Document #:

Status: Draft

Version: 0.1

SunSpec Cybersecurity Certification

Phase 1 Test Suite

Abstract

TBD.

22

License Agreement and Copyright Notice

Prepared by the SunSpec Alliance
4040 Moorpark Avenue, Suite 110
San Jose, CA 95117

Website: sunspec.org
Email: info@sunspec.org

44

About the SunSpec Alliance

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

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

About the SunSpec Specification Process

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

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

SunSpec Interoperability Specifications follow a lifecycle pattern of: DRAFT, TEST, APPROVED, and SUPERSEDED.

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

Revision History

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

Contents

1 Scope

TBD

2 References

[1] SunSec Alliance, SunSpec Cybersecurity Certification, Phase 1 Requirements, Version 1.0, 2022. Available from https://docs.google.com/document/d/1IKLeOAyjgk_XdZw9eOGK603t850gRyijQjD2gEur8fo/

3 Definitions and abbreviations

3.1 Definitions

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

None

3.2 Abbreviations

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

AUTH	Authentication
DCOM	Device Communication
DER	Distributed energy resource
ICS	Implementation Conformance Statement
IUT	Implementation under test
SWUP	Software Update

4 Setup preambles

4.1 Operational states

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

State of the IUT required to operate normally.

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

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

4.2 Required Equipment

- IUT (provided by manufacturer)
- Communication endpoints (provided by the manufacturer)
- Remote log server (provided by the manufacturer)
- Remote incident notification service (provided by the manufacturer)
- Secrets (keys, passwords, tokens, etc.) required to conduct tests (provided by the manufacturer)
- Completed and signed ICS document (provided by the manufacturer)
- User or instruction manual for IUT (provided by the manufacturer)
- Network traffic monitor (provided by the test lab)
- USB tester (provided by the test lab)
- Wi-Fi scanner (provided by the test lab)

5 Test cases

5.1 Software Update

5.1.1 DER/SWUP/BV-01: Updatable Software

Test Purpose

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

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

1. The test engineer determines the software version of the currently installed security and operational software functions.
2. The test engineer installs the software update on the IUT and records the time of software update.
3. The test engineer determines the software version of the currently installed security and operational software functions.

Expected Outcome

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

Remaining questions

- How to determine which components IUT is able to update

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

Test Purpose

Verify that the IUT supports remote updates.

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

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

Expected Outcome

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

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

Test Purpose

Verify that the IUT supports automatic updates

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

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

Expected Outcome

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

5.1.4 DER/SWUP/BV-04: Secure Updates

Test Purpose

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

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

1. The test engineer determines the software version of the currently installed software.
2. The test engineer installs the first software update on the IUT and records the time.
3. The test engineer determines the software version of the currently installed software.
4. The test engineer installs the second software update on the IUT and records the time..
5. The test engineer determines the software version of the currently installed software.

Expected Outcome

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

5.1.5 DER/SWUP/BV-05: Downgrade Prevention

Test Purpose

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

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

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

Expected Outcome

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

5.2 Device Communication

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

Test Purpose

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

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

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

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

Expected Outcome

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

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

Test Purpose

Ensure the IUT does not downgrade to unsecure protocols.

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

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

1. Set up the IUT so it can activate the communication capability
2. For the first deprecated protocol listed in Table 5-1 associated with the communication capability's protocol, set up the endpoint so that it will request the protocol to downgrade to this deprecated protocol.
3. Attach the network monitor so it can analyze the traffic between the device and endpoint.
4. Activate the communication capability and record the time
5. Observe the network traffic with the monitor.
6. Go back to step 1 for the next deprecated protocol associated with the communication capability's protocol. If there is no remaining deprecated protocol associated with the communication capability in question, move to test the next communication capability listed in the ICS document.

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

Expected Outcome

- IUT rejects all connections.

5.2.3 DER/DCOM/BV-03: Deprecated Ciphersuites

Test Purpose

Ensure the IUT is only using approved ciphersuites.

Obligation

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

Reference

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

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.

Test Procedure

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

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

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

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

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

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		
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	

Expected Outcome

- IUT rejects each connection.

5.3 Authentication

5.3.1 DER/AUTH/BV-01: Unique Credentials

Test Purpose

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

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

1. Create the first user account on the IUT with its own unique ID and authentication credentials.
2. If the IUT allows creation of more than one user account, create a second account with a different ID and authentication credential.
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.

Expected Outcome

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

5.3.2 DER/AUTH/BV-02: Authentication

Test Purpose

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

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

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

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

Expected Outcome

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

5.3.3 DER/AUTH/BV-03: Session Timeout

Test Purpose

Ensure every authenticated session times out after inactivity.

Obligation

Mandatory

Reference

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

Initial Condition

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

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

Test Procedure

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

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

Expected Outcome

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

5.3.4 DER/AUTH/BV-04: Configurable Timeout

Test Purpose

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

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

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

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

Expected Outcome

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

5.3.5 DER/AUTH/BV-05: Strong Passwords

Test Purpose

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

Obligation

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

Reference

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

Initial Condition

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

Test Procedure

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

1. Create one password that conforms to each format listed Table 5-4.
2. Attempt to set up the device with each of the passwords.
3. Observe all stored passwords on the IUT.

Table 5-4: Unsecure password formats

Format	Example	Requirement
Less than 8 characters	“pass”	Fail
64 characters	0123456789012345678901234567890123456789012345678901234567890123	Pass

Expected Outcome

- IUT rejects each password and asks the user to pick a stronger one.
- Observed passwords on the IUT do not conform to one of the formats listed in Table 5-4.

5.3.6 DER/AUTH/BV-06: Unique Passwords

Test Purpose

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

Obligation

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

Reference

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

Initial Condition

- The IUT is in its factory default state, as defined in DER/PRE/ST-02.

Test Procedure

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

Expected Outcome

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

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

Test Purpose

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

Obligation

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

Reference

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

Initial Condition

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

Test Procedure

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

Expected Outcome

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

5.3.8 DER/AUTH/BV-08: Password Protection

Test Purpose

Ensure the IUT does not reveal passwords.

Obligation

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

Reference

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

Initial Condition

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

Test Procedure

1. Study the instruction manual and record the mechanism for accessing user profile data.
2. Log into the IUT at the highest access control security level.
3. Look up passwords utilizing each mechanism.

Expected Outcome

- All passwords are obfuscated and cannot be viewed.

5.4 Device Security

5.4.1 DER/DSEC/BV-01: Minimal Interfaces

Test Purpose

Ensure the IUT has no unused interfaces or ports.

Obligation

Mandatory

Reference

- DER/DSEC/REQ-01: Minimal Interfaces [1]

Initial Condition

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

Test Procedure

1. Observe the IUT and review the specifications.
2. Note any hardware interfaces not listed in the ICS document.
3. Test the existence of any of the logical ports listed in Table 5-5 that are not listed in Section 1 of the ICS document.
4. Test hardware interfaces not listed in the ICS list using the appropriate tester for the hardware interface (e.g.- USB tester for a USB interface).

Table 5-5: List of possible hardware interfaces

Interface/Port	Test Procedure
Ethernet	Connect the network monitor to see how many of the possible 65,535 ports are open.
WiFi Station	Check if active using the WiFi scanner
WiFi Access Point	Check if active using the WiFi scanner
WiFi Bridge	Check if active using the WiFi scanner
WiFi Router	Check if active using the WiFi scanner

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

Expected Outcome

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

5.4.2 DER/DSEC/BV-02: Factory Reset

Test Purpose

Ensure the IUT is able to reset to factory settings.

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

1. Activate the factory reset function.

Expected Outcome

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

5.5 Logging

5.5.1 DER/LOG/BV-01: Log Storage

Test Purpose

Ensure the DER device stores logs in persistent memory.

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

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

Expected Outcome

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

5.5.2 DER/LOG/BV-02: Configuration Logs

Test Purpose

Ensure the IUT stores changes to configuration.

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

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

Expected Outcome

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

5.5.3 DER/LOG/BV-03: Network Logs

Test Purpose

Ensure the IUT logs network communication events.

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

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

1. Activate the communication capability.
2. View the IUT logs on the IUT

Expected Outcome

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

5.5.4 DER/LOG/BV-04: Security Logs

Test Purpose

Ensure the IUT stores security event logs.

Obligation

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

Reference

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

Initial Condition

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

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

Test Procedure

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

Expected Outcome

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

5.5.5 DER/LOG/BV-05: Remote Logs

Test Purpose

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

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

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

Expected Outcome

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

5.5.6 DER/LOG/BV-06: Log Retention

Test Purpose

Ensure the manufacturer stores logs at least 90 days.

Obligation

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

Reference

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

Initial Condition

None

Test Procedure

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

Expected Outcome

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

5.5.7 DER/LOG/BV-07: Incident Reporting

Test Purpose

Ensure the IUT reports security incident events.

Obligation

Mandatory

Reference

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

Initial Condition

None.

Test Procedure

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

Expected Outcome

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

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

Test Purpose

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

Obligation

Mandatory

Reference

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

Initial Condition

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

Test Procedure

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

Expected Outcome

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