Document #:

Status: APPROVED

Version: 1.0

SunSpec Cybersecurity Certification

Phase 1 Requirements

License Agreement and Copyright Notice

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

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

Prepared by the SunSpec Alliance

4040 Moorpark Avenue, Suite 110

San Jose, CA 95117

Website: sunspec.org

Email: info@sunspec.org

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 180 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/.

1 Revision History

Version	Date	Comments
0.1	22-11-23	Initial draft based on Lumian contribution
0.2	23-03-31	Incorporated comments
0.3	23-06-03	Incorporated comments from review meetings
0.4	23-06-04	Incorporated comments
0.5	23-06-06	Removed log retention requirement
0.6	23-06-07	Correct typos and references
1.0	23-07-11	Integrate remaining public comments

2 Contents

3 Scope

This document describes the cybersecurity requirements for devices to conform to Phase 1 of the SunSpec Cybersecurity Certification Program.

4 References

[1] IETF, RFC 2119, “Keys words for use in RFCs to Indicate Requirement Levels”, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

[2] NIST, Special Publication 800-63B. https://pages.nist.gov/800-63-3/sp800-63b.html.

[3] NERC, CIP-007-6 — Cyber Security – Systems Security Management. https://www.nerc.com/pa/Stand/Prjct2014XXCrtclInfraPrtctnVr5Rvns/CIP-007-6_CLEAN_06022014.pdf.

[4] NSA, Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations, https://media.defense.gov/2021/Jan/05/2002560140/-1/-1/0/ELIMINATING_OBSOLETE_TLS_UOO197443-20.PDF

[5] IETF Deprecation of IKEv1 and obsoleted algorithms. https://datatracker.ietf.org/doc/rfc9395/

5 Definitions, abbreviations, and terminology

5.1 Definitions

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

Power Cycle: A power Cycle consists of two steps: 1) Power down or remove power from a device, and 2) turn the device back on.

5.2 Abbreviations

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

AUTH	Authentication
DCOM	Device communications
DER	Distributed energy resource
DSEC	Device security
SWUP	Software updates

5.3 Terminology

The specification lists a series of requirements, either explicitly or within the text, which are mandatory elements for compliant solutions. Recommendations are given, to ensure optimal usage and to provide suitable performance. All recommendations are optional.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are following the notation as described in RFC 2119 3[1].

1. MUST: This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute requirement of the specification.
2. MUST NOT: This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
3. SHOULD: This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
5. MAY: This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option,

though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

6 Requirements

6.1 Software Updates/Product Support

6.1.1 DER/SWUP/REQ-01: Software Updates

Summary

The DER device SHALL support updating mutable security and operational software components.

Description

The DER device SHALL have the ability to have software components, listed in Table 6-1, updated, if the respective component is installed on the device.

Component/Functionality	Must be updatable?
Operating system (kernel)	Yes
Operating system (non-kernel)	Yes
Boot loader or BIOS	Yes
Applications	Yes
Libraries	Yes
Configuration	Yes
Certificates	Yes

Table 6-1: Updatable Software Components

Rationale

The security community is constantly finding new vulnerabilities in software. These new vulnerabilities are reported to the public at least 60 days after they have been found. Adversaries often design attacks around these newly found vulnerabilities. Devices that are not able to be updated will continue to be a target of these adversaries. Similarly, a user needs to know the software version of a device to determine if the device has the latest version.

6.1.2 DER/SWUP/REQ-02: Software Version

Summary

The DER device SHALL include a mechanism for a user to read the current software version of the device and components listed in Table 6-1.

Description

The DER device SHALL offer the user a mechanism to read the current software version of the device as well as the version of each of the components in Table 6-1.

Rationale

A user needs to know the software version of a device to determine if the device has the latest version.

6.1.3 DER/SWUP/REQ-03: Remote Updates

Summary

The DER device SHALL have the capability to support remote updates.

Description

A device SHALL communicate with a remote server at least once per day to download and install a software update when available. The device MAY allow a user to turn off remote updates, but remote updates SHALL be active by default (default factory setting).

Rationale

DER devices are located on site and are not easily (or inexpensively) accessible by maintenance crew for local software updates. Even if cost and resources were not a factor, the time required to visit all sites and manually update software is more time than adversaries need to conduct their attacks. Remote updates allow vendors and site managers to trigger software updates remotely in seconds, giving adversaries much less time.

6.1.4 DER/SWUP/REQ-04: Automatic Updates

Summary

The DER device SHALL support automated updates.

Description

No additional explanation.

Rationale

Without automated updates a user needs to manually trigger a device to obtain an update. If thousands of devices are in the field, this takes too much time even if the update can be triggered remotely and even if the user acts quickly when an update is available.

6.1.5 DER/SWUP/REQ-05: Secure Updates

Summary

The DER device SHALL verify the authenticity and integrity of software updates, prior to installing it.

Description

The DER device SHALL use a mechanism that verifies that the software update package came from a trusted source, such as the manufacturer. An example of an authentication mechanism is a cryptographic signature. The DER device SHALL verify that the software update package was not modified by a third party. An example of an integrity mechanism is a checksum or hash.

Rationale

Attacking the software update system is commonly used by adversaries, and can allow an adversary to gain complete control over a device. Checking the authenticity (the creator/author) and integrity (the package has not been modified) of a package prevents such attacks.

6.1.6 DER/SWUP/REQ-06: Local Updates

Summary

If the DER device supports local updates, then this functionality SHALL comply with the same security requirements of the remote update functionality.

Description

No other explanation necessary.

Rationale

Same as the Secure Updates requirement.

6.2 Device Communications

6.2.1 DER/DCOM/REQ-01: Secure Communications

Summary

The DER device SHALL implement at least one of TLS 1.2 (or higher), IPSec Version 2 (or higher), or SSH-2 for all communications that can access the public Internet.

Description

Any DER device functionality that can communicate over the public Internet MUST be secured by the latest versions of either TLS, IPSec, or SSH. This includes not only default functionality but also optional or configurable functionality. For example, if a DER device can communicate to a local device using MODBUS over a serial line, and this communication functionality can also be configured to communicate MODBUS over an IP network, this functionality MUST be secured. This also includes utility protocols like DNS and NTP.

TLS 1.2 (or higher), IPSec Version 2 (Committee on National Security Systems Policy 15-compliant), and SSH-2 SHALL be the only allowed protocols for securing such communications.

Rationale

Network access to a device is one of the easiest attack vectors for adversaries because an adversary does not need physical access to the device to carry out an attack. Attacks can modify data in transit, spoof communications from a trusted endpoint, and eavesdrop on sensitive data. TLS, IPSec, and SSH are widely used and scrutinized protocols that offer the authentication and encryption capabilities that prevent these attacks, and the required versions are specified because previous versions of these protocols contain vulnerabilities. While there are other protocols that have the same capabilities of TLS, IPSec, and SSH they do not receive the same scrutiny and are therefore considered less trustworthy.

6.2.2 DER/DCOM/REQ-02: Downgrade Prevention

Summary

A DER device SHALL reject security technology deprecated by the NSA [4] and IETF [5].

Description

TLS 1.2 contains ciphersuites that have been found to be vulnerable (Table 6-2). TLS 1.3 removes these ciphersuites. TLS 1.2 implementations must only use TLS 1.3 ciphersuites. The NSA has also deprecated several ciphersuites and key exchange algorithms used in IPSEC and SSH (Table 6-3). These MUST not be used.

Rationale

NSA deprecates security technology when they no longer are secure. TLS 1.3 is the latest version of TLS, but it is not yet widely supported in software libraries. TLS 1.2 is still allowed and widely supported but contains deprecated technology by default. Fortunately it is straightforward to remove deprecated ciphersuites.

Ciphersuite	Key Exchange
RC2	
RC4	
DES	
IDEA	
TDES/3ES	
	ANON
	EXPORT
	RSA (<1024 bits or between 1024 and 2048 bits)
	DHE (<1024 bits or between 1024 and 2048 bits)
	ECDHE with custom curves

Table 6-2: Deprecated TLS ciphersuites and key exchange algorithms, derived from NSA 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	
	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	

Table 6-3: Deprecated IPSEC transforms, derived from IETF recommendations.

References

IETF, RFC 2119 [1]

NSA, Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations [4]

6.3 Authentication

6.3.1 DER/AUTH/REQ-01: Unique Credentials

Summary

The DER device SHALL require the use of unique security credentials (such as passwords or keys) for each level of privilege and user account available on the Device.

Description

All users MUST be associated with a unique account with unique security credentials. If the DER device has multiple access levels or multiple user accounts, it MUST support unique security credentials for each access level.

Rationale

Sharing credentials among multiple users is generally not a good security practice. A device must allow for different credentials for each security access level and user. However, if users wants to use the same credentials across access levels and user accounts, the device is allowed to accommodate this desire. In this case the user could use a secure password management application to mitigate the risks of using shared credentials.

6.3.2 DER/AUTH/REQ-02: Authentication

Summary

All electronic access to the device, whether locally through a control panel or diagnostic port, or remotely through communications channels, SHALL be protected with an authentication mechanism that securely identifies a subject with a unique user identification (ID).

Description

This requirement specifies that a device MUST have the ability to differentiate between different users (with an ID) and authenticate them securely. The authentication means is not specified, but MUST be secure. If passwords are used as the authentication mechanism, they MUST comply with the requirements in this document. There are also many passwordless authentication mechanisms such as X.509 certificates, unique login codes sent out-of-band, and use of FIDO-compatible devices.

Rationale

Authenticating a user’s electronic access to a device prevents installation of malicious code, unauthorized access to data, and control of a device by an adversary. Unique IDs are required for authentication methods and allow devices to allocate different permissions to different users.

References

NIST Special Publication 800-63B [2]

6.3.3 DER/AUTH/REQ-03: Session Timeout

Summary

All authenticated sessions SHALL have a timeout.

Description

The DER device MUST have a timeout feature that automatically logs out a user who remains logged in after a period of inactivity. Inactivity SHALL be defined as the absence of input from local or remote DER interfaces and endpoints.

Rationale

This requirement addresses sessions wherein the user can be replaced by an adversary. For example, if a user logs into an admin panel (physically on the device or via remote computer) and the user walks away without logging off, an adversary who gains access to the panel can start an attack.

6.3.4 DER/AUTH/REQ-04: Configurable Timeout

Summary

The length of time before a session automatically times out SHALL be settable by an authorized user.

Description

This requirement states that a device MUST give an authorized user the capability to change the session timeout period. Examples of this capability include a configuration screen on a physical panel or a configuration API.

Rationale

The ideal timeout period is dependent on the characteristics of the site where the device is installed. If the device is within a secured perimeter the timeout period can be longer. The timeout for a remote technician can also be longer if the technician's computer has access control. A physical admin panel in a public space could require a shorter timeout period.

6.3.5 DER/AUTH/REQ-05: Strong Passwords

Summary

If a DER device uses passwords for authentication, then the DER device SHALL enforce strong passwords and SHALL notify users of the password requirements if they attempt to use a non-compliant password.

Description

Compliance with this requirement SHALL be achieved in one of two ways:

1. Password strength meter: Device implements a password strength meter that follows NIST password recommendations (5.1.1.2 of the NIST Special Publication 800-63B [2]). Only passwords deemed by the strength meter to be "strong" SHALL be allowed.

2. Password MUST meet the following set of rules to be allowed:
    - At least 8 characters in length, and the device MUST allow passwords up to 64 characters in length
    - Case sensitive
    - At least one number
    - At least one letter
    - At least one non-alphanumeric character (not a letter or a number)

Rationale

Passwords are an often-used attack vector for adversaries. Strong passwords prevent basic password attacks. The latest password research has concluded that length and entropy of a password is the best predictor of strength. Requiring numbers and symbols has shown to not increase the strength of a password. However, this requirement mimics NERC CIP-007-6 [3] which has such requirements.

References

NIST Special Publication 800-63B [2]

NERC CIP-007-6 — Cyber Security – Systems Security Management [3]

6.3.6 DER/AUTH/REQ-06: Unique Passwords

Summary

If pre-installed passwords are shared among many devices, or the pre-installed password is displayed on the device, then the DER device SHALL require users to create a new password when they first login.

Description

If a DER device manufacturer loads the same password on multiple devices, then the DER device MUST require the user to create a different password when the device is first accessed by the user. If a manufacturer prints the default password on the IUT, then the DER device MUST require the user to create a different password when the device is first accessed by the user.

Rationale

Default common passwords are one of the most used attack vectors compromise devices. Many jurisdictions around the world have outlawed the practice of using default common passwords.

6.3.7 DER/AUTH/REQ-07: Brute Force Prevention

Summary

If a DER device uses passwords as the only method of authentication, The device SHALL support an approved (see description) brute force prevention mechanism.

Description

The only current approved brute force prevention mechanism is account lockouts. After a maximum of 10 consecutive failed password login attempts to a unique user account, the device MUST lock out the user for at least 5 minutes. The maximum number of consecutive failed password login attempts is 10 before this lock out occurs. SunSpec may add other approved mechanisms in the future. Devices that use a second factor of authentication (e.g.- one-time codes generated via text, email, mobile app, or hardware key) do not need to meet this requirement.

Rationale

Brute force password attacks can break even strong passwords given enough time. Temporary lockouts make brute force attacks infeasible by dramatically increasing the amount of time necessary to guess the correct password.

6.3.8 DER/AUTH/REQ-08: Password Protection

Summary

The DER device SHALL prevent storage or display of unencrypted passwords.

Description

The DER device MUST NOT display stored plain text passwords on screens, including the local display panel, configuration software (local or remote; offline or online), web browser, and terminal access, after a password is first created. A device MUST NOT store plain text passwords in audit trails, the memory area or files, or other records and configuration files. A DER device MAY display the password a user enters for authentication to the user only (e.g.- entering a password so the user can see if they entered the password).

Rationale

Passwords stored in plain text can be copied and distributed to adversaries. Adversaries that gain access to the device through a lower clearance security channel could copy passwords of users with much higher clearance.

6.3.9 DER/AUTH/REQ-09: Admin Login without Brute Force Protection

Summary

The DER device SHALL support at least one network-accessible admin account that does not utilize brute force prevention.

Description

At least one admin account must be authenticated with a mechanism different than passwords, or with passwords as one of at least two authentication factors. Such an account should not utilize brute force prevention and therefore does not require DER/AUTH/REQ-7.

Rationale

Brute force prevention mechanisms can be used as a denial of service attack on user accounts. If all of a device’s admin accounts use passwords as the single authentication factor, an adversary can disable all accounts by triggering the lock-out mechanism. However, if at least one of the admin accounts does not have brute force prevention this account can be used to access the device.

6.4 Device Security

6.4.1 DER/DSEC/REQ-01: Minimal Interfaces

Summary

The DER device SHALL have any unneeded logical interfaces and ports removed (or disabled if removal is not possible) prior to transfer of device custody.

Description

A device manufacturer MUST list (in PICS) all logical interfaces and ports used by the device, as well as the use. Any logical interfaces and ports not on this list MUST be removed or disabled before the device is transferred from the manufacturer’s custody. The manufacturer must not rely on a customer or installer to remove or disable unused logical interfaces and ports. Examples of physical interfaces include: WiFi, Bluetooth, and Ethernet ports. Examples of logical interfaces include TCP ports (e.g.- port 5590).

Rationale

Many operating systems default to opening multiple ports (port 21, port 53, port 80, port 110, port 23, port 139 etc.). If these ports are not used, they become targets for adversaries especially if they are not secured properly. Wireless interfaces are more important to disable if not used because they allow remote access to a device, which is different from wired interfaces like USB which require physical access.

6.4.2 DER/DSEC/REQ-02: Factory Reset

Summary

The DER device SHALL support a "factory reset" option for end-of-life or repurposing the device.

Description

A factory reset option allows the owner of the device to wipe data from the device and return it to the “factory setting”, which is the state the device was in when it was first manufactured, before giving up ownership. Software update files need not be wiped as they do not contain sensitive data and remove vulnerabilities in previous software versions.

Rationale

Over a device’s lifetime in service it could collect and store sensitive data such as logs, encrypted passwords, and configuration files. These files can be utilized by an adversary to initiate an attack on the original owner's existing assets.

6.5 Logging

6.5.1 DER/LOG/REQ-01: Secure Logs

Summary

The DER device SHALL store logs that are only readable and writable by a privileged level of access control.

Description

No further explanation needed.

Rationale

Logs are required to analyze and stop security breaches. Protecting them is important to prevent adversaries from covering their tracks.

6.5.2 DER/LOG/REQ-02: Timestamp Logs

Summary

The DER device SHALL log events with a timestamp.

Description

No further explanation needed.

Rationale

Logging events with a timestamp is useful for security forensics.

6.5.3 DER/LOG/REQ-03: Timestamp Resolution

Summary

The DER device SHALL timestamp logs with a resolution of at least 1 millisecond.

Description

No additional explanation necessary.

Rationale

To record the correct order of security events a resolution of at least 1 millisecond is required.

6.5.4 DER/LOG/REQ-04: Timestamp Accuracy

Summary

The DER device SHALL maintain time accuracy within +/- 1 min of Coordinated Universal Time (UTC) for all logging timestamps.

Description

This requires devices to synchronize with a remote reliable information source such as a cellphone service, Internet server, or GPS signal.

Rationale

Monitoring logs across multiple devices requires timestamps to be consistent.

6.5.5 DER/LOG/REQ-05: Configuration Logs

Summary

The DER device SHALL log any changes in security-related configurations.

Description

If interfaces and ports listed in the Minimal Interfaces requirement have modifiable security settings, any change to these settings MUST be logged. Security configurations (firewalls settings, etc.) MUST be logged as well.

Rationale

When a security-related configuration is changed the device needs to log this change so if there is a breach remediation efforts can analyze such changes.

6.5.6 DER/LOG/REQ-06: Security Logs

Summary

The DER device SHALL log security events.

Description

Security events MUST include: (a) successful and unsuccessful login attempts, (b) detected failure of event logging, (c) software updates and changes, (d) changes to access controls or accounts, (e) changes to session timeout.

Rationale

This information is also needed for breach remediation.

6.5.7 DER/LOG/REQ-07: Remote Logs

Summary

If the DER device has communication capabilities, then it SHALL send logs to a remote central repository with an upload frequency of at least once per day.

Description

More explanation is not necessary.

Rationale

Centrally-stored logs allow monitoring solutions to detect threats over a large number of devices. It also reduces the storage needs of devices and allows logs to be kept for a longer period of time. Last, it provides log redundancy because if a hacker accesses a device and modifies or deletes the logs on the device the remote repository still has the original logs. An upload frequency of once per day strikes a balance between keeping logs safe and minimizing the network load.

6.5.8 DER/LOG/REQ-08: Incident Reporting

Summary

The DER device SHALL upload security events to a remote central repository within one minute of the event.

Description

Security events include the following events:

- Failed non-password authentication attempts
- Triggering password brute force account lockout
- Failed software update attempts
- Failed connection attempts
- Network activity that deviates from the normal range of activity
- Attempted access to protected data such as private keys
- When a device is Power Cycled.

Rationale

If security events are uploaded to a remote repository, a central monitoring service can detect patterns across a wide range of devices. If events are reported quickly an attack can be thwarted before it does damage.

6.5.9 DER/LOG/REQ-9: Power Setting Logs

Summary

The DER devices SHALL store power setting event logs.

Description

Power setting event logs include at minimum: (a) when an IEEE 2030.5-related function is enabled or disabled (b) when there is a change to adjustable IEEE 2030.5-related settings of the device.

Rationale

The purpose of a DER device is to manage the behavior of a DER. If an adversary has control of the device, the adversary can attack the power grid by manipulating the power control settings. Logging such manipulations can help detect or analyze unauthorized manipulations.

6.5.10 DER/LOG/REQ-10: Power Cycle Logs

Summary

The DER devices SHALL store Power Cycle event logs.

Description

Power Cycle logs MUST include timestamp.

Rationale

Logging device Power Cycles can detect nefarious activity.

6.5.11 DER/LOG/REQ-11: Panel Logs

Summary

If the DER device has an admin panel, then it must log login activity in a manner consistent with the above logging requirements.

Description

This requirement gives more clarity to how physical access logs are to be handled.

Rationale

Physical access must also be monitored, especially if the device is protecting a high-value target.