COMMONWEALTH OF VIRGINIA

IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

GUIDANCE DOCUMENT 5
Certification of Trust Framework Operators

Table of Contents

1 Publication Version Control

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

Publication Version	Date	Revision Description
1.0	10/24/2017	Initial Draft of Document

2 Reviews

- The initial version of the document was prepared by staff from the Virginia Information Technologies Agency (VITA) at the direction of the Identity Management Standards Advisory Council (IMSAC).

3 Purpose and Scope

Pursuant to §§ 2.2-436 and 2.2-437, this guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to establish minimum specifications for digital identity systems so as to warrant liability protection pursuant to the Electronic Identity Management Act ("the Act"), §§ 59.1-550 to -555. This guidance document was prepared to provide information or guidance of general applicability to the public for interpreting or implementing the Act. This guidance document was not developed as a Commonwealth of Virginia Information Technology Resource Management (ITRM) Policy, Standard, and Guideline, pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive branch agencies of the Commonwealth of Virginia.

4 Statutory Authority

The following section documents the statutory authority established in the Code of Virginia for the development of minimum specifications and standards for certification of identity trust framework operators, the process for certification, and requirements for certification authorities. References to statutes below and throughout this document shall be to the Code of Virginia, unless otherwise specified.

Governing Statutes:

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

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

Commonwealth Identity Management Standards
§ 2.2-436. Approval of electronic identity standards
http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/

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

5 Terminology and Definitions

The core terms used within the digital identity management domain may be assigned a wide range of definitions, depending on the context or community of interest. For the purpose of the IMSAC guidance document series, the terminology has been defined in the *IMSAC Reference Document: Terminology and Definitions*, which may be accessed at http://vita.virginia.gov/default.aspx?id=6442475952

The IMSAC terminology aligns with the definitions published in the following documents:

- National Institute of Standards and Technology Special Publication 800-63-3, available at https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3
- Electronic Identity Management Act (§ 59.1-550), available at http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550

6 Background

In 2015, the Virginia General Assembly passed the Electronic Identity Management Act (§§ 59.1-550 to -555) to address demand in the state's digital economy for secure, privacy enhancing digital authentication and identity management. Growing numbers of communities of interest have advocated for stronger, scalable and interoperable identity solutions to increase consumer protection and reduce liability for principal actors in the identity ecosystem – identity providers, credential service providers and relying parties.

To address the demand contemplated by the Electronic Identity Management Act, the General Assembly created the Identity Management Standards Advisory Council (IMSAC) to advise 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**.

IMSAC 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 to -555); 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

This guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to provide information or guidance of general applicability to the public for interpreting or implementing the Electronic Identity Management Act (the Act). Specifically, the document establishes criteria and recommended processes for certifying compliance with the Commonwealth's identity management minimum specifications and standards adopted pursuant to § 2.2-436.

The document provides a reference for criteria that must be met to certify compliance of identity trust framework operators. The document assumes a specific identity trust framework will address the business, legal, and technical requirements for each distinct digital identity system; these requirements will be designed based on the specific assurance model supported by the system; and the identity trust framework will be compliant with applicable laws, regulations, and statutes.

This guidance document focuses on certification, certification criteria, and requirements for certification authorities to qualify as eligible to perform certifications pursuant to the Act. Separate IMSAC guidance documents in this series define minimum specifications for other components of a digital identity system.

7 Certification of Identity Trust Framework Operators

The Electronic Identity Management Act limits the liability of identity trust framework operators who comply with the Commonwealth's identity management minimum specifications and standards adopted pursuant to § 2.2-436, who meet applicable contractual obligations, and who comply with rules established under the governing trust framework.[1] Furthermore, an identity trust framework operator's compliance with the Commonwealth's identity management minimum specifications and standards affects the public's trust in the identity trust framework itself. Thus, an identity trust framework operator's compliance with the Commonwealth's identity management specifications and standards is of vital importance.

In light of the foregoing, each identity trust framework operator shall demonstrate compliance with the Commonwealth's identity management specifications and standards to an independent, third-party certification authority. Certification authorities have become an integral part of the global identity ecosystem. They provide objective, consistent, auditable compliance reviews based on clearly defined certification criteria. This enables identity trust framework operators to fully document compliance – based on an independent review – with the Commonwealth's identity management minimum specifications and standards. The resulting certification acts as an affirmative statement of compliance for the certified identity trust framework operator.

IMSAC has designed this guidance document to serve as a reference for criteria that must be met to certify compliance of identity trust framework operators. The certification criteria stated herein should be used as a summary checklist of, not a replacement for, the Commonwealth's identity management minimum specifications and standards. The document assumes a specific identity trust framework will address the business, legal, and technical requirements for each distinct digital identity system; these requirements will be designed based on the specific assurance model supported by the system; and the identity trust framework will be compliant with applicable laws, regulations, and statutes.

Certification Criteria

The following components of an identity trust framework have been established as minimum specifications and standards defined in *IMSAC Guidance Document 2: Identity Trust Frameworks*. The certification of identity trust framework operators shall be based on these certification criteria.

[1] *See* Va. Code § 59.1-552.B.

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.

- Governance Authority & Change Processes: Governance model for the identity trust framework built on a transparent, clearly defined structure and change-management process.

- Operating Policies & Procedures: Policies and procedures for the operations, maintenance, and business continuity of the identity trust framework's operational authority, and across the digital identity system.

- Security, Privacy & Confidentiality (Business): Compliant business processes and documentation for notifying a person of the security, privacy, and confidentiality provisions in the identity trust framework and for gaining consent from the person for using identity information.

- Suspension & Termination (Voluntary & Involuntary): Provisions for suspending or terminating a member due to failure to meet the obligations in the agreement, or the member's self-suspension or termination of participation in the identity trust framework.

- Data Elements & Data Classification: Attribute-level documentation, classification, and labeling of the person identity information used within the identity trust framework to support compliant handling of the data through the entire data lifecycle.

- Expectations of Performance: Provisions in the identity trust framework that set the performance and service criteria for all members – IdPs, CSPs, and RPs – including requirements for breach response and resolution, system(s) interruption or failure, and other risk situations.

- Use Cases (Exchange & Member Types): Documented examples for roles and responsibilities of members of the identity trust framework and data flows across the digital identity system.

Legal Components

- Definition/Identification of Applicable Law: Provisions requiring members of the identity trust framework to comply with all governing laws, statutes, rules, and regulations of the jurisdiction in which each member operates.

- Legal Agreements for Exchange Structure: Statement of requirements for the architecture, performance, and service specifications, and member obligations for the operation and maintenance of the exchange of person identity information within the identity trust framework.

- Security, Privacy & Consent Provisions (Legal): Terms and conditions establishing member obligations for the collection, labeling, operational use, and maintenance of person identity information and for gaining consent from the person for using identity information.

- Assignment of Liability & Risk for Members: Articles that define how liability and risk within the identity trust framework will be distributed among members, with indemnification provisions for violation of the agreement.

- Representations & Warranties: Statements of factual principles in the identity trust framework upon which 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 members of the identity trust framework to assign to the Governance Authority decision-making authority over the identity trust framework.

- Dispute Resolution: Statement of requirements and processes for mediation and the resolution of disputes among members in the identity trust framework in a manner that avoids adjudicative procedures.

- Authorizations for Data Requests by Members: Articles defining role-based rules, requirements, and processes for members of the identity trust framework 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 digital identity system for the handling of person identity information.

- Confidential Person Information: Statements documenting the business, legal and technical requirements for the classification, labeling and handling of confidential person identity information.

- Audit, Accountability & Compliance: Terms of conditions documenting and requiring members of the identity trust framework to comply with audit procedures, and the consequences of members 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 for all members covering full end-to-end integration for the digital identity system supported by the 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 trust framework designed for the collection, labeling, 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, and related risk situations, within the identity trust framework.

- System Access: Standards-based, open architecture processes, protocols, and requirements for member authentication and access to the 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 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 Members: Terms and conditions requiring identity trust framework member systems to respond to and process messaging requests – inbound and outbound – within the digital identity system, normally establishing the time in which the member system must respond and process the request.

- Onboarding, Testing & Certification Requirements: Documented processes, protocols, specifications, and requirements for onboarding, testing, and certifying prospective member systems in the 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 member compliance with governing external standards for the identity trust framework, including standards for information processing, Electronic Authentication, and Authorization.

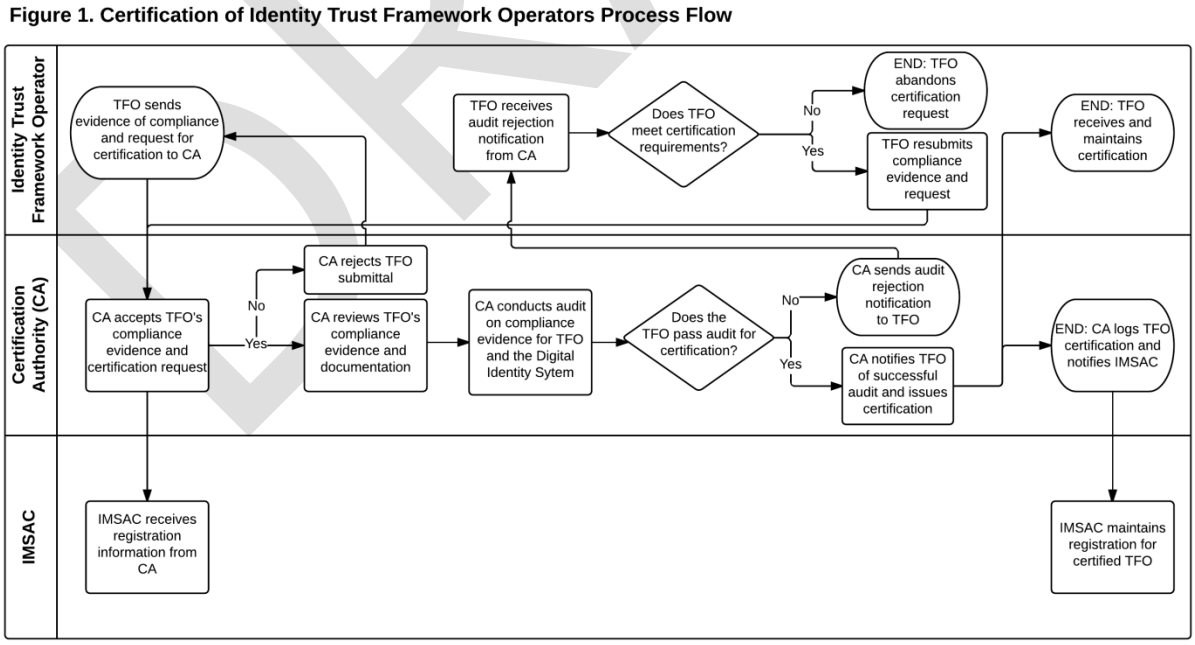
8 Certification Process and Requirements

Certification Process Model

The Electronic Identity Management Act does not specify how identity trust framework operators seeking a limitation of liability may demonstrate compliance with adopted minimum specifications and standards. IMSAC considered a range of process models for identity trust framework operators to demonstrate compliance with the Commonwealth's identity management specifications and standards. Ultimately, IMSAC selected a process model that leveraged existing certification authorities in the global identity ecosystem and allows identity trust framework operators to select a certification authority most appropriate for their line of business, domain, or level of governance.

The process model provided in this guidance document requires an identity trust framework operator to choose from eligible certification authorities. Eligibility requirements for certification authorities are stated below in this document. IMSAC shall maintain and publish on the VITA website a list of eligible certification authorities. Once the identity trust framework operator has chosen an eligible certification authority, the identity trust framework operator shall demonstrate compliance with the Commonwealth's identity management specifications and standards based on the certification criteria defined in this guidance document and in *IMSAC Guidance Document 2: Identity Trust Frameworks*. A process flow diagram for certification of trust framework operators has been provided in **Figure 1**.

Figure 1. Process Flow Model for Certification of Trust Framework Operators



Requirements for Certification Authorities

In addition to the functional requirements listed below, the certification authority must be a legal entity with the requisite standing to perform certifications of compliance of identity trust framework operators within the Commonwealth of Virginia.[2]

The certification authority must ensure, through pre-and post-certification activities, that identity trust framework operators, and the digital identity systems they oversee, comply with the certification criteria stated in this guidance document, the minimum specifications and standards adopted pursuant to § 2.2-436, and all other provisions of the Act.

Certification authorities must meet the following functional requirements:

1. Establish a clearly defined, transparent, and compliant process for granting, suspending, or terminating certification of identity trust framework operators
2. Analyze evidence of compliance submitted by identity trust framework operators to inform a determination of certification
3. Perform audits on, or review qualified audit reports submitted by, identity trust framework operators to grant, suspend, or terminate the certification status
4. Grant, suspend, or terminate the certification status of identity trust framework operators, based on the result of pre- or post-certification audits
5. Cooperate with jurisdictional authorities with legal, regulatory, or security oversight of identity trust framework operators by notifying them of the certification status
6. Notify IMSAC of decisions to grant, suspend, or terminate the certification status of identity trust framework operators
7. Require identity trust framework operators to remedy any failure to comply with the Commonwealth's identity management minimum specifications and standards
8. Cooperate with other certification authorities, as appropriate, and provide them with assistance in meeting the requirements for certification authorities established in this guidance document
9. Inform Commonwealth Security of the Virginia Information Technologies Agency, IMSAC, other jurisdictional authorities, other certification authorities, and the general public of breaches of security or loss of integrity in a certified identity trust framework operator, the digital identity system, or members of the identity trust framework
10. Submit an annual report, on or before December 31 of each year, to IMSAC describing the certification authority's main activities performed during the calendar year

[2] The requirements for certification authorities have been specified to align with Chapter 3, Section 2. Supervision, of Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014.

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.