

1  
2  
3  
4  
5  
6  
7

# COMMONWEALTH OF VIRGINIA



8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

## IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

### GUIDANCE DOCUMENT 6 Certification of Trust Framework Operators

25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35

## 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	Certification of Identity Trust Framework Operators .....	6
8	Certification Process and Requirements .....	10

DRAFT

## 36 **1 Publication Version Control**

---

37

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

39

<b>Publication Version</b>	<b>Date</b>	<b>Revision Description</b>
1.0	08/28/2016	Initial Draft of Document

40

## 41 **2 Reviews**

---

42

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

46

### 47 **3 Purpose and Scope**

---

48

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

58

DRAFT

## 59 **4 Statutory Authority**

---

60

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

66

### 67 **Governing Statutes:**

68

#### 69 **Secretary of Technology**

70 **§ 2.2-225. Position established; agencies for which responsible; additional powers**

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

72

#### 73 **Identity Management Standards Advisory Council**

74 **§ 2.2-437. Identity Management Standards Advisory Council**

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

76

#### 77 **Commonwealth Identity Management Standards**

78 **§ 2.2-436. Approval of electronic identity standards**

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

80

#### 81 **Electronic Identity Management Act**

82 **Chapter 50. Electronic Identity Management Act**

83 <http://law.lis.virginia.gov/vacode/title59.1/chapter50/>

84

85

86

87

88

89

## 90 **5 Terminology and Definitions**

---

91

92 The core terms used within the digital identity management domain may be assigned a wide  
93 range of definitions, depending on the context or community of interest. For the purpose of  
94 the IMSAC guidance document series, the terminology has been defined in the *IMSAC*

95 *Reference Document: Terminology and Definitions*, which may be accessed at

96 <http://vita.virginia.gov/default.aspx?id=6442475952>

97

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

99 • National Institute of Standards and Technology Special Publication 800-63-3, available at

100 <https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3>

101 • Electronic Identity Management Act (§ 59.1-550), available at

102 <http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550>

103

## 104 **6 Background**

---

105

106 In 2015, the Virginia General Assembly passed the Electronic Identity Management Act  
107 (§§ 59.1-550 to -555) to address demand in the state’s digital economy for secure, privacy  
108 enhancing digital authentication and identity management. Growing numbers of communities  
109 of interest have advocated for stronger, scalable and interoperable identity solutions to  
110 increase consumer protection and reduce liability for principal actors in the identity ecosystem  
111 – identity providers, credential service providers and relying parties.

112

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

118

119 IMSAC recommends to the Secretary of Technology guidance documents relating to  
120 (i) nationally recognized technical and data standards regarding the verification and  
121 authentication of identity in digital and online transactions; (ii) the minimum specifications and  
122 standards that should be included in an identity trust framework, as defined in § 59.1-550, so as  
123 to warrant liability protection pursuant to the Electronic Identity Management Act (§§ 59.1-550  
124 to -555); and (iii) any other related data standards or specifications concerning reliance by third  
125 parties on identity credentials, as defined in § 59.1-550.

126

### 127 **Purpose Statement**

128

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

135

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

142

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

## 147 **7 Certification of Identity Trust Framework Operators**

---

148  
149 The Electronic Identity Management Act limits the liability of identity trust framework  
150 operators who comply with the Commonwealth’s identity management minimum specifications  
151 and standards adopted pursuant to § 2.2-436, who meet applicable contractual obligations, and  
152 who comply with rules established under the governing trust framework.<sup>1</sup> Furthermore, an  
153 identity trust framework operator’s compliance with the Commonwealth’s identity  
154 management minimum specifications and standards affects the public’s trust in the identity  
155 trust framework itself. Thus, an identity trust framework operator’s compliance with the  
156 Commonwealth’s identity management specifications and standards is of vital importance.

157  
158 In light of the foregoing, each identity trust framework operator shall demonstrate compliance  
159 with the Commonwealth’s identity management specifications and standards to an  
160 independent, third-party certification authority. Certification authorities have become an  
161 integral part of the global identity ecosystem. They provide objective, consistent, auditable  
162 compliance reviews based on clearly defined certification criteria. This enables identity trust  
163 framework operators to fully document compliance – based on an independent review – with  
164 the Commonwealth’s identity management minimum specifications and standards. The  
165 resulting certification acts as an affirmative statement of compliance for the certified identity  
166 trust framework operator.

167  
168 IMSAC has designed this guidance document to serve as a reference for criteria that must be  
169 met to certify compliance of identity trust framework operators. The certification criteria  
170 stated herein should be used as a summary checklist of, not a replacement for, the  
171 Commonwealth’s identity management minimum specifications and standards. The document  
172 assumes a specific identity trust framework will address the business, legal, and technical  
173 requirements for each distinct digital identity system; these requirements will be designed  
174 based on the specific assurance model supported by the system; and the identity trust  
175 framework will be compliant with applicable laws, regulations, and statutes.

### 176 177 **Certification Criteria**

178  
179 The following components of an identity trust framework have been established as minimum  
180 specifications and standards defined in *IMSAC Guidance Document 2: Identity Trust*  
181 *Frameworks*. The certification of identity trust framework operators shall be based on these  
182 certification criteria.

183  
184

---

<sup>1</sup> See Va. Code § 59.1-552.B.



## 185 Business Components

186

187  Limitations on Use of Data: Collection, maintenance, and use of a person's identity  
188 information solely for the purpose for which it was collected.

189

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

193

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

197

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

202

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

207

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

211

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

216

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

220

## 221 Legal Components

222

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

226

- 227       Legal Agreements for Exchange Structure: Statement of requirements for the  
228      architecture, performance, and service specifications, and member obligations for the  
229      operation and maintenance of the exchange of person identity information within the  
230      identity trust framework.  
231
- 232       Security, Privacy & Consent Provisions (Legal): Terms and conditions establishing  
233      member obligations for the collection, labeling, operational use, and maintenance of  
234      person identity information and for gaining consent from the person for using identity  
235      information.  
236
- 237       Assignment of Liability & Risk for Members: Articles that define how liability and risk  
238      within the identity trust framework will be distributed among members, with  
239      indemnification provisions for violation of the agreement.  
240
- 241       Representations & Warranties: Statements of factual principles in the identity trust  
242      framework upon which members may rely, and assurances of the implied  
243      indemnification obligation in the event the principles are violated or proven false.  
244
- 245       Grant of Authority: Provisions requiring members of the identity trust framework to  
246      assign to the Governance Authority decision-making authority over the identity trust  
247      framework.  
248
- 249       Dispute Resolution: Statement of requirements and processes for mediation and the  
250      resolution of disputes among members in the identity trust framework in a manner that  
251      avoids adjudicative procedures.  
252
- 253       Authorizations for Data Requests by Members: Articles defining role-based rules,  
254      requirements, and processes for members of the identity trust framework to access  
255      person identity information.  
256
- 257       Open Disclosure & Anti-Circumvention: Provisions requiring transparency in the rules,  
258      policies, and practices for operations and governance of the identity trust framework,  
259      and prohibiting the circumvention of technical protections within the digital identity  
260      system for the handling of person identity information.  
261
- 262       Confidential Person Information: Statements documenting the business, legal and  
263      technical requirements for the classification, labeling and handling of confidential  
264      person identity information.  
265
- 266       Audit, Accountability & Compliance: Terms of conditions documenting and requiring  
267      members of the identity trust framework to comply with audit procedures, and the  
268      consequences of members failing to comply with the audit findings and corrective  
269      action plan to address deficiencies.

## 270 Technical Components

271

272  Performance & Service Specifications: Architecture and infrastructure specifications,  
273 protocols, and requirements for all members covering full end-to-end integration for the  
274 digital identity system supported by the identity trust framework, including technical,  
275 solutions, and information architecture.

276

277  Security, Privacy & Confidentiality: Architecture and infrastructure specifications,  
278 protocols, and requirements within the digital identity system supported by the identity  
279 trust framework designed for the collection, labeling, operational use, and maintenance  
280 of person identity information and for gaining consent from the person for using  
281 identity information.

282

283  Breach Notification: Processes, protocols, and requirements compliant with applicable  
284 law for notifying the appropriate authorities in the event of a breach of person identity  
285 information, and related risk situations, within the identity trust framework.

286

287  System Access: Standards-based, open architecture processes, protocols, and  
288 requirements for member authentication and access to the digital identity system  
289 supported by the identity trust framework.

290

291  Provisions for Future Use of Data: Terms and conditions defining limitations on, and  
292 permitted purposes for, the use of person identity information after the information has  
293 been used for the Registration event and the issuance of a credential by a credential  
294 service provider.

295

296  Duty of Response by Members: Terms and conditions requiring identity trust framework  
297 member systems to respond to and process messaging requests – inbound and  
298 outbound – within the digital identity system, normally establishing the time in which  
299 the member system must respond and process the request.

300

301  Onboarding, Testing & Certification Requirements: Documented processes, protocols,  
302 specifications, and requirements for onboarding, testing, and certifying prospective  
303 member systems in the identity trust framework.

304

305  Handling of Test Data v. Production Data: Terms and conditions compliant with  
306 applicable law preventing the use of production data in a test environment.

307

308  Compliance with Governing Standards: Terms and conditions identifying and stating  
309 requirements for member compliance with governing external standards for the identity  
310 trust framework, including standards for information processing, Electronic  
311 Authentication, and Authorization.

312

## 313 8 Certification Process and Requirements

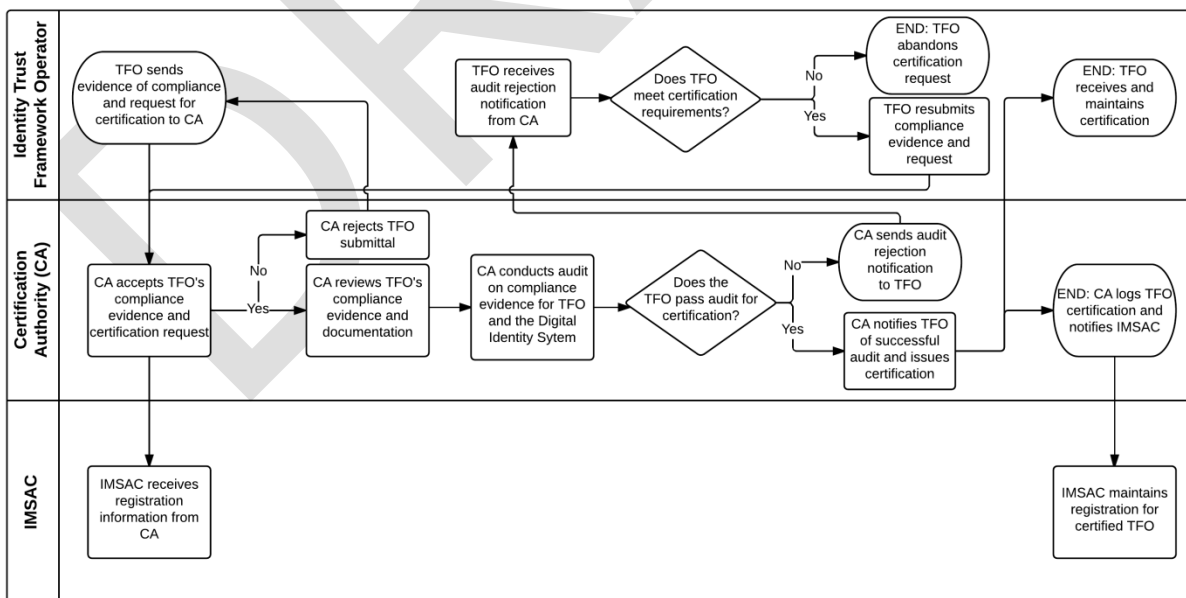
### 314 Certification Process Model

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

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

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

333 **Figure 1. Certification of Identity Trust Framework Operators Process Flow**



337  
338

## 339 Requirements for Certification Authorities

340

341 In addition to the functional requirements listed below, the certification authority must be a  
342 legal entity with the requisite standing to perform certifications of compliance of identity trust  
343 framework operators within the Commonwealth of Virginia.<sup>2</sup>

344

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

349

350 Certification authorities must meet the following functional requirements:

351

352 1. Establish a clearly defined, transparent, and compliant process for granting, suspending,  
353 or terminating certification of identity trust framework operators

354 2. Analyze evidence of compliance submitted by identity trust framework operators to  
355 inform a determination of certification

356 3. Perform audits on, or review qualified audit reports submitted by, identity trust  
357 framework operators to grant, suspend, or terminate the certification status

358 4. Grant, suspend, or terminate the certification status of identity trust framework  
359 operators, based on the result of pre- or post-certification audits

360 5. Cooperate with jurisdictional authorities with legal, regulatory, or security oversight of  
361 identity trust framework operators by notifying them of the certification status

362 6. Notify IMSAC of decisions to grant, suspend, or terminate the certification status of  
363 identity trust framework operators

364 7. Require identity trust framework operators to remedy any failure to comply with the  
365 Commonwealth's identity management minimum specifications and standards

366 8. Cooperate with other certification authorities, as appropriate, and provide them with  
367 assistance in meeting the requirements for certification authorities established in this  
368 guidance document

369 9. Inform Commonwealth Security of the Virginia Information Technologies Agency,  
370 IMSAC, other jurisdictional authorities, other certification authorities, and the general  
371 public of breaches of security or loss of integrity in a certified identity trust framework  
372 operator, the digital identity system, or members of the identity trust framework

373 10. Submit an annual report, on or before December 31 of each year, to IMSAC describing  
374 the certification authority's main activities performed during the calendar year

375

376

377

---

<sup>2</sup> 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.

## 378 Appendix 1. IMSAC Charter

379

380

### COMMONWEALTH OF VIRGINIA

381

### IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL

382

### CHARTER

383

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

385

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

389

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

397

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

399

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

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

408

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

410

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

413

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

416

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

418

419

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

422

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

425

426 C. Proposed guidance documents and general opportunity for oral or written submittals as to  
427 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published  
428 in the Virginia Register of Regulations as a general notice following the processes and  
429 procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§  
430 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written  
431 comments following the posting and publication and shall hold at least one meeting dedicated  
432 to the receipt of oral comment no less than 15 days after the posting and publication. The  
433 Advisory Council shall also develop methods for the identification and notification of interested  
434 parties and specific means of seeking input from interested persons and groups. The Advisory  
435 Council shall send a copy of such notices, comments, and other background material relative to  
436 the development of the recommended guidance documents to the Joint Commission on  
437 Administrative Rules.

438

439

440 This charter was adopted by the Advisory Council at its meeting on December 7, 2015.