

1 Document #:
2 Status: Draft
3 Version: 0.1

4

5 SunSpec Cybersecurity Certification

6 Phase 1 Test Suite

7

8

9

10

11



12

13

14

15

16

17

18

19

20 **Abstract**

21 TBD.

23 Copyright © SunSpec Alliance 2022. All Rights Reserved.

24 All other copyrights and trademarks are the property of their respective owners.

25 **License Agreement and Copyright Notice**

26 This document and the information contained herein is provided on an "AS IS" basis and the
27 SunSpec Alliance DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT
28 NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL
29 NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF
30 MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

31

32 This document may be used, copied, and furnished to others, without restrictions of any kind,
33 provided that this document itself may not be modified in anyway, except as needed by the
34 SunSpec Technical Committee and as governed by the SunSpec IPR Policy. The complete
35 policy of the SunSpec Alliance can be found at sunspec.org.

36

37 Prepared by the SunSpec Alliance

38 4040 Moorpark Avenue, Suite 110

39 San Jose, CA 95117

40

41

42 Website: sunspec.org

43 Email: info@sunspec.org

45 **About the SunSpec Alliance**

46 The SunSpec Alliance is a trade alliance of developers, manufacturers, operators, and service
47 providers together pursuing open information standards for the distributed energy industry.
48 SunSpec standards address most operational aspects of PV, storage, and other distributed
49 energy power plants on the smart grid, including residential, commercial, and utility-scale
50 systems, thus reducing cost, promoting innovation, and accelerating industry growth.

51 Over 100 organizations are members of the SunSpec Alliance, including global leaders from
52 Asia, Europe, and North America. Membership is open to corporations, non-profits, and
53 individuals. For more information about the SunSpec Alliance, or to download SunSpec
54 specifications at no charge, visit sunspec.org.

55 **About the SunSpec Specification Process**

56 SunSpec Alliance specifications are initiated by SunSpec members to establish an industry
57 standard for mutual benefit. Any SunSpec member can propose a technical work item. Given
58 sufficient interest and time to participate, and barring significant objections, a workgroup is
59 formed and its charter is approved by the board of directors. The workgroup meets regularly to
60 advance the agenda of the team.

61 The output of the workgroup is generally in the form of a SunSpec Interoperability Specification.
62 These documents are considered to be normative, meaning that there is a matter of
63 conformance required to support interoperability. The revision and associated process of
64 managing these documents is tightly controlled. Other documents are informative, or make
65 some recommendation with regard to best practices, but are not a matter of conformance.
66 Informative documents can be revised more freely and more frequently to improve the quality
67 and quantity of information provided.

68 SunSpec Interoperability Specifications follow a lifecycle pattern of: DRAFT, TEST,
69 APPROVED, and SUPERSEDED.

70 For more information or to download a SunSpec Alliance specification, go to
71 <https://sunspec.org/about-sunspec-specifications/>.

72

73

74 **Revision History**

Version	Date	Comments
0.1	22-11-23	Initial draft based on Lumian contribution

75 Contents

76	Revision History.....	7
77	Contents	8
78	1 Scope.....	10
79	2 References.....	11
80	3 Definitions and abbreviations.....	12
81	3.1 Definitions	12
82	3.2 Abbreviations	12
83	4 Setup preambles.....	13
84	4.1 Operational states.....	13
85	4.1.1 DER/PRE/ST-01: Basic operational state	13
86	4.1.2 DER/PRE/ST-02: Factory default state	13
87	4.2 Required Equipment	13
88	5 Test cases.....	14
89	5.1 Software Update	14
90	5.1.1 DER/SWUP/BV-01: Updatable Software	14
91	5.1.2 DER/SWUP/BV-02: Support of Remote Updates	14
92	5.1.3 DER/SWUP/BV-03: Support of Automatic Updates.....	15
93	5.1.4 DER/SWUP/BV-04: Secure Updates	16
94	5.1.5 DER/SWUP/BV-05: Downgrade Prevention	16
95	5.2 Device Communication	17
96	5.2.1 DER/DCOM/BV-01: Support of Secure Communications.....	17
97	5.2.2 DER/DCOM/BV-02: Protocol Downgrade Prevention.....	18
98	5.2.3 DER/DCOM/BV-03: Deprecated Ciphersuites	19
99	5.3 Authentication	21
100	5.3.1 DER/AUTH/BV-01: Unique Credentials	21
101	5.3.2 DER/AUTH/BV-02: Authentication	22
102	5.3.3 DER/AUTH/BV-03: Session Timeout	22
103	5.3.4 DER/AUTH/BV-04: Configurable Timeout.....	23
104	5.3.5 DER/AUTH/BV-05: Strong Passwords.....	24
105	5.3.6 DER/AUTH/BV-06: Unique Passwords	25
106	5.3.7 DER/AUTH/BV-07: Brute Force Prevention.....	26
107	5.3.8 DER/AUTH/BV-08: Password Protection.....	26

108	5.4	Device Security	27
109	5.4.1	DER/DSEC/BV-01: Minimal Interfaces.....	27
110	5.4.2	DER/DSEC/BV-02: Factory Reset	28
111	5.5	Logging	28
112	5.5.1	DER/LOG/BV-01: Log Storage.....	28
113	5.5.2	DER/LOG/BV-02: Configuration Logs	29
114	5.5.3	DER/LOG/BV-03: Network Logs	30
115	5.5.4	DER/LOG/BV-04: Security Logs	30
116	5.5.5	DER/LOG/BV-05: Remote Logs.....	31
117	5.5.6	DER/LOG/BV-06: Log Retention.....	32
118	5.5.7	DER/LOG/BV-07: Incident Reporting	32
119	5.5.8	DER/LOG/BV-08: Power System Logs	33

120 **1 Scope**

121 TBD

122 2 References

- 123 [1] SunSec Alliance, SunSpec Cybersecurity Certification, Phase 1 Requirements,
124 Version 1.0, 2022. Available from
125 [https://docs.google.com/document/d/1IKLeOAYjgk_XdZw9eOGK603t850gRyijQjD2gE](https://docs.google.com/document/d/1IKLeOAYjgk_XdZw9eOGK603t850gRyijQjD2gEur8fo/)
126 [ur8fo/](https://docs.google.com/document/d/1IKLeOAYjgk_XdZw9eOGK603t850gRyijQjD2gEur8fo/)

127 **3 Definitions and abbreviations**

128 **3.1 Definitions**

129 For the purposes of the present document, the following terms and definitions apply:

130 None

131 **3.2 Abbreviations**

132 For the purposes of the present document, the following abbreviations apply:

133 AUTH Authentication

134 DCOM Device Communication

135 DER Distributed energy resource

136 ICS Implementation Conformance Statement

137 IUT Implementation under test

138 SWUP Software Update

139

140 **4 Setup preambles**

141 **4.1 Operational states**

142 **4.1.1 DER/PRE/ST-01: Basic operational state**

143 State of the IUT required to operate normally.

144 **4.1.2 DER/PRE/ST-02: Factory default state**

145 State of the IUT when it comes out of the box for the first time.

146 **4.2 Required Equipment**

- 147 • IUT (provided by manufacturer)
- 148 • Communication endpoints (provided by the manufacturer)
- 149 • Remote log server (provided by the manufacturer)
- 150 • Remote incident notification service (provided by the manufacturer)
- 151 • Secrets (keys, passwords, tokens, etc.) required to conduct tests (provided by the
152 manufacturer)
- 153 • Completed and signed ICS document (provided by the manufacturer)
- 154 • User or instruction manual for IUT (provided by the manufacturer)
- 155 • Network traffic monitor (provided by the test lab)
- 156 • USB tester (provided by the test lab)
- 157 • Wi-Fi scanner (provided by the test lab)

158 **5 Test cases**

159 **5.1 Software Update**

160 **5.1.1 DER/SWUP/BV-01: Updatable Software**

161 *Test Purpose*

162 Verify that the IUT supports updating mutable security and operational software functions.

163 *Obligation*

164 Mandatory

165 *Reference*

- 166 • DER/SWUP/REQ-01: Software Updates [1]

167 *Initial Condition*

- 168 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- 169 • A software update for mutable security and operational software functions is
- 170 available.
- 171 • Remote incident notification service is initialized and ready to receive reports from
- 172 IUT.

173 *Test Procedure*

- 174 1. The test engineer determines the software version of the currently installed security
- 175 and operational software functions.
- 176 2. The test engineer installs the software update on the IUT and records the time of
- 177 software update.
- 178 3. The test engineer determines the software version of the currently installed security
- 179 and operational software functions.

180 *Expected Outcome*

- 181 • The software versions of the security and operational software functions in step 3 are
- 182 higher than the versions in step 1.
- 183 • The IUT is operational.

184 *Remaining questions*

- 185 • How to determine which components IUT is able to update

186 **5.1.2 DER/SWUP/BV-02: Support of Remote Updates**

187 *Test Purpose*

188 Verify that the IUT supports remote updates.

189

190 *Obligation*

191 Mandatory

192 *Reference*

- 193 • DER/SWUP/REQ-02: Remote Updates [1]

194 *Initial Condition*

- 195 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- 196 • A remote update is available.
- 197 • Remote incident notification service is initialized and ready to receive reports from
- 198 IUT.

199 *Test Procedure*

- 200 1. The test engineer determines the software version of the currently installed software.
- 201 2. The test engineer executes a remote software update on the IUT and records the
- 202 time of update.
- 203 3. The test engineer determines the software version of the currently installed software.

204 *Expected Outcome*

- 205 • The software versions in step 3 are higher than the versions in step 1.
- 206 • The IUT is operational.

207 **5.1.3 DER/SWUP/BV-03: Support of Automatic Updates**

208 *Test Purpose*

209 Verify that the IUT supports automatic updates

210 *Obligation*

211 Mandatory

212 *Reference*

- 213 • DER/SWUP/REQ-03: Automatic Updates [1]

214 *Initial Condition*

- 215 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- 216 • A remote update is available.
- 217 • Remote incident notification service is initialized and ready to receive reports from
- 218 IUT.

219 *Test Procedure*

- 220 1. The test engineer determines the software version of the currently installed software.
- 221 2. The test engineer waits 24 hours.
- 222 3. The test engineer determines the software version of the currently installed software.

223

224 *Expected Outcome*

- 225 • The software versions in step 3 are higher than the versions in step 1.
- 226 • The IUT is operational.

227 **5.1.4 DER/SWUP/BV-04: Secure Updates**

228 *Test Purpose*

229 Verify that the IUT verifies the security of a software update before installing it.

230 *Obligation*

231 Mandatory

232 *Reference*

- 233 • DER/SWUP/REQ-04: Secure Updates [1]

234 *Initial Condition*

- 235 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- 236 • A first software update that is not authenticated is available.
- 237 • A second software update that has been modified by an unauthorized third party is
- 238 available.
- 239 • Remote incident notification service is initialized and ready to receive reports from
- 240 IUT.

241 *Test Procedure*

- 242 1. The test engineer determines the software version of the currently installed software.
- 243 2. The test engineer installs the first software update on the IUT and records the time.
- 244 3. The test engineer determines the software version of the currently installed software.
- 245 4. The test engineer installs the second software update on the IUT and records the
- 246 time..
- 247 5. The test engineer determines the software version of the currently installed software.

248 *Expected Outcome*

- 249 • The software versions in step 3 and 5 are the same as the versions in step 1.
- 250 • The IUT is operational.
- 251 • The Remote incident notification service recorded the security incidents in step 2 and
- 252 4.

253 **5.1.5 DER/SWUP/BV-05: Downgrade Prevention**

254 *Test Purpose*

255 Verify that the IUT rejects updates to software versions older than the currently installed

256 versions.

257 *Obligation*

258 Mandatory

259

260 *Reference*

- 261 • DER/SWUP/REQ-05: Downgrade Prevention [1]

262 *Initial Condition*

- 263 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- 264 • A first software update that is an older version of the first software update is
265 available.
- 266 • Remote incident notification service is initialized and ready to receive reports from
267 IUT.

268 *Test Procedure*

- 269 1. The test engineer determines the software version of the currently installed software.
- 270 2. The test engineer installs the first software update on the IUT and records the time.
- 271 3. The test engineer determines the software version of the currently installed software.

272 *Expected Outcome*

- 273 • The software versions in step 1 and 3 are the same.
- 274 • The IUT is operational.
- 275 • The Remote incident notification service recorded the security incidents in step 2.

276 **5.2 Device Communication**

277 **5.2.1 DER/DCOM/BV-01: Support of Secure Communications**

278 *Test Purpose*

279 Ensure all communication capabilities that can be used over the open Internet are properly
280 secured.

281 *Obligation*

282 Mandatory

283 *Reference*

- 284 • DER/DCOM/REQ-01: Secure Communications [1]
- 285 • ICS document

286 *Initial Condition*

- 287 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- 288 • Endpoints are in their basic operational state.
- 289 • Valid secrets required to authenticate communications are installed in IUT and
290 endpoints.

291

292 *Test Procedure*

293 For each of the communication capabilities listed in Section 1 of the ICS document, perform
294 the following test procedure:

- 295 1. Set up the IUT so it can activate the communication capability.
- 296 2. Set up the network monitor to use the protocol listed for the communication capability
297 in the ICS document (TLS, IPsec, or SSH).
- 298 3. Attach the network monitor so it can analyze the traffic between the device and
299 endpoint.
- 300 4. Activate the communication capability.
- 301 5. Observe the network traffic with the monitor.

302 *Expected Outcome*

- 303 • IUT is successfully using the protocol specified for each communication capability.

304 **5.2.2 DER/DCOM/BV-02: Protocol Downgrade Prevention**

305 *Test Purpose*

306 Ensure the IUT does not downgrade to unsecure protocols.

307 *Obligation*

308 Mandatory

309 *Reference*

- 310 • DER/DCOM/REQ-02: Downgrade Prevention [1]

311 *Initial Condition*

- 312 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- 313 • Endpoints are configured to request downgrade to the unapproved protocols listed in
314 Table X.

315 *Test Procedure*

316 For each of the communication capabilities listed in Section X of the ICS document, perform
317 the following test procedure:

- 318 1. Set up the IUT so it can activate the communication capability
- 319 2. For the first deprecated protocol listed in [Table 5-1](#) associated with the
320 communication capability's protocol, set up the endpoint so that it will request the
321 protocol to downgrade to this deprecated protocol.
- 322 3. Attach the network monitor so it can analyze the traffic between the device and
323 endpoint.
- 324 4. Activate the communication capability and record the time
- 325 5. Observe the network traffic with the monitor.
- 326 6. Go back to step 1 for the next deprecated protocol associated with the
327 communication capability's protocol. If there is no remaining deprecated protocol
328 associated with the communication capability in question, move to test the next
329 communication capability listed in the ICS document.

330

Table 5-1: Deprecated security protocols

Protocol	Deprecated Versions
TLS	SSL 1.0
TLS	SSL 2.0
TLS	SSL 3.0
TLS	TLS 1.0
TLS	TLS 1.1
IPSEC	IKEv1

331

332 *Expected Outcome*

- IUT rejects all connections.

334 5.2.3 DER/DCOM/BV-03: Deprecated Ciphersuites

335 *Test Purpose*

336 Ensure the IUT is only using approved ciphersuites.

337 *Obligation*

338 Excluded IF IUT only supports TLS 1.3 (observed from **DER/DCOM/BV-03**), otherwise
339 Mandatory

340 *Reference*

- DER/DCOM/REQ-03: Ciphersuites [1]
- [National Security Agency Eliminating Obsolete TLS Protocol Configurations](#)
- [IETF Deprecation of IKEv1 and obsoleted algorithms](#)

344 *Initial Condition*

- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- Endpoints for each communication capability are created and configured to accept only the ciphersuites listed in **Table X**.

348 *Test Procedure*

349 This test may be performed in conjunction with **DER/DCOM/BV-03** to save on IUT and
350 endpoint setup time. For each of the communication capabilities listed in Section 1 of the
351 ICS document, perform the following test procedure:

- 352 1. Set up the network monitor to use the protocol listed for the communication capability
353 in the ICS document (TLS, IPsec, or TLS).
- 354 2. Attach the network monitor so it can analyze the traffic between the device and
355 endpoint.

- 356 3. Activate the communication capability with the endpoint configured to support one of
 357 the ciphersuites listed in [Table 5-2](#) or [Table 5-3](#) (depending on the protocol) and
 358 record the time.
 359 4. Observe the network traffic with the monitor.
 360 5. Repeat steps 3 and 4 for each of the appropriate ciphersuites for the communication
 361 capability protocol.

362 Table 5-2: Deprecated TLS ciphersuites and key exchange algorithms, derived from NSA
 363 recommendations

Ciphersuite	Key Exchange
RC2	
RC4	
DES	
IDEA	
TDES/3ES	
	ANON
	EXPORT
	RSA < 1024 bits
	ECDHE with custom curves

364

365 Table 5-3: Deprecated IPSEC transforms, derived from IETF recommendations

Algorithm ID	Transform ID	Key Exchange
		IKEv1
ENCR_DES_IV64		
ENCR_DES		
ENCR_RC5		
ENCR_IDEA		
ENCR_CAST		
ENCR_BLOWFISH		
H		
ENCR_3IDEA		
ENCR_DES_IV32		
	PRF_HMAC_MD5	
	PRF_HMAC_TIGER	
	AUTH_HMAC_MD5_96	
	AUTH_DES_MAC	

Algorithm ID	Transform ID	Key Exchange
	AUTH_KPDK_MD5	
	AUTH_HMAC_MD5_128	
	AUTH_HMAC_SHA1_160	
	768-bit MODP Group	
	1024-bit MODP Group with 160-bit Prime Order Subgroup	

366

367 *Expected Outcome*

- 368
- IUT rejects each connection.

369 **5.3 Authentication**

370 **5.3.1 DER/AUTH/BV-01: Unique Credentials**

371 *Test Purpose*

372 Ensure each access control level of security or user account in the IUT requires separate
373 credentials.

374 *Obligation*

375 Mandatory

376 *Reference*

- 377
- DER/AUTH/REQ-01: Unique Credentials [1]

378 *Initial Condition*

- 379
- The IUT is in its original factory setting state, as defined in **DER/PRE/ST-02**.

380 *Test Procedure*

- 381
- 382 1. Create the first user account on the IUT with its own unique ID and authentication
383 credentials.
 - 384 2. If the IUT allows creation of more than one user account, create a second account
385 with a different ID and authentication credential.
 - 386 3. If the IUT has more than one access control security level, create a user account for
each security level with unique IDs and authentication credentials.

387 *Expected Outcome*

- 388
- 389 • Test engineer is able to successfully create an account with a unique ID with unique
390 credentials in step 1 and 2.
 - 391 • For each access control security level, test engineer is able to create an account with
a unique ID and unique credentials.

392 **5.3.2 DER/AUTH/BV-02: Authentication**

393 *Test Purpose*

394 Ensure the IUT authenticates all logical connections, including the physical admin panel
395 should one exist.

396 *Obligation*

397 Mandatory

398 *Reference*

- 399 • DER/AUTH/REQ-02: Authentication [1]

400 *Initial Condition*

- 401 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- 402 • Endpoints are configured to connect without credentials or false credentials.
- 403 • Remote incident notification service is initialized and ready to receive reports from
404 IUT.

405 *Test Procedure*

406 For each of the communication capabilities listed in Section X of the ICS document, perform
407 the following test procedure:

- 408 1. Set up the IUT so it can activate the communication capability
- 409 2. Set up the endpoint with credentials removed.
- 410 3. Activate the communication capability and record the time
- 411 4. If there is a physical admin panel, attempt to access the panel with incorrect
412 credentials and record the time.

413 *Expected Outcome*

- 414 • IUT rejects all connections and login attempts.
- 415 • The Remote incident notification service records each rejected attempt.

416 **5.3.3 DER/AUTH/BV-03: Session Timeout**

417 *Test Purpose*

418 Ensure every authenticated session times out after inactivity.

419 *Obligation*

420 Mandatory

421 *Reference*

- 422 • DER/AUTH/REQ-03: Session Timeout [1]

423 *Initial Condition*

- 424 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.

- 425
- Endpoints are set up to communicate with proper authentication credentials.

426 *Test Procedure*

427 This test case may be run in conjunction with DER/AUTH/BV-02. For each of the
428 communication capabilities listed in Section 1 of the ICS document, perform the following
429 test procedure:

- 430
1. Note the timeout time of the communication capability in Section 1 of the ICS
431 document.
 - 432 2. Start the communication capability.
 - 433 3. For communication capabilities that require human operation:
434 a. Pause operations for the timeout time and then attempt to continue
435 operations.
 - 436 4. For machine-based communication capabilities:
437 b. Observe the communications using the network monitor.
438 c. Stop communications for the timeout time (if possible).
439 d. Record network activity observed by the monitor for a time equal to twice the
440 communication capability's timeout time.

441 *Expected Outcome*

- 442
- For communication capabilities that require human operation, attempts to continue
443 operations after the timeout time fail and the user is prompted to re-authenticate.
 - 444 • For machine communication capabilities, analyze the network activity records. If
445 there is a period of time greater than the timeout time that shows no network traffic,
446 confirm that the communication capability goes through the authentication process
447 again before any more network traffic is attempted.

448 **5.3.4 DER/AUTH/BV-04: Configurable Timeout**

449 *Test Purpose*

450 Ensure the session timeout time can be configured by the end user.

451 *Obligation*

452 Mandatory

453 *Reference*

- 454
- DER/AUTH/REQ-04: Configurable Timeout [1]

455 *Initial Condition*

- 456
- The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
 - 457 • Endpoints are set up to communicate with proper authentication credentials.

458 *Test Procedure*

459 For each of the communication capabilities listed in Section 1 of the ICS document, perform
460 the following test procedure:

- 461 1. Modify the timeout time of the communication capability.
462 2. Start the communication capability.
463 3. For communication capabilities that require human operation:
464 a. Pause operations for the new timeout time and then attempt to continue
465 operations.
466 4. For machine-based communication capabilities:
467 b. Observe the communications using the network monitor.
468 c. Stop communications for the timeout time (if possible).
469 d. Record network activity observed by the monitor for a time equal to twice the
470 communication capability's new timeout time.

471 *Expected Outcome*

- 472 • For communication capabilities that require human operation, attempt to continue
473 operations fails and the user is prompted to re-authenticate.
474 • For machine communication capabilities, analyze the network activity records. If
475 there is a period of time greater than the new timeout time that shows no network
476 traffic, confirm that the communication capability goes through the authentication
477 process again before any more network traffic is attempted.

478 **5.3.5 DER/AUTH/BV-05: Strong Passwords**

479 *Test Purpose*

480 Ensure all passwords are strong and the IUT notifies the user if a weak password is entered.

481 *Obligation*

482 Mandatory for password authentication mechanisms only (if the IUT does not use
483 passwords for authentication, must be skipped).

484 *Reference*

- 485 • DER/AUTH/REQ-05: Strong Passwords [1]

486 *Initial Condition*

- 487 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
488 • Remote incident notification service is initialized and ready to receive reports from
489 IUT.

490 *Test Procedure*

491 For each of the communication capabilities listed in Section 1 of the ICS document that use
492 password for authentication, and for the IUT admin panel (if any), perform the following test
493 procedure:

- 494 1. Create one password that conforms to each format listed [Table 5-4](#).
495 2. Attempt to set up the device with each of the passwords.
496 3. Observe all stored passwords on the IUT.

497

498

Table 5-4: Unsecure password formats

Format	Example	Requirement
Less than 8 characters	“pass”	Fail
64 characters	01234567890123456789012345 67890123456789012345678901 234567890123	Pass

499

500 *Expected Outcome*

- 501 • IUT rejects each password and asks the user to pick a stronger one.
- 502 • Observed passwords on the IUT do not conform to one of the formats listed in [Table](#)
- 503 [5-4](#).

504 **5.3.6 DER/AUTH/BV-06: Unique Passwords**

505 *Test Purpose*

506 Ensure the user is prompted to create a new password on first login..

507 *Obligation*

508 Mandatory for password authentication mechanisms only (if the IUT does not use
509 passwords for authentication this must be skipped).

510 *Reference*

- 511 • DER/AUTH/REQ-06: Unique Passwords [1]

512 *Initial Condition*

- 513 • The IUT is in its factory default state, as defined in [DER/PRE/ST-02](#).

514 *Test Procedure*

- 515 1. Check the ICS to see if the IUT has a unique password installed at the factory.
- 516 2. If yes, check to see if the password is shown on the IUT (either a label or on a
517 screen).
- 518 3. If no, log in to the IUT according to the manufacturer's instructions.

519 *Expected Outcome*

- 520 • If the ICS document states the IUT has a factory-installed unique password, the
521 password is not shown on the IUT.
- 522 • If there is no factory-installed unique password or the factory-installed unique
523 password is shown on the IUT, the technician is prompted to create a new password
524 on first login.

525 **5.3.7 DER/AUTH/BV-07: Brute Force Prevention**

526 *Test Purpose*

527 Ensure the IUT locks login capability after at most 10 failed password login attempts.

528 *Obligation*

529 Mandatory for password authentication mechanisms only (if the IUT does not use
530 passwords for authentication, must be skipped).

531 *Reference*

- 532 • DER/AUTH/REQ-07: Brute Force Prevention [1]

533 *Initial Condition*

- 534 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- 535 • At least one user has set up an account with password.
- 536 • Remote incident notification service is initialized and ready to receive reports from
537 IUT.

538 *Test Procedure*

- 539 1. Attempt to log in to the IUT at least 10 times using an incorrect password
- 540 2. Record the time

541 *Expected Outcome*

- 542 • IUT disables login for at least 5 minutes
- 543 • The Remote incident notification service records the account lockout.

544 **5.3.8 DER/AUTH/BV-08: Password Protection**

545 *Test Purpose*

546 Ensure the IUT does not reveal passwords.

547 *Obligation*

548 Mandatory for password authentication mechanisms only (if the IUT does not use
549 passwords for authentication, must be skipped).

550 *Reference*

- 551 • DER/AUTH/REQ-08: Password Protection [1]

552 *Initial Condition*

- 553 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- 554 • At least one user has set up a password.

Interface/Port	Test Procedure
Cellular	TBD
Serial	TBD
USB	Check if active using the USB tester

580

581 *Expected Outcome*

- 582 • All active interfaces and ports are listed in ICS.
583 • All hardware interfaces not listed in the ICS list are disabled.

584 **5.4.2 DER/DSEC/BV-02: Factory Reset**

585 *Test Purpose*

586 Ensure the IUT is able to reset to factory settings.

587 *Obligation*

588 Mandatory

589 *Reference*

- 590 • DER/DSEC/REQ-02: Factory Reset [1]

591 *Initial Condition*

- 592 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
593 • At least one user has set up a password.

594 *Test Procedure*

- 595 1. Activate the factory reset function.

596 *Expected Outcome*

- 597 • IUT is back in factory mode and no user information is on the IUT

598 **5.5 Logging**

599 **5.5.1 DER/LOG/BV-01: Log Storage**

600 *Test Purpose*

601 Ensure the DER device stores logs in persistent memory.

602 *Obligation*

603 Mandatory

604 *Reference*

- 605 • DER/LOG/REQ-02: Log Storage [1]

606 *Initial Condition*

- 607 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.

608 *Test Procedure*

- 609 1. Remove power from the device and record the time.
- 610 2. Power the device again.
- 611 3. Print the device logs from the beginning of the testing cycle. This is copy 3.

612 *Expected Outcome*

- 613 • Copy 2 (from BV-25) and copy 3 should match up to the time the power is removed
614 from the device.

615 **5.5.2 DER/LOG/BV-02: Configuration Logs**

616 *Test Purpose*

617 Ensure the IUT stores changes to configuration.

618 *Obligation*

619 Mandatory

620 *Reference*

- 621 • DER/LOG/REQ-06: Configuration Logs [1]

622 *Initial Condition*

- 623 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- 624 • Test engineer's clock is synchronized with Coordinated Universal Time (UTC)
- 625 • Remote log repository is able to receive logs.

626 *Test Procedure*

- 627 1. Make a list of all IUT configuration settings from the manual (ICS document?)
- 628 2. For each setting, record the old value, change the configuration value, record the
629 new value, and record the time.
- 630 3. View the IUT logs by following manufacturer instructions.

631 *Expected Outcome*

- 632 • Each configuration change is shown in the logs.
- 633 • Each change has the correct timestamp (within 1 minute of the test engineer's
634 notebook) with a resolution of 1 millisecond.

635 **5.5.3 DER/LOG/BV-03: Network Logs**

636 *Test Purpose*

637 Ensure the IUT logs network communication events.

638 *Obligation*

639 Mandatory

640 *Reference*

- 641 • DER/LOG/REQ-07: Networks Logs [1]

642 *Initial Condition*

- 643 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- 644 • Remote log repository is able to receive logs.

645 *Test Procedure*

646 The below must be performed for every communication capability listed in the ICS
647 document:

- 648 1. Activate the communication capability.
- 649 2. View the IUT logs on the IUT

650 *Expected Outcome*

- 651 • IUT logs the events of the communication capability including:
 - 652 ○ Device address
 - 653 ○ Endpoint address
 - 654 ○ Authentication messages
 - 655 ○ Session start time, session end time, session timeout events
- 656 • Each event has a timestamp with a resolution of 1 millisecond.

657 **5.5.4 DER/LOG/BV-04: Security Logs**

658 *Test Purpose*

659 Ensure the IUT stores security event logs.

660 *Obligation*

661 Mandatory. This test can be conducted with DER/AUTH/BV-02.

662 *Reference*

- 663 • DER/LOG/REQ-08: Security Logs [1]

664 *Initial Condition*

- 665 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- 666 • Prepare a list of false credentials for each of the communication capabilities listed in
667 Section 1 of the ICS document.

- 668 • Test engineer's clock is synchronized to UTC.
- 669 • Remote log repository is able to receive logs.

670 *Test Procedure*

- 671 1. For each of the communication capabilities listed in Section 1 of the ICS document,
672 activate the capability using the appropriate false credential and record the time of
673 the activation.
- 674 2. If there is a physical administration panel, attempt to login to each access control
675 level with a false credential and record the time of login attempt.
- 676 3. Add and remove users at each level of access control, and record the time each user
677 is added or removed.
- 678 4. Change the access control credentials of a user at each level of access control, and
679 record the time of change.

680 *Expected Outcome*

- 681 • IUT log shows each recorded event with the proper time.
- 682 • Each event has the correct timestamp (within 1 minute of the test engineer's
683 notebook) with a resolution of 1 millisecond.

684 **5.5.5 DER/LOG/BV-05: Remote Logs**

685 *Test Purpose*

686 Ensure the IUT sends logs to a remote central repository at least once a day.

687 *Obligation*

688 Mandatory

689 *Reference*

- 690 • DER/LOG/REQ-09: Remote Logs [1]

691 *Initial Condition*

- 692 • The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
- 693 • Remote log repository is able to receive logs.

694 *Test Procedure*

- 695 1. Print the IUT logs. This is copy 1.
- 696 2. Let the IUT run in a normal fashion for at least 24 hours.
- 697 3. Print the IUT logs. This is copy 2.
- 698 4. View the IUT's logs on the remote server.

699 *Expected Outcome*

- 700 • The IUT logs on the remote server contain the log events recorded from copy 1 to
701 copy 2.

702 **5.5.6 DER/LOG/BV-06: Log Retention**

703 *Test Purpose*

704 Ensure the manufacturer stores logs at least 90 days.

705 *Obligation*

706 This test need not be completed before the device applies for certification.

707 *Reference*

- 708
 - DER/LOG/REQ-10: Log Retention [1]

709 *Initial Condition*

710 None

711 *Test Procedure*

- 712 1. 90 days after the Remote Logs test case, read the IUT's logs on the remote
713 repository.

714 **Expected Outcome**

- 715
 - The log files on the remote repository contain network events at least 7 days old.
 - 716 • The log files on the remote repository contain non-network events at least 90 days
717 old.

718 **5.5.7 DER/LOG/BV-07: Incident Reporting**

719 *Test Purpose*

720 Ensure the IUT reports security incident events.

721 *Obligation*

722 Mandatory

723 *Reference*

- 724
 - DER/LOG/REQ-11: Incident Reporting [1]

725 *Initial Condition*

726 None.

727 *Test Procedure*

- 728 1. Print all the security incidents on the remote incident notification service from the
729 beginning of the testing cycle.

730 *Expected Outcome*

- 731
 - Every failed authentication and failed software update is recorded in the print out.

732 **5.5.8 DER/LOG/BV-08: Power System Logs**

733 *Test Purpose*

734 Ensure the DER device stores power configuration changes and power cycle events.

735 *Obligation*

736 Mandatory

737 *Reference*

- 738
 - DER/LOG/REQ-12: Power System Logs [1]

739 *Initial Condition*

- 740
 - The IUT is in its basic operational state, as defined in DER/PRE/ST-01.
 - Remote log repository is able to receive logs.

742 *Test Procedure*

- 743
 1. Change power configuration settings on the IUT and record the time of each
 - 744 configuration change.
 - 745 2. Remove power from the device and record the time.
 - 746 3. Power the device again and record the time.

747 *Expected Outcome*

- 748
 - IUT log shows each power configuration change event with the proper time.
 - 749 • IUT log shows the time of the power cycle boot up.
 - 750 • Each event has the correct timestamp (within 1 minute of the test engineer's
 - 751 notebook) with a resolution of 1 millisecond.