

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 5 Certification of Identity 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

Publication Version	Date	Revision Description
1.0	10/24/2017	Initial draft of Guidance Document
1.0	07/16/2018	Document revised by staff based on public comment

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 • The document was revised based on public comment received in verbal form during the 30-  
47 day comment period, pursuant to § 2.2-437.C. IMSAC allowed at least 30 days for the  
48 submission of written comments following the posting and publication and held a meeting  
49 dedicated to the receipt of oral comment on June 30, more than 15 days after the posting  
50 and publication.

51

52

### 53 **3 Purpose and Scope**

---

54

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

64

DRAFT

## 65 **4 Statutory Authority**

---

66

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

72

### 73 **Governing Statutes:**

74

#### 75 **Secretary of Technology**

76 **§ 2.2-225. Position established; agencies for which responsible; additional powers**

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

78

#### 79 **Identity Management Standards Advisory Council**

80 **§ 2.2-437. Identity Management Standards Advisory Council**

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

82

#### 83 **Commonwealth Identity Management Standards**

84 **§ 2.2-436. Approval of electronic identity standards**

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

86

#### 87 **Electronic Identity Management Act**

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

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

90

91

92

93

94

95

## 96 **5 Terminology and Definitions**

---

97

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

103

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

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

109

## 110 6 Background

---

111  
112 In 2015, the Virginia General Assembly passed the Electronic Identity Management Act  
113 (§§ 59.1-550 to -555) to address demand in the state’s digital economy for secure, privacy  
114 enhancing digital authentication and identity management. Growing numbers of communities  
115 of interest have advocated for stronger, scalable and interoperable identity solutions to  
116 increase consumer protection and reduce liability for principal actors in the identity ecosystem  
117 – identity providers, credential service providers and relying parties.

118  
119 To address the demand contemplated by the Electronic Identity Management Act, the General  
120 Assembly created the Identity Management Standards Advisory Council (IMSAC) to advise the  
121 Secretary of Technology on the adoption of identity management standards and the creation of  
122 guidance documents pursuant to § 2.2-436. A copy of the IMSAC Charter has been provided in  
123 **Appendix 1.**

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

### 132 133 **Purpose Statement**

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

141  
142 The document provides ~~a~~ reference ~~for~~ criteria that must be met to certify compliance of  
143 identity trust framework operators. The document assumes ~~a specific~~ identity trust frameworks  
144 will address the business, legal, and technical requirements for each distinct digital identity  
145 system; ~~these such~~ requirements will be designed based on the specific assurance model  
146 supported by the system; and the identity trust framework will be compliant with applicable  
147 laws, regulations, and statutes.

148  
149 This guidance document focuses on certification, certification criteria, and requirements for  
150 certification authorities to qualify as eligible to perform certifications pursuant to the Act.  
151 Separate IMSAC guidance documents in this series define minimum specifications for other  
152 components of a digital identity system.

## 7 Certification of Identity Trust Framework Operators

---

153  
154  
155 The Electronic Identity Management Act limits the liability of identity trust framework  
156 operators who comply with the Commonwealth’s identity management minimum specifications  
157 and standards adopted pursuant to § 2.2-436, who meet applicable contractual obligations, and  
158 who comply with rules established under the governing trust framework.<sup>1</sup> Furthermore, an  
159 identity trust framework operator’s compliance with the Commonwealth’s identity  
160 management minimum specifications and standards affects the public’s trust in the identity  
161 trust framework itself. Thus, an identity trust framework operator’s compliance with the  
162 Commonwealth’s identity management specifications and standards is of vital importance.  
163

164 In light of the foregoing, [and in order to seek liability protection pursuant to the Act](#), each  
165 identity trust framework operator ~~shall~~ [will need to](#) demonstrate compliance with the  
166 Commonwealth’s identity management specifications and standards ~~to through~~ an  
167 independent, third-party certification authority. Certification authorities have become an  
168 integral part of the global identity ecosystem. They provide objective, consistent, auditable  
169 compliance reviews based on clearly defined certification criteria. This enables identity trust  
170 framework operators to fully document compliance – based on an independent review – with  
171 the Commonwealth’s identity management minimum specifications and standards. The  
172 resulting certification acts as an affirmative statement of compliance for the certified identity  
173 trust framework operator.  
174

175 IMSAC has designed this guidance document to ~~serve as a~~ [provide](#) reference ~~for~~ criteria that  
176 must be met to certify compliance of identity trust framework operators. The certification  
177 criteria stated herein should be used as a summary checklist of, not a replacement for, the  
178 Commonwealth’s identity management minimum specifications and standards. The document  
179 assumes ~~a specific~~ identity trust framework~~s~~ will address the business, legal, and technical  
180 requirements for each distinct digital identity system; ~~these~~ [such](#) requirements will be designed  
181 based on the specific assurance model supported by the system; and the identity trust  
182 framework will be compliant with applicable laws, regulations, and statutes.  
183

### Certification Criteria

184  
185  
186 The following components of an identity trust framework have been established as minimum  
187 specifications and standards defined in *IMSAC Guidance Document 2: Identity Trust*  
188 *Frameworks*. The certification of identity trust framework operators shall be based on these  
189 certification criteria.  
190  
191

---

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

192 Business Components

193

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

196

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

200

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

204

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

209

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

214

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

218

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

223

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

227

228 Legal Components

229

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

233

- 234       Legal Agreements for Exchange Structure: Statement of requirements for the  
235      architecture, performance, and service specifications, and member obligations for the  
236      operation and maintenance of the exchange of person identity information within the  
237      identity trust framework.  
238
- 239       Security, Privacy & Consent Provisions (Legal): Terms and conditions establishing  
240      member obligations for the collection, labeling, operational use, and maintenance of  
241      person identity information and for gaining consent from the person for using identity  
242      information.  
243
- 244       Assignment of Liability & Risk for Members: Articles that define how liability and risk  
245      within the identity trust framework will be distributed among members, with  
246      indemnification provisions for violation of the agreement.  
247
- 248       Representations & Warranties: Statements of factual principles in the identity trust  
249      framework upon which members may rely, and assurances of the implied  
250      indemnification obligation in the event the principles are violated or proven false.  
251
- 252       Grant of Authority: Provisions requiring members of the identity trust framework to  
253      assign to the Governance Authority decision-making authority over the identity trust  
254      framework.  
255
- 256       Dispute Resolution: Statement of requirements and processes for mediation and the  
257      resolution of disputes among members in the identity trust framework in a manner that  
258      avoids adjudicative procedures.  
259
- 260       Authorizations for Data Requests by Members: Articles defining role-based rules,  
261      requirements, and processes for members of the identity trust framework to access  
262      person identity information.  
263
- 264       Open Disclosure & Anti-Circumvention: Provisions requiring transparency in the rules,  
265      policies, and practices for operations and governance of the identity trust framework,  
266      and prohibiting the circumvention of technical protections within the digital identity  
267      system for the handling of person identity information.  
268
- 269       Confidential Person Information: Statements documenting the business, legal and  
270      technical requirements for the classification, labeling and handling of confidential  
271      person identity information.  
272
- 273       Audit, Accountability & Compliance: Terms of conditions documenting and requiring  
274      members of the identity trust framework to comply with audit procedures, and the  
275      consequences of members failing to comply with the audit findings and corrective  
276      action plan to address deficiencies.

277 Technical Components

278

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

283

284  Security, Privacy & Confidentiality: Architecture and infrastructure specifications,  
285 protocols, and requirements within the digital identity system supported by the identity  
286 trust framework designed for the collection, labeling, operational use, and maintenance  
287 of person identity information and for gaining consent from the person for using  
288 identity information.

289

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

293

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

297

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

302

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

307

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

311

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

314

315  Compliance with Governing Standards: Terms and conditions identifying and stating  
316 requirements for member compliance with governing external standards for the identity  
317 trust framework, including standards for information processing, Electronic  
318 Authentication, and Authorization.

319

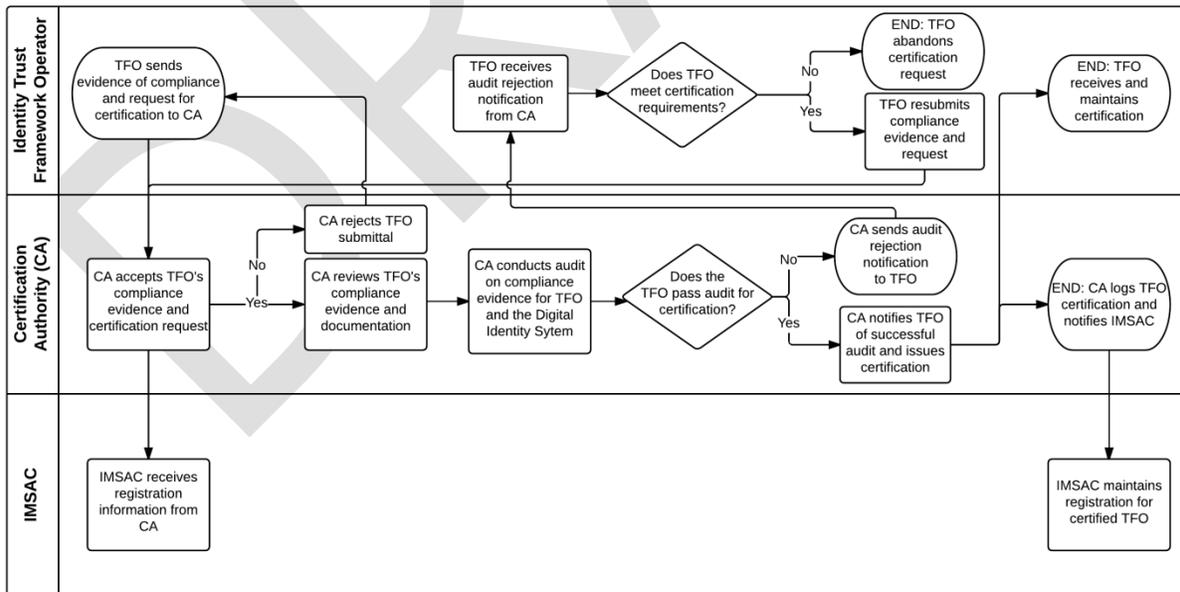
## 320 8 Certification Process and Requirements

### 321 Certification Process Model

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

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

Figure 1. Certification of Identity Trust Framework Operators Process Flow



343  
344

## 345 Requirements for Certification Authorities

346

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

350

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

355

356 Certification authorities must meet the following functional requirements:

357

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

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

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

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

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

368 6. Notify [IMSAC, Commonwealth Security of the Virginia Information Technologies Agency,](#)  
369 [IMSAC, other jurisdictional authorities](#) of decisions to grant, suspend, or terminate the  
370 certification status of identity trust framework operators

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

373 8. Cooperate with other certification authorities, as appropriate, and provide them with  
374 assistance in meeting the requirements for certification authorities established in this  
375 guidance document

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

380 10. Submit an annual report, on or before December 31 of each year, to [IMSAC](#)  
381 [Commonwealth Security of the Virginia Information Technologies Agency, IMSAC, other](#)  
382 [jurisdictional authorities](#) describing the certification authority's main activities  
383 performed during the calendar year

384

385

---

<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.

## 386 Appendix 1. IMSAC Charter

387

388

**COMMONWEALTH OF VIRGINIA**

389

**IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL**

390

**CHARTER**

391

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

393

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

397

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

405

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

407

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

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

416

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

418

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

421

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

424

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

426

427

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

430

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

433

434 C. Proposed guidance documents and general opportunity for oral or written submittals as to  
435 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published  
436 in the Virginia Register of Regulations as a general notice following the processes and  
437 procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§  
438 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written  
439 comments following the posting and publication and shall hold at least one meeting dedicated  
440 to the receipt of oral comment no less than 15 days after the posting and publication. The  
441 Advisory Council shall also develop methods for the identification and notification of interested  
442 parties and specific means of seeking input from interested persons and groups. The Advisory  
443 Council shall send a copy of such notices, comments, and other background material relative to  
444 the development of the recommended guidance documents to the Joint Commission on  
445 Administrative Rules.

446

447

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