COMMONWEALTH OF VIRGINIA

IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

GUIDANCE DOCUMENT 7
Trustmarks for Digital Identity Management

Table of Contents

1 Publication Version Control 1
2 Reviews 1
3 Purpose and Scope 2
4 Statutory Authority 3
5 Terminology and Definitions 4
6 Background 5
7 Minimum Specifications and Standards 6

1 Publication Version Control

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

Publication Version	Date	Revision Description
1.0	08/28/2016	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 trustmarks in digital identity systems. 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 minimum specifications and standards for trustmarks in digital identity systems, pursuant to the Act.

The minimum specifications and standards defined in this document have been developed to align with international standards, specifically Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014. Reference also has been given to the trustmark framework and governance model developed by the Georgia Tech Research Institute (GTRI) during its pilot project under the National Strategy for Trusted Identities in Cyberspace (NSTIC).

The document assumes an identity trust framework will address the business, legal, and technical requirements for each distinct digital identity system. The document focuses on trustmarks for identity trust framework operators and digital identity systems. Separate IMSAC guidance documents in this series define minimum specifications for other components of a digital identity system.

7 Minimum Specifications

The Electronic Identity Management Act extends a limitation of liability to identity trust framework operators and identity providers who comply with the minimum specifications and standards adopted pursuant to the Act, who meet applicable contractual obligations, and who comply with rules established under the governing trust framework, as follows:

> § 59.1-552.B. An identity trust framework operator or identity provider shall not be liable if the issuance of the identity credential or assignment of an identity attribute or a trustmark was in compliance with (i) the Commonwealth's identity management standards in place at the time of issuance or assignment, (ii) applicable terms of any contractual agreement with a contracting party, and (iii) any written rules and policies of the identity trust framework of which it is a member, provided such identity trust framework operator or identity provider did not commit an act or omission that constitutes gross negligence or willful misconduct. An identity trust framework operator or identity provider shall not be liable for misuse of an identity credential by the identity credential holder or by any other person who misuses an identity credential.

A primary mechanism anticipated by the Act for establishing the verified status of an identity credential, an identity trust framework, or a component of an identity trust framework, is the trustmark. The Act defines a trustmark as "a machine-readable official seal, authentication feature, certification, license, or logo that may be provided by an identity trust framework operator to certified identity providers within its identity trust framework to signify that the identity provider complies with the written rules and policies of the identity trust framework."

Furthermore, § 59.1-551 establishes a warranty on trustmarks: "The use of a trustmark on an identity credential provides a warranty by the identity provider that the written rules and policies of the identity trust framework of which it is a member have been adhered to in asserting the identity and any related attributes contained on the identity credential. No other warranties are applicable unless expressly provided by the identity provider."

IMSAC has defined the following minimum specifications and standards for trustmarks in digital identity systems. These align with Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014:

1. An indication, at least in a form suitable for automated processing, that the trustmark has been issued as a qualified trustmark;
2. A set of data unambiguously representing the qualified identity trust framework operator issuing the qualified trustmark and, for a person's identity credential, the name and, where applicable, identification number as stated in the official records;
3. The title of the identity trust framework operator that issued the trustmark;
4. Validation data for the trustmark, which corresponds to the trustmark creation data;

5. Documentation of the duration – beginning and end – of the trustmark's period of validity;
6. The trustmark's identifier, or identification code, which must be unique for the qualified identity trust framework operator;
7. The digital signature or digital certification of the identity trust framework operator that issued the trustmark;
8. The location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point;
9. The host of the digital services that can be used to enquire as to the validity status of the trustmark;
10. where the trustmark creation data related to the validation data is located in a trustmark creation device, an appropriate indication of this, at least in a form suitable for automated, machine readable processing.

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.