications, and Participant obligations for the operation and maintenance of the exchange of person identity information.
- Security, Privacy & Consent Provisions (Legal): Terms and conditions establishing Participant obligations for the collection, operational use, and maintenance of person identity information and for gaining consent from the person for using identity information.
- Assignment of Liability & Risk for Participants: Articles that define how liability and risk within the identity management system will be distributed among Participants, with indemnification provisions for violation of the agreement.
- Representations & Warranties: Statements of factual principles in the trust framework upon which Participants 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 in the trust framework to assign to the governing entity decision-making authority over the identity management system.
- Dispute Resolution: Statement of requirements and processes for mediation and the resolution of disputes among Participants in the identity management system in a manner that avoids adjudicative procedures.
- Authorizations for Data Requests by Participant: Articles defining role-based rules, requirements, and processes for Participants 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 trust framework, and prohibiting the circumvention of technical protections within the identity management system for the handling of person identity information.
- Confidential Participant Information: Statements documenting the business, legal and technical requirements for the handling of confidential person identity information.
- Audit, Accountability & Compliance: Terms of conditions documenting and requiring Participants to comply with audit procedures, and the consequences of Participants failing to comply with the audit findings and corrective action plan to address deficiencies.

## Technical Components

- Performance & Service Specifications: Architecture and infrastructure specifications, protocols, and requirements covering full end-to-end integration for the identity management system, including technical, solutions, and information architecture.
- Security, Privacy & Confidentiality: Architecture and infrastructure specifications, protocols, and requirements within the identity management system designed for the collection, operational use, and maintenance of person identity information and for gaining consent from the person for using 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 information within the identity management system.
- System Access (ID/Authentication): Standards-based, open architecture processes, protocols, and requirements for Participant authentication and access to the identity management system.
- Provisions for Future Use of Data: Terms and conditions defining limitations on, and permitted purposes for, the use of person identity information after the information has been used for the Registration event and the issuance of a credential by a Credential Service Provider.
- Duty of Response by Participants: Terms and conditions requiring Participant information systems to respond to and process messaging requests – inbound and outbound – within the identity management system, normally establishing the time in which the Participant system must respond and process the request.
- Onboarding, Testing & Certification Requirements: Documented processes, protocols, specifications, and requirements for onboarding, testing, and certifying prospective Participants in the identity management system.
- 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 compliance with governing external standards for the identity management system, including standards for information processing, e-authentication, and authorization.

# 7 Alignment Comparison

The minimum specifications for trust frameworks established in this document have been developed based on a detailed comparison analysis of trust frameworks and related governance models currently operational in the identity management ecosystem. Specifically, the minimum specifications build upon core components of existing trust frameworks while adapting or extending them to meet the requirements of IMSAC, pursuant to §2.2-436-§2.2-437. This document assumes that each trust framework developed or modified to meet these minimum specifications will comply with Applicable Law.

The following operational trust frameworks were evaluated by IMSAC. Results from the alignment comparison analysis have been compiled into matrix form in **Appendix 2**.

- State Identity, Credential and Access Management (SICAM) Guidance and Roadmap – Strategic framework published by the National Association of State Chief Information Officers (NASCIO) to promote alignment with FICAM within state government.[4]
- AAMVA DL/ID Security Framework – Set of requirements, recommendations and standards maintained by the American Association of Motor Vehicle Administrators (AAMVA) for use by Motor Vehicle Administrations to ensure driver's license and identification security.
- eHealth Exchange Data Use & Reciprocal Support Agreement (DURSA) – Trust framework established to support the exchange health information and messaging within eHealth Exchange, the Nationwide Health Information Network.
- InCommon Trust Framework – Trust framework designed to facilitate authentication and identity management for students, faculty, staff and other service providers for institutions of higher education.
- Kantara Initiative Trust Framework – Trust framework developed on a for-profit, subscription basis to enable secure, identity-based, online interactions in a secure environment.
- Open Identity Exchange (OIX)/OITF Model – Set of guidelines and recommended mechanisms (Level of Assurance and Level of Protection) for developing and implementing a trust framework for secure, confidence-based exchange of information.



[4] 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

# Appendix 1. IMSAC Charter

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Appendix 2. IMSAC Charter

| | Trust Framework (TF) Components for IMSAC | | | |
|---|---|---|---|---|
| | **Business** | **Legal** | **Technical** | **Other** |
| **Trust Framework (TF) Comparison Matrix** | • Limitations on Use of Data ("Permitted Purpose")<br>• Governing Body & Change Processes<br>• Operating Policies & Procedures<br>• Security, Privacy & Confidentiality-Business: Consent/Auth.)<br>• Suspension & Termination (Voluntary & Involuntary)<br>• Data Elements & Data Classification (Attribute Level/Person Identity Information)<br>• Expectations of Performance<br>• Use Cases (Exchange & Participant Types) | • Definition/Identification of "Applicable Law"<br>• Legal Agreements for Exchange Structure<br>• Security, Privacy & Consent Provisions<br>• Assignment of Liability & Risk for Participants<br>• Representations & Warranties<br>• Grant of Authority<br>• Dispute Resolution<br>• Authorizations for Data Requests by Participant<br>• Open Disclosure & Anti-Circumvention<br>• Confidential Participant Information<br>• Audit, Accountability & Compliance | • Performance & Service Specifications<br>• Security, Privacy & Confidentiality (Technical: Infrastructure/ Architecture)<br>• Breach Notification<br>• System Access (ID/Authentication)<br>• Provisions for Future Use of Data<br>• Duty of Response by Participants<br>• Onboarding, Testing & Certification Requirements<br>• Handling of Test Data v. Production Data<br>• Compliance Governing Standards | • Openness & Transparency<br>• TF Lifecycle Management ("Living Agreement")<br>• Support & Capacity Building (IGs)<br>• Scalability to Support Array of Participants (Horizontal/Vertical)<br>• Glossary of TF Terms/Definitions<br>• Component-based Approach for TF Elements |

| Trust Framework Comparison Analysis | Alignment (+) with Core Components for IMSAC | | | |
|---|---|---|---|---|
| | **Business** | **Legal** | **Technical** | **Other** |
| **State Identity, Credential and Access Management (SICAM) Guidance and Roadmap** | + Limitations on Use of Data (§6.6)<br>+ Governing body & change processes (§6.6)<br>+ Operating policies & procedures (§6.6)<br>+ Security, privacy & confidentiality (§6.6)<br>+ Suspension & termination (§6.6)<br>+ Data elements & data classification (attribute level/PII) (§5.5, §6.5, §6.6)<br>+ Expectations of performance (§6.6) | + Compliance w/ applicable law (§6.6)<br>+ Legal agreements for exchange structure (§6.6)<br>+ Security, privacy & consent (§6.6)<br>+ Liability (§6.6)<br>+ Representations & warranties (§6.6)<br>+ Grant of authority (§6.6)<br>+ Dispute resolution (§6.6)<br>+ Authorizations for data exchange (§6.6)<br>+ Non-exclusivity (§6.6)<br>+ Confidential Participant information (§6.6, §6.3)<br>+ Audit (§6.6)<br>+ Accountability & compliance (§6.9) | + Performance & service specifications (§5, §6.4)<br>+ Security, privacy & confidentiality (§5, §6.4)<br>+ Breach notification (§5, §6.4; §6.6)<br>+ System access (§6.6)<br>+ Provisions for future use of data/services (§6)<br>+ Expectations of Participants (§6.6)<br>+ Duty of response by Participants (§6.6)<br>+ Onboarding, testing & certification (§6.6)<br>+ Compliance with governing standards (§5, §6.6) | + Openness & transparency (§6.6)<br>+ TF lifecycle management (§6.6)<br>+ Scalability to support array of Participants (§6.8)<br>+ Glossary of TF terms/definitions (§1.4)<br>+ Component-based approach for different Participant types (§6.6) |

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

| Trust Framework Comparison Analysis | Alignment (+) with Core Components for IMSAC | | | |
|---|---|---|---|---|
| | **Business** | **Legal** | **Technical** | **Other** |
| **AAMVA DL/ID Security Framework** | + Data element-level verification and validation (§1.3 #9, §1.4 #10, §1.4 #13, §3.3.4, §7.4, Appdx.)<br>+ Data (Name) collection, use and maintenance (§3.3.4, § 7.1, Appdx.)<br>+ AAMVA DL/ID Personal ID Card Design Specification (§1.4 #12, §3.3.4, 7.3, Appdx.)<br>+ Procedures for initial customer ID and validation (§3.3.3, §6.0)<br>+ Record & document use, permitted purpose (§3.3.5, §4.6, §7.1, §8.0)<br>+ Benefits/ business drivers (§2.0, §3.1)<br>+ Business-driven agreement among MVAs (§3.1, §3.3, §4.5)<br>+ Business requirements for P&Ps, document issuing systems, and internal controls, Driver License Agreement (DLA) (§3.3.1, §4.2, §4.5, Appdx.) | + 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.)<br>+ Enforcement thru business requirements (§2.0, §3.1, §4.5)<br>+ Audit plan (§1.1 #2, §1.2 #5, §3.3.2, §5.1, Appdx.)<br>+ Compliance and oversight, internal controls (§3.3.2, §4.4, §5.2)<br>+ Risk assessment & management (§1.1 #3, §3.3.5, § 4.2, §4.4, §8.0)<br>+ Privacy (§1.1 #4, §4.2, Appdx., §3.3.4, §3.3.5, §4.5, §4.6, §7.1, §7.4, §8.3)<br>+ Common set of verifiable resources (§1.3 #8, §3.3.3, §6.2, Appdx.)<br>+ Machine-Readable Technology (MRT) (§3.3.5, §8.2, Appdx.)<br>+ Restrictions, minimum penalties and sanctions (§3.3.5, §8.1, Appdx.) | + Electronic verification (w/issuing entity) of DL/ID data elements (§1.3 #9, §3.3.3, §6.3)<br>+ Standards for MVA system integrity, interoperability & reciprocity (§2.0, §3.1, §3.3.2, §4.2, §4.5)<br>+ Compliance with governing standards (§3.3.2, §4.5, §5.2)<br>+ System integrity, security & privacy (§4.6) | + Compliance and implementation support thru FDR employee training (§1.1 #1, §3.3.1, §4.1)<br>+ Common definition of "residency" (§1.3 #6, §3.3.3) tied to DL/ID verification (§1.3 #7, §3.3.3, §6.1)<br>+ "End of stay" on immigration doc. as expiration date for DL/ID - data element derivation (§1.4 #11, §3.3.4, §7.2, Appdx.)<br>+ Horizontal scalability thru reciprocity (§3.1)<br>+ Openness enforced thru privacy provisions (§4.6, §7.1)<br>+ Limits on disclosure enforced thru privacy provisions (§4.6, 7.1)<br>+ Glossary of abbreviations/ acronyms (§9.0)<br>+ 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)** | + Limitations on use of data (§1.jj; §3; §5.01-5.03)<br>+ Governing body (§4) & change processes (§10.03; §11.03)<br>+ Operating policies & procedures (§11; Appdx.; change process in §11.03)<br>+ Security, privacy & confidentiality (§7; §8; §14)<br>+ Suspension & termination ( §19)<br>+ Data elements & data classification (attribute level/PII) (§1.v; §1.w; §1.kk)<br>+ Expectations of performance (§12) | + Definition/compliance w/ applicable law (§1.a; §15.11; §23.01; Appdx.)<br>+ Legal agreements for exchange structure (recitals; §1.ee; §3.01; §23.07)<br>+ Security, privacy & consent (§14)<br>+ Liability (§18)<br>+ Representations & warranties (§15; disclaimers in §17)<br>+ Grant of authority (§4.03)<br>+ Dispute resolution (§21; Appdx.)<br>+ Authorizations for data exchange (§12; §13)<br>+ Open disclosure & anti-circumvention (§15; §23.04; §23.07)<br>+ Confidential Participant information (§16)<br>+ Audit (§9)<br>+ Accountability & compliance (§10.01; 11.01; §15.03; §15.06) | + Performance & service specifications (§10; Appdx.; change process in §10.03)<br>+ Security, privacy & confidentiality (§7; §8; §14)<br>+ Breach notification (§14.03)<br>+ System access (§6)<br>+ Provisions for future use of data (§5.02)<br>+ Expectations of Participants (§12)<br>+ Duty of response by Participants (§13)<br>+ Onboarding, testing & certification (§10.01)<br>+ Handling of test data v. production data (§15.07) | + Openness & transparency (overview; recitals)<br>+ TF lifecycle management ("living agreement") (overview; §4; §10.03; §11.03)<br>+ Scalability to support array of Participants (horizontal/vertical) (Participant types defined in §1; expectations in §12.02; duties in §13)<br>+ Glossary of TF terms/definitions (§1)<br>+ Component-based approach for different Participant 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** | + Limitations on use of data (ICPOP; IAS; limits on use of ID information in PA §9)<br>+ Governing body & change processes (ICPOP; PA §17)<br>+ Operating policies & procedures (ICPOP)<br>+ Security, privacy & confidentiality (PA §6, §9; ICPOP)<br>+ Suspension & termination (PA §5.b, §5.c)<br>+ Data elements & data classification (attribute level/PII) (IAS; PA §6.b)<br>+ Expectations of performance (PA §6, §7)<br>+ Use cases and examples (InCommon Website; ICBP; Participants) | + Definition/compliance w/ applicable law (PA §15)<br>+ Legal agreements for exchange structure (ICPP; PA §6, §7.b)<br>+ Security, privacy & consent (PA §6, §9)<br>+ Liability (PA §11, includes disclaimer & limitations)<br>+ Representations & warranties (addressed in PA §7.b)<br>+ Grant of authority to executive (PA §18)<br>+ Dispute resolution process (PA §10; ICBL §5)<br>+ Authorizations for data exchange (PA §18)<br>+ Open disclosure & anti-circumvention (PA §14, §16)<br>+ Confidential Participant information (PA §8, §9)<br>+ Audit (ICPOP)<br>+ Accountability & compliance (PA §15) | + Performance & service specifications (PA §6, §7)<br>+ Security, privacy & confidentiality (ICPOP)<br>+ Breach notification (PA and addenda; ICPOP)<br>+ System access (ICPOP)<br>+ Provisions for future use of data (ICPOP)<br>+ Expectations of Participants (PA §6, §7)<br>+ Duty of response by Participants (PA §6, §7)<br>+ Onboarding, testing & certification (ICPOP)<br>+ Handling of test data v. production data (ICPOP) | + Openness & transparency (ICBP)<br>+ TF lifecycle management (“living agreement”) (ICBL; PA §17)<br>+ Implementation support (ICPOP)<br>+ Scalability to support array of Participants (horizontal/vertical) (Participant types defined in Join §1, Participants)<br>+ Glossary of TF terms/definitions (InCommon Website)<br>+ Component-based approach for different Participant types (Participants) |

ICPOP=InCommon Participant 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** | + Limitations on use of data (KTR MTAU)<br>+ Governing body (BL §4; OP §2) & change/ amendment processes (BL §12; OP §9; MA §3)<br>+ Operating policies & procedures (OP)<br>+ Security, privacy & confidentiality (AP; MA)<br>+ Suspension & termination (MA §2; BL §8.11; KTR MTAU)<br>+ Data elements & data classification (KTR; KIC)<br>+ Expectations of performance (AP; KTR MTAU; KIC)<br>+ Use cases (Working groups for business cases-trusted federations) | + Definition/identification of applicable law (KTR MTAU; see also "Governing law and jurisdiction" provision in KTR MTAU)<br>+ Legal agreement for exchange structure (MA)<br>+ Security, privacy & consent provisions<br>+ Liability (KTR MTAU)<br>+ Warranty (KTR MTAU)<br>+ Grant of authority (MA)<br>+ Authorizations for data requests by Participant<br>+ Open disclosure & anti-circumvention (Other agreements in KTR MTAU)<br>+ Confidential Participant information (Options set in IPRP; IPRP Art. 3)<br>+ Accountability & compliance (w/ antitrust laws in BL §17; MA) | + Performance & service specifications (AP; KTR/KTV; KTR MTAU; KIC; Member protection & treatment in IPRP)<br>+ Security, privacy & confidentiality (AP; MA)<br>+ Technical certification & testing (AP; KIC)<br>+ Standards for technical & operational interoperability (KTR; MA goal #3; #7; KIC) | + Open & transparent governance model (MA goals #3, #4; op; BL §3)<br>+ TF lifecycle management (MA goals #4, #6)<br>+ Support & capacity building (IGs)<br>+ Scalability to support array of Participants (horizontal/vertical) (member types BL §8)<br>+ 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** | + Limitations on use of data (OITF §III.B, §III.C, §V)<br>+ Governing body & change processes (OIX; OITF §III.C)<br>+ Operating policies & procedures (OIX; OITF §II, §III.B, §III.C)<br>+ Security, privacy & confidentiality (OIX; OITF §III.A, §V)<br>+ Suspension & termination (OITF §III.C)<br>+ Data elements & data classification (attribute level/PII) (OIX; OITF §III.A, §III.B)<br>+ Expectations of performance (OIX; OITF §II, §III.C)<br>+ Use cases for agreement, transaction & Participant types (OITF §I, §III; OIX) | + Compliance w/ applicable law (OIX; OITF §V)<br>+ Legal agreements for exchange structure (OIX; OITF §II, §III.C)<br>+ Security, privacy & consent (OIX; OITF §III.A)<br>+ Liability, representations & warranties (OITF §III.C)<br>+ Grant of authority (OIX; OITF §III.C)<br>+ Dispute resolution (OITF §II, §III.C, §V)<br>+ Authorizations for data exchange (OIX; OITF §III.A)<br>+ Anti-circumvention & open disclosure (OITF §V)<br>+ Audit (OIX; OITF §II, §III.B, §V)<br>+ Accountability & compliance (OIX; OITF §II, §V) | + Performance & service specifications (OIX; OITF §II, §III.A, §III.B)<br>+ Security, privacy & confidentiality (OIX; OITF §III.A; §V)<br>+ Expectations of Participants (OIX; OITF §III.A, §III.B, §III.C)<br>+ Onboarding, testing & certification (OIX; OITF §II, §III.B) | + Openness & transparency (OIX; OITF §I; statement in OITF §V, §VI)<br>+ TF lifecycle management (OIX; OITF §II)<br>+ Scalability to support array of Participants (horizontal/vertical) (OITF §II, §III.C, §IV)<br>+ High-level definitions (OITF §I)<br>+ Component-based approach for different Participant types (OIX; OITF §II, §III.C)<br>+ 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)