SUNSPEC ALLIANCE CERTIFICATION PRACTICE STATEMENT

Version 1.0

Table of Contents

Section 1 Introduction

This section identifies and introduces the set of provisions, and indicates the types of entities and applications, for which this Certification Practice Statement (CPS) is targeted.

1.1 Overview

This CPS is written to support the SunSpec Alliance in securing the Distributed Energy Resources (DER) network, which consists of power generation and storage devices. All gateways, aggregators, or devices that communicate directly with a Utility Communication Gateway require digital Certificates to complete mutual Transport Layer Security (TLS) authentication.

Any use of or reference to this CPS outside the purview of the SunSpec Alliance Policy Authority (PA) is completely at the using party's risk.

This CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure using X.509 (PKIX) Certificate Policy and Certification Practices Framework as described in RFC 3647. All Certificates issued under this CPS conform to RFC 5280.

1.1.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described below, taken from IETF RFC 2119 and updated by RFC 8174.

Note that the force of these words is modified by the requirement level of the document in which they are used.

- MUST: This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute requirement of the specification.
- MUST NOT: This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
- 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.
- 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.
- MAY: This word, or the adjective "OPTIONAL", means that an item is truly optional. An implementation that does not include a particular option MUST be prepared to interoperate with another implementation that does include the option, though perhaps with reduced functionality. Similarly, an implementation that does include a particular option MUST be prepared to interoperate with another implementation that does not include the option (except for the feature the option provides.)

1.2 Document Name and Identification

The SunSpec Alliance CPS is hereafter referred to as "CPS" without the SunSpec Root moniker for brevity. The SunSpec CA will use the CP OID *{ iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) SunSpec(53630) cp(0) 2030.5v.18(0) }* in the Certificates.

Within the SunSpec Alliance PKI, the Smart Energy Root CA (SERCA) issues either a Manufacturing Issuing CA (MICA) or Manufacturer's CA (MCA) Intermediate Certificate to manufacturers.

1.3 PKI Participants

The following are roles relevant to the administration and operation of the SunSpec Alliance PKI.

1.3.1 Policy Authority

1.3.1.1 SunSpec Policy Authority

The SunSpec Alliance PA, hereafter reference to as the SunSpec PA, is the entity that approves this CPS and henceforth unless otherwise noted the term PA in this CPS refers to the SunSpec PA

The PA also approves all agreements, including the Certificate Policy (CP), Relying Party (RP) agreements, and Subscriber agreements. The PA will make the approved CP publicly available. This CPS MAY be kept private or made available at the discretion of the PA.

The PA MAY delegate these functions to a committee or specific individuals.

1.3.2 Certification Authority

The CA is the collection of technologies and procedures to issue Certificates under this CPS. The CA Operator is the legal entity responsible for all aspects of the issuance and management of Certificates including:

- Registration,
- Identification and authentication,
- Issuance, and
- Ensuring that all aspects of the CA services and CA operations and infrastructure related to Certificates issued under the SunSpec Alliance CP are performed in accordance with the requirements, representations, and warranties of their CPS.

The following are the different types of CAs in the SunSpec Alliance PKI:

- Root CA (SERCA) is the entity that creates, signs, and issues Intermediate CAs to manufacturers. There is one Root CA.
- Intermediate CAs are the entities that create, sign, and issue Certificates to CAs that are subordinate to it and to Subscribers as well as provide Certificate status information for RPs. For example:
  - Manufacturing Issuing CAs (MICA) is the entity that creates, signs, and issues Certificates to their Subscribers.
  - Manufacturer's CAs (MCA) is the entity that creates, signs, and issues Certificates to vendor specific MICAs, for manufacturers with different production lines.

Note that IEEE 2030.5 allows the direct issuance of Certificates from the SERCA to Subscribers. This is not supported under this CPS.

In the remainder of this document, the term CA only applies to CAs and not RAs. Distinction between Root and Intermediate CAs is only made when the requirements are different for a type of CA.

1.3.3 Registration Authority

The RA is the entity that collects and verifies each Subscriber's identity and the information that is to be entered into the Certificate. The RA interacts with the CA to enter and approve the Subscriber Certificate request information.

1.3.4 Subscribers

A Subscriber is the entity's whose name appears in the subject in a Certificate and who asserts that the Certificate and the keying material will be used in accordance with this CPS. In this CPS, none of the various types of CAs and RAs are referred to as Subscribers.

1.3.5 Relying Parties

Relying Parties("RPs") are recipients of a Certificate who rely on the Certificate and/or the digital signatures verified by the Certificate in the SunSpec Alliance PKI. As used in the remainder of this document, the term RPs only applies to such entities, and not CAs and RAs.

1.3.6 OCSP Responders

No stipulation.

1.3.7 Other Participants

Management Authority (MA)

The MA's role is to provide trust management services to support the SunSpec Alliance PKI in meeting its security goals.

Activities of the MA include:

- Registration of Authorized Applicants.
- Process for collecting and verifying Authorized Applicant identity, information, and agreements.
- Process for MCAs to submit CPSs
- Process for PA to approve CPSs
- Process for Audits

1.4 Certificate Usage

The end entity Certificates issued within the SunSpec Alliance PKI are only to be used by a Subscriber for performing mutual TLS authentication between systems that communicate via the IEEE 2030.5 protocol.

The Root CA is used to validate Certificates issued to Intermediate CAs.

The Intermediate CAs are used to validate CA Certificates that are subordinate to it, and Subscribers Certificates.

All other uses are expressly prohibited.

1.5 Policy Administration

The PA is responsible for all aspects of this CPS and approval of all PKI-related agreements.

Intermediate CAs SHALL submit their CPS and the results of their SunSpec compliance audit to the PA for approval.

All communications regarding this CPS should be directed to pa@SunSpec.org

Section 2 Publication and Repository Response

This section specifies requirements for publication of CA information and Certificates.

2.1 Repositories

The SunSpec Alliance operates a repository that is publicly accessible by RPs.

2.2 Publication of Certificate Information

2.2.1 Publication of Certificate and Certificate Status

The CA Operator publishes all issued Certificates in the SunSpec Repository and is accessible to RPs through an HTTPS URI (HyperText Transmission Protocol Uniform Resource Identifier) references; see https://pki.SunSpec.org.

2.2.2 Publication of CA Information

On behalf of the SunSpec PA, the CA Operator publish information concerning the SunSpec Alliance PKI necessary to support its use and operation. The CP is publicly available on the SunSpec website (see https://pki.SunSpec.org). The CPS will not be published; a redacted version of the CPS will be publicly available from the SunSpec website (see https://pki.SunSpec.org).

2.3 Time or Frequency of Publication

CA Certificates are published within 48 hours of issuance. Subscriber Certificates are published within one hour of issuance.

2.4 Access Controls on Repositories

Information published in the SunSpec Repository is available to RPs. Logical and physical controls are implemented to restrict access and prevent unauthorized modification or deletion of information.

Section 3 Identification and Authentication

This section describes the procedures for Identification and Authentication (I&A) of Certificates issued by CAs in the SunSpec Alliance ecosystem.

3.1 Naming

3.1.1 Types of Names

Within the SunSpec Alliance PKI, an X.501 Distinguished Name (DN) is carried in the Root CA Certificate. The following name forms are used in Certificates issued by the Root CA:

- Root CA: O=SunSpec Alliance, CN=IEEE 2030.5 Root, SN=<XXX>
- Intermediate CA(MCA): C=<Country>, O=<Manufacturing Org>, CN= IEEE 2030.5 MCA, SN=<XXX>
- Intermediate CA(MICA): C=<Country>, O=<Manufacturing Org>, CN= IEEE 2030.5 MICA, SN=<XXX>
- Device: <Empty>

When present, the order of the naming attributes includes (X.500 compliant order): Country (C=), Organization (O=), Common Name (CN=), and Serial Number (SN=).

To allow for rollover of Certificates issued by the Root and Intermediate CA Operator, a monotonically increasing integer is included in the Serial Number after the common name naming attribute to distinguish between CA Certificates issued to the same CA.

The Subject of Device Certificates MUST be empty to be compliant with IEEE 2030.5; the Subject Alternative Name extension contains a *HardwareModuleName* as defined in RFC 4108 to identify the manufacturer.

When the naming element is a *DirectoryString, PrintableString* is used for all Certificates issued.

3.1.2 Meaningfulness

Names in CA Certificates are meaningful and defined unambiguously to identify the entity.

3.1.3 Anonymity of Pseudonymity of Subjects

Names are not anonymous nor a pseudonym.

3.1.4 Rules for Interpreting Various Name Forms

See Section 3.1.1.

3.1.5 Uniqueness of Names

To comply with IEEE 2030.5, the Subject name in Subscriber Certificates is left empty and uniqueness need not enforced.

The PA and CA Operator is responsible for ensuring name uniqueness in Certificates issued by the Root CA.

3.1.6 Recognition, Authentication, and Role of Trademarks

A CA will not knowingly issue a Certificate with a name that a court of competent jurisdiction has determined infringes on the trademark of another without verification that the applicant is authorized to do so on behalf of the trademark owner.

The Subject and Issuer names include the string “IEEE 2030.5” which is trademarked. Permission has been granted by IEEE for this use; contact the PA for further information if required.

Root CA Certificates include the string “SunSpec Alliance” in their name.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

A Certificate Signing Request (CSR), see Section 7.2, is used to demonstrate proof of possession (PoP) of the Private Key that corresponds to a Public Key, the CA will use the Public Key in the CSR to validate the digital signature on the CSR.

3.2.2 Authentication of Organization Identity

The MA ensures the manufacturing organization is authorized the issuance of an Intermediate CA Certificate.

The manufacturing organization is provided credentials by the CA Operator, their identity is authenticated when accessing the portal.

3.2.3 Authentication of Subject Identity

The device manufacturer ensures each end-entity CSR contains a unique hardware serial number. The Intermediate CA ensures the Public Key in the CSR is not associated with a hardware serial in a previously issued Certificate and the Subject field is empty.

3.2.4 Non-verified Subject Information

Information in Certificates is verified; any non-verified information is not included in the Certificate.

3.2.5 Validation of Authority

The identities of Authorized Applicants are verified by the web-based account portal which issues Certificates in bulk and in batch mode to Subscribers. An account is created for a manufacturer only after the following has been confirmed:

- An organization signs the terms and conditions to operate.

3.2.6 Criteria for Interoperation

See Section 1.4.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication of Re-Key and Renewal Requests

Re-key, where a new key pair is generated and bound into a new MCA or MICA Certificate with a new serialNumber component of the SubjectName; see Section 3.2.

Renewal is not supported in the SunSpec Alliance PKI.

3.3.2 Identification and Authentication of Re-Key and Renewal Requests After Revocation

No stipulation.

3.4 Identification and Authentication for Revocation Requests

CA and Subscriber have an indefinite lifetime and can not be revoked.

Section 4 Certificate Life-Cycle Operational Requirements

This section specifies the requirements for Certificate life-cycle management by all PKI entities.

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Authorized Applicants can submit Certificate applications for Subscriber Certificates; see Section 3.2.

4.1.2 Enrollment Process and Responsibilities

Authorized Applicants provide their information to the MA to demonstrate their identity, to demonstrate their authority, and to provide contact information.

The enrollment process for a Certificate Applicant includes, but is not limited to:

- Completing an Authorized Applicant and Certificate Application
- Providing the requested information
- Submitting required payment

See Section 3.2.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The MA verifies and authenticates the identity of each Authorized Applicant, as described in Section 3.2 for initial requests.

The RA performs the activities in Section 3.2 for each Certificate Request.

4.2.2 Approval or Rejection of Certificate Applications

Approval is granted if the applicant's identity has been authenticated as described in Section 3.2 for initial requests and Section 3.3 for initial requests, and payment, if required, has been received. Rejection is based on the inability to successfully authenticate the applicant, not receiving required information from the applicant, or not receiving required payment for the Certificate.

The PA authorizes the issuance of each Intermediate CA Certificate.

The RA rejects Certificate Requests from any source other than an Authorized Applicant in accordance with Section 3.2.

4.2.3 Time to Process Certificate Applications

Requests are processed in a no more than 10 business days.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

The RA accepts Certificate Requests only from Authorized Applicants. RAs verify and authenticate the Applicant of each Certificate request or batch request. If the CA determines the request is acceptable, the CA will issue a properly formed Certificate and provide the Certificate via the Web Portal (or via other means defined by the PA) and publish it to the Repository.

4.3.2 Notification to Applicant of Certificate Issuance

The Authorized Applicant is notified of their CA Certificate issuance after it has been published to the Repository.

Authorized Applicants are notified via email that Certificate Requests have been signed and are available via the web portal.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Acceptance of an Intermediate CA Certificate is deemed accepted if the Root CA Operator and PA receives no complaint within 2 business days of confirmed notification.

Subscriber Certificates are deemed accepted upon retrieval of the Certificate from the web portal.

4.4.2 Publication of the Certificate by the CA

Issued Certificates are posted in the SunSpec Repository; see Section 2.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No other entitles are notified of the issuance of Certificates, unless otherwise requested by the PA.

4.5 Key Pair and Certificate Usage

4.5.1 Private Key Usage

The Root CA, Intermediate CAs, and Subscribers are responsible for protecting their private keys from unauthorized use and access. Private keys are only used as specified in the key usage extension of the corresponding Certificate.

4.5.2 Relying Party Public Key and Certificate Usage

RPs ensure that the public key in a Certificate is used only for appropriate purposes as identified in critical Certificate extensions (see Section 7).

4.6 Certificate Renewal

Renewal is not supported.

4.6.1 Circumstance for Certificate Renewal

No stipulation.

4.6.2 Who May Request Renewal

No Stipulation.

4.6.3 Processing Certificate Renewal Requests

No Stipulation.

4.6.4 Notification of New Certificate Issuance to Applicant

No Stipulation.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No Stipulation.

4.6.6 Publication of the Renewal Certificate by the CA

No Stipulation.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation.

4.7 Certificate Re-key

Re-key is supported for CA Certificates; see Section 3.3.1.

4.7.1 Circumstance for Certificate Re-key

No Stipulation.

4.7.2 Who May Request Certification of a New Public Key

The CA Operator can submit Re-key requests.

4.7.3 Processing Certificate Re-key Requests

See Section 4.2.

4.7.4 Notification of New Certificate Issuance to Applicant

See Section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 Certificate Modification

4.8.1 Circumstance for Modification

Certificate modification is not supported.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Applicant

No stipulation.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

Certificate Revocation and Suspension is prohibited.

4.9.1 Circumstances for Revocation

No stipulation.

4.9.2 Who Can Request Revocation

No stipulation.

4.9.3 Procedure for Revocation Request

No stipulation.

4.9.4 Revocation Request Grace Period

No stipulation.

4.9.5 Time Within which CA Must Process the Revocation Request

No stipulation.

4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation.

4.9.7 CRL Issuance Frequency

No stipulation.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 On-line Revocation/Status Checking Availability

OCSP is not supported.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

Certificate suspension is prohibited.

4.9.14 Who can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Subscriptions SHALL end if there is a termination of service.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Private keys are never escrowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

Section 5 Facility, Management, and Operational Controls

This section specifies the requirements for facility, management, and operational controls in the SunSpec Alliance PKI. The CPS describes the controls and procedures for all the areas identified in this Section.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

The locations and construction of the facility that will house SunSpec Alliance PKI equipment and operations are in accordance with that afforded to sensitive business information. SunSpec CA operations are conducted within a physically protected environment designed to deter, prevent, and detect unauthorized access to such operations.

5.1.2 Physical Access

The physical security requirements pertaining to SunSpec CAs are:

- Ensure no unauthorized access to the hardware is permitted;

- Ensure manual or electronic monitoring for unauthorized intrusion at all times;
- Ensure an access log is maintained and inspected periodically; and
- Require two-person physical access control to both the cryptographic module and computer system.

When not in use:

- Paper containing sensitive plain-text information is stored in secure containers; and
- Media storing the Root CA private key material is deactivated when not in use. The media and the activation information, see Section 6.4, for the Root CA private keys is stored in a secure container.
- Activation data is either memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and not stored with the cryptographic module.

If the facility is not continuously attended, the last people to depart initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated. A security check of the facility housing the CA equipment occurs if the facility is to be left unattended. At a minimum, the check verifies the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”; and for the Root CA, that all equipment other than the repository is shut down);
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized access.

If at any time the Hardware Security Module (HSM) containing a SunSpec CA private key is physically moved permanently from one location to another (i.e., not during normal activation), then:

- The HSM is protected from destruction, unauthorized disclosure, and unauthorized modification;
- The PA approves the movement;
- The PA or authorized representative are present; and
- A record of when the HSM leaves the old location and when the HSM arrives at the new location.

5.1.3 Power and Air Conditioning

The facilities that house the SunSpec CA equipment is supplied with power and air conditioning sufficient to create a reliable operating environment.

5.1.4 Water Exposures

Facilities that house the SunSpec CA equipment are installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors). Moisture detectors are installed in areas susceptible to flooding. CA Operators who have sprinklers for fire control have a contingency plan for recovery should the sprinklers malfunction, or cause water damage outside of the fire area. A description of the CA Operators approach for recovery from water exposure is in the Disaster Recovery Plan as specified in Section 5.7.4.

5.1.5 Fire Prevention and Protection

Facilities that house the SunSpec CA equipment are constructed and equipped, and procedures are implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures meet all local applicable safety regulations. A description of the CA’s approach for recovery from a fire disaster is included in the Disaster Recovery Plan as specified in Section 5.7.4.

5.1.6 Media Storage

The cryptographic modules storing the Root CA private key are stored in a secure container and in a secure room in encrypted form. Media that contains security audit and backup information is stored in a separate location from the Root CA equipment.

The cryptographic modules storing the Intermediate CA Private Key are stored in a secure datacenter cage in encrypted form. Media that contains security audit and backup information is replicated and stored in at least one other location from the Intermediate CA equipment.

5.1.7 Waste Disposal

The CA Operator implements procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing sensitive information.

5.1.8 Off-Site backup

The CA Operator performs system backups, sufficient to recover from system failure, on a periodic schedule.

A backup of the Root CA is stored at an alternate site after each key generation ceremony. Intermediate CAs are replicated to a second HSM in a different online datacenter; the data is synchronized over an encrypted channel.

Backups are performed and stored off-site not less than quarterly or when the Root CA is operational, whichever is less frequent. At least one backup copy is stored at an offsite location (separate from the Root CA equipment). Only the latest backup need be retained. The backup is stored at a site with physical and procedural controls commensurate to that of the operational Root CA system.

The CA Operator performs system backups, sufficient to recover from system failure, on a periodic schedule. Only the latest full backup need be retained. Such backup is replicated and stored in at least one other location (separate from the Intermediate CA equipment) with physical and procedural controls commensurate to that of the operational Intermediate CA system.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted roles are defined in the SunSpec Alliance CP.

The following are the trusted Roles within the SunSpec Alliance PKI:

- Administrator: installs, configures, and maintains SunSpec CAs; configures Certificate profiles and parameters; generates and performs backup of SunSpec CA keys;
- Officer: approves/rejects certification requests;
- Auditor: maintains and reviews audit logs;
- Backup Operator: performs routine system backup and recovery; and
- Trusted Shareholder: 3 of 5 required to access the Private Key within the HSM.

The CA Operator maintains a list of personnel serving in a Trusted Role. This list includes name, role, organization, and email.

Multi-Person control requirements are specified in Section 6.2.2.

5.2.2 Number of Persons Required Per Task

The following CA private key actions require at least “Two-Party Control” when not performed by a secure computer program or process, and require physical access:

- Generation of CA keys;
- Access to CA keys;
- Transport of HSM containing CA keys;
- Destruction of CA Keys;
- Backup of CA keys; and
- Access to backup copies of CA keys.

Where multiparty control is required, at least one of the participants is an Administrator. All participants serve in a trusted role as defined in Section 5.2.1. A person serving in the Auditor Trusted Role is not permitted to serve in any other Trusted Role, and multi-party control will not be achieved using personnel that serve in the Auditor Trusted Role.

5.2.3 Identification and Authentication for Each Role

A person occupying a trusted role has their identity and authorization verified, before being permitted to perform any action for that role or identity.

5.2.4 Roles Requiring Separation of Duties

Individuals do not hold more than one of the Officer, Administrator, Trusted Shareholder, and Auditor roles, but any individual can assume the Backup Operator role. CA software and hardware will identify and authenticate its users, and ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel engaged in the PKI have suitable qualifications and experience as determined by the CA Operator.

5.3.2 Background Check Procedures

The CA Operator uses an approved vetting process for trusted personnel engaged in the PKI.

5.3.3 Training Requirements

Prior to operation, the SunSpec CA Operator will be appropriately trained. Topics include the operation of the CA software and hardware, operational and security procedures, and the stipulations of this policy and local guidance.

5.3.4 Retraining Frequency and Requirements

Refresher training will be provided to the extent and frequency required to ensure the required level of proficiency to perform job responsibilities competently.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

If an unauthorized action takes place, then an appropriate action is taken to ensure disciplinary or other appropriate action is taken. In cases where an unauthorized action brings into question the security of the system, then recovery procedures will be followed; see Section 5.7.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the SunSpec Alliance PKI meet the personnel requirements set forth in Section 5.3.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role is provided to their personnel filling that role.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Any security auditing capabilities of the underlying CA equipment operating system are enabled during installation and operation. At a minimum, the following events are included in the audit log:

- Access to CA equipment (e.g., logon, logout);
- Operating system logon/logoff;
- CA application access;
- CA private key generation;
- CA private key use;
- Certification request;
- Certificate issuance;
- Posting material to a repository;
- Attempts to modify audit data;
- Software and/or configuration updates to the CA and account management;
- Clock Adjustments;
- Anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages; and
- Any known or suspected violations of physical security, suspected or known attempts to attack the CA equipment via network attacks, equipment failures, power outages, network failures, or violations of this CP.

At a minimum, for each auditable event the record includes:

- The type of event;
- The date and time the event occurred;
- A success or failure indication for signing; and
- The identity of the equipment Operator who initiated the action.

Audit logs are generated automatically and periodically backed up.

5.4.2 Frequency of Processing Log

The Root CA audit logs are reviewed at least annually or any time the Root CA is made operational.

The Intermediate CA audit logs are reviewed routinely, but at least quarterly.

The audit log review include searches for anomalous patterns. Action taken as a result of this review is documented and shared with the PA.

Audit log reviews are also conducted when requested by the PA.

5.4.3 Retention Period for Audit Log

Audit logs generated on the CA equipment are kept on the CA equipment until they are moved to an appropriate archive facility. Audit logs are available for a minimum of three months, then are moved to an offsite archive; see Section 5.5.

5.4.4 Protection of Audit Log

The CA Operator procedures ensure that only personnel assigned to a Trusted Role have read access to the audit logs and archive audit logs, which protects against unauthorized viewing, modification, and deletion. The CA Operator procedures ensure audit logs are only be deleted from a system after they have been archived.

5.4.5 Audit Log Backup Procedures

When the Root CA is operational, audit logs are generated and backed up at the end of the key ceremony.

Audit logs for the Intermediate CA are replicated in multiple online datacenters and synchronized over an encrypted channel.

A copy of the audit logs are stored at an offsite location (separate from the Root and Intermediate CA equipment).

5.4.6 Audit Collection System (Internal vs. External)

Automated audit processes are invoked at system (or application) startup, and cease only at system (or application) shutdown.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Personnel in Trusted Roles will routinely assess the Intermediate CA system and its components for anomalous events and malicious activity at least quarterly.

Vulnerability assessments are also conducted when requested by the PA.

5.5 Records Archival

5.5.1 Types of Events Archived

Archive records are detailed enough to establish the validity of a signature and of the operation of the PKI. The following are recorded at a minimum:

- CA accreditation;
- CA equipment certification, if any;
- Updates to the CP;
- Updates to the CPS;
- Subscriber agreements;
- System equipment configuration;
- Modification and updates to system or configuration;
- Contractual obligations;
- Key Signing Ceremony video footage;
- Identity authentication data from Section 3.1.9;
- Documentation of receipt and acceptance of Certificates;
- All Certificate requests for which the authorization failed;
- All Certificates issued;
- Audit logs from Section 5.4.1;
- Remedial action taken as a result of violations of physical security;
- Violations of CP;
- Violations of CPS;
- Other data or applications to verify archive contents; and
- Documentation required by compliance auditors; see Section 8.

5.5.2 Retention Period for Archive

Archive data is maintained for a minimum of the period of validity three (3) years.

5.5.3 Protection of Archive

Archive data has adequate physical protection to ensure there is no unauthorized disclosure, modification, or destruction. Archive media is stored in a safe, secure storage facility separate from the CA equipment itself.

5.5.4 Archive Backup Procedures

The archive facility support backups.

5.5.5 Requirements for Time-Stamping of Records

The archive data indicates the date on which the archive was created.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

The PA or its authorized representatives are granted timely access to archive information when requested.

5.6 Key Changeover

Certificates in the SunSpec Alliance PKI are not renewed; see Section 4.6.

Certificates in the SunSpec Alliance PKI may be re-keyed; see Section 4.7.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

In the event of suspected compromise of a CA, the CA Operator will notify the PA and will investigate to determine the nature and the degree of damage. Action taken as a result of this review are documented and shared with the PA. The PA will authorize any action taken, in advance, by the CA Operator.

If an MCA or MICA is suspected of being compromised or is actually compromised, then new keys are generated and a new Certificate is issued to replace the old Certificate after PA approval. Compromised CA private keys are not used to sign new Certificates.

The CA Operator has an Incident Response Plan and Disaster Recovery Plan.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

Backup or Archived data is used when computing resources, software, and data are corrupted.

The CA Operator responds to computing resources, software, and/or data corruption as follows:

- Notify the PA
- Ensure the system's integrity has been restored and determine the extent of lost data since the last point of backup
- Once CA operations have been reestablished the PA is notified.

5.7.3 CA Private Key Compromise Procedures

See Section 5.7.1.

5.7.4 Business Continuity Capabilities After a Disaster

In the case of a disaster in which the CA equipment is damaged and inoperative, CA operations are established as quickly as reasonably possible.

The CA Operator maintains a Disaster Recovery Plan. The Disaster Recovery Plan identifies the management and operations procedures to mitigate risks to facilities, systems, networks, and application controls. It identifies procedures for annual testing of processes to restore service, individuals on call for management, response and recovery activities, and the order of restoral of equipment and services.

5.8 CA Termination

In the event a CA terminates, or ceases operation, the CA operator destroys the CA private keys, and any backup copies after approval by the PA.

Prior to ceasing operations, the PA SHALL advise all Subscribers that the CA operation has terminated.

Section 6 Technical Security Controls

This section specifies the Root and Intermediate CA requirements for technical security controls to securely perform the functions of key generation, subject authentication, Certificate issuance, and Certificate revocation.

6.1 Key Pair Generation and Installation

The private key associated with the Root CA Certificate is generated offline in the removable HSM.

The Private key associated with an Intermediate CA Certificate is available in a minimum of two active production servers' HSM which are geographically separated by at least one time zone and not less than 100 miles.

6.1.1 Key Pair Generation

Root and Intermediate CA keys are generated in FIPS 140-2, or later, validated cryptographic module. The HSM meets security level 3 or above and keys are generated as part of a multiparty operation. Promptly after generation, the encrypted private keys are transferred to an HSM at a geographically separate location.

Subscriber key pair generation is performed by an Authorized Applicant on behalf of a Subscriber.

6.1.2 Private Key Delivery to Subject

No stipulation.

6.1.3 Public Key Delivery to Certificate Issuer

The public key and identity are delivered securely to the Root or Intermediate CA as part of the CSR; see Section 7.

6.1.4 CA Public Key Delivery to Relying Parties

CA Certificates are posted in the Repository; see Section 2.

6.1.5 Key Sizes

CAs use Elliptic Curve Digital Signature Algorithm (ECDSA) with the NIST P-256 and SHA-256 to sign Certificates.

6.1.6 Public Key Parameters Generation and Quality Checking

See FIPS 186-4 for the key generation requirements for ECDSA with the NIST P-256 elliptic curve.

6.1.7 Key Usage Purposes (as per X.509v3 key usage field)

See Section 7.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is FIPS 140-2, or later.

6.2.2 Private Key Multi-Person Control

Use of the Root CA private key requires action by multiple persons as set forth in Section 5.2.2.

Generation, transport, and backup of the Intermediate CA private key requires action by multiple persons; see Section 5.2.2.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

CA private keys are backed up under multi-person control, as required in Section 5.2.2.

After generation of the Root CA private key is stored at the primary Root CA location, and a backup copy of the Private Key is moved to the secondary location as soon as practical which is expected to occur within one week. Accountability is maintained for all copies of the Private Key.

The encrypted Intermediate CA private keys are transferred to an HSM at a geographically separate colo-location datacenter promptly after generation.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA private keys never leave the cryptographic module in an unencrypted form; see Section 6.2.4.

6.2.7 Private Key Storage on Cryptographic Module

See Section 6.2.1.

6.2.8 Method of Activating Private Keys

Activation of the Root CA signing key requires multiparty control, as specified in Section 5.2.2. The Root CA private key media are not left unattended when active.

No stipulation for activating Intermediate CA signing keys.

6.2.9 Methods of Deactivating Private Keys

The Root CA private keys are deactivated and the media holding the Root CA private key are stored in a secure container; see Section 5.1.6. Root CA private keys are deactivated and stored in encrypted form in a secure room when not in use; see Section 5.1.6. These actions require multiparty control, as specified in Section 5 2.2.

No stipulation for deactivating Intermediate CA signing keys.

6.2.10 Method of Destroying Private Key

Private keys are destroyed when they are no longer needed. Root CA private keys are destroyed under control of at least three people holding a Trusted Role; see Section 5.2.2. Intermediate CA private keys are destroyed under control of at least three people holding a Trusted Role; see Section 5.2.2.

The method for destroying private keys is chosen to minimize the impact on CA operations. The CA Operator will perform an assessment and will obtain PA approval prior to taking actions.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public keys are archived as part of the Certificate archival.

6.3.2 Certificate Operational Periods/Key Usage Periods

Certificate validity periods are defined in the Certificate Profile; see Section 7

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data generation and installation for CA private keys use methods that protect the activation data to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.4.2 Activation Data Protection

Activation Data to invoke Private Keys will use methods that protect the Activation Data to the extent necessary to mitigate against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such Private Keys by a combination of cryptographic and physical access control mechanisms.

The protection mechanism for the Root CA includes an entry of a PIN, and an entry of an incorrect PIN terminates the application.

6.4.3 Other Aspects of Activation Data

Before the Root CA Private Key Activation Data is entered, the media storing the Root CA Private Key is retrieved from the locked container under control of at least two people holding a Trusted Roles.

No stipulation for the Intermediate CAs.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

For the Root CA, Intermediate CA, and Web Portal the computer security functions listed below are required. These functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards. The SunSpec Alliance PKI and its ancillary parts include the following functionality:

- Require authenticated logins;
- Provide Discretionary Access Control;
- Provide a security audit capability;
- Restrict access control to Trusted Roles;
- Enforce separation of Trusted Roles;

- Require identification and authentication;
- Only the applications needed for the Root CA, Intermediate CA, and Web Portal will be permitted;
- Require use of cryptography for session communications and database security;
- Archive Root CA, Intermediate CA, and Web Portal history and audit data;
- Require a transmission mechanism for encrypted private keys between HSMs; and
- Require a recovery mechanism for keys, CA system, and CA application.

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

The System Development Controls for the Root CA, Intermediate CA, and Web Portal are as follows:

- For commercial off-the-shelf software, the software are designed and developed under a formal, documented development methodology.
- For hardware and software developed specifically for the SunSpec Alliance PKI, the applicant demonstrates that security requirements were achieved through a combination of software development methodology as well as software verification and validation.
- Where open source software has been utilized, the CA Operator demonstrates that security requirements were achieved through software verification and validation as well as structured development/life-cycle management.
- Hardware and software procured to operate the SunSpec Alliance PKI is purchased and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- The software on these systems are dedicated to the SunSpec Alliance PKI. There are no applications other than those needed for the SunSpec Alliance PKI; hardware devices, network connections, or component software installed which are not part of these applications.
- Proper care is taken to prevent malicious software from being loaded onto SunSpec Alliance PKI equipment. Hardware and software is scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates are purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a manner defined in this CPS.
- Any code provided to the open source community does not disclose security relevant information.

6.6.2 Security Management Controls

The configuration of the Root CA, Intermediate CA, and Web Portal systems as well as any modifications and upgrades are documented and controlled. There is a mechanism for detecting unauthorized modification to software or configuration of these systems. A formal configuration management methodology is used for installation and ongoing maintenance of these systems.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

The Root CA, Intermediate CA, and Web Portal is protected to prevent unauthorized access, tampering, and denial-of-service. Communications of sensitive information is protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

The Root CA is offline.

The Intermediate CAs and Web Portal are online; see Section 4.9.9.

The data centers hosting the Intermediate CA services provided managed bandwidth services with additional controls against Distributed DoS (DDoS) attacks. Additionally, the data centers provide dedicated replication circuits between Intermediate CA facilities.

Firewalls are employed as the demarcation between Wide Area Network (WAN) and Intermediate CA Local Area Network (LAN) services. This includes policies limiting access to Intermediate CA services to externally facing web portal, user interfaces, and load balancing.

Audit Data for application and services outside of the facility leverages an automated security platform that is monitored by the CA Operator.

6.8 Timestamping

Times asserted in Certificates are accurate to within three minutes. Electronic or manual procedures are used to maintain system time. Clock adjustments are auditable events; see Section 5.4.1. The Network Time Protocol (NTP) is used to synchronize computer clock time on the system. The system will leverage the National Institute of Standards and Technology (NIST) Internet Time Servers for managing system time (IP address examples 129.6.15.28 or 129.6.15.29). Clock adjustments are auditable events; see Section 5.4.1.

Section 7 Certificate Profiles

This section specifies the requirements for the Certificate formats.

7.1 Certificate Profiles

Certificates issued in the SunSpec Alliance PKI adhere to the X.509 v3 Certificate profile documented in RFC 5280; see SunSpec Alliance PKI Profiles.

7.2 PKCS#10 Profile

See SunSpec Alliance PKI Profiles.

Section 8 Compliance Audit and Other Assessments

This section specifies the requirements for audits.

8.1 Frequency of Audit or Assessments

The SunSpec Alliance PKI is subject to a compliance audit at the request of the SunSpec Alliance PA.

8.2 Identity and Qualifications of Assessor

The auditor demonstrates competence in the field of compliance audits. The PA approves the compliance auditor for the SunSpec Alliance PKI. The PA provides access to the auditor.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor is either a private firm, that is independent from the entity being audited, or it is sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation.

The PA determines whether a compliance auditor meets this requirement.

8.4 Topics Covered By Assessment

The compliance auditor verifies that the CA Operator is implementing all provisions of the SunSpec Alliance CP and this CPS, as approved by the PA.

8.5 Actions Taken As A Result of Deficiency

Any discrepancies between how the SunSpec Alliance PKI is designed to or is being operated or maintained and the requirements of this CPS will result in the compliance auditor documenting the discrepancy.

8.6 Communication of Results

If the compliance Auditor pursuant to this Section 8 identifies any noncompliance with applicable law, the SunSpec Alliance CP, this CPS, or in any other contractual obligations related to the SunSpec Alliance PKI, then the Auditor will promptly report such noncompliance to the CA Operator, as applicable. The CA Operator, as applicable, will develop a plan to cure such noncompliance, subject to the approval of the PA.

Section 9 Other Business and Legal Matters

This section specifies requirements on general business and legal matters.

9.1 Fees

9.1.1 Certificate Issuance/Renewal Fees

The fee schedule is approved by the SunSpec Alliance.

9.1.2 Certificate Access Fees

The fee schedule, if any, MUST be approved by the SunSpec Alliance. The fee schedule is included in Relying Party Agreements.

9.1.3 Revocation or Status Information Access Fee

No stipulation.

9.1.4 Fees for other Services

All fees are approved by the SunSpec Alliance.

9.1.5 Refund Policy

Any refund policy is approved by the SunSpec Alliance.

9.2 Financial Responsibility

The CA Operator has assets and resources that ensure an ability to meet all operational requirements as a CA on an uninterrupted basis and to pay damages that could reasonably occur as a result of CA operations. The levels of such assets and resources is reasonably acceptable to the PA.

9.2.1 Insurance Coverage

The CA Operator has adequate insurance coverage. The coverage amount is approved by the SunSpec Alliance.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance/warranty Coverage for Subscribers

No Stipulation.

9.3 Confidentiality of Business Information

Sensitive and confidential information will be exchanged and provided under this CPS. Written confidential information is adequately marked in writing as confidential. Oral confidential information is identified as confidential. In addition, any information that, by its nature is reasonably understood to be confidential, treated as confidential.

9.3.1 Scope of Confidential Information

Confidential Information means all information in written or oral form that the disclosing party identifies as confidential, and any trade secret or other proprietary information that the recipient knows or reasonably ought to know to be treated as confidential.

9.3.2 Information Not Within the Scope of Confidential Information

Information that is not Confidential Information includes information that is generally known to the public or properly known by the receiving party at the time of disclosure and other typical exceptions.

The following information is not considered confidential:

- Information included in Certificates,
- Information contained in the SunSpec Alliance CP,
- Information that, at the time of disclosure or thereafter, is generally available to or known by the public (other than as a result of disclosure in violation of the SunSpec Alliance CP and this CPS), or
- Information that, at the time of disclosure, was rightfully in the possession of the receiving party.

9.3.3 Responsibility to Protect Confidential Information

The PA, CAs Operators, Subscribers, and Auditors protect Confidential Information from unauthorized disclosure and treat such Confidential Information with the same degree of care and security as the entity treats its own most confidential information.

9.4 Privacy of Personal Information

It is the responsibility of all parties to ensure privacy of personal information under their control. Personal information is not included in any Certificate issued by the Root CA or Intermediate CA. The Root CA and Intermediate CA Operators retain information as part of certification request, which is subsequently logged and later archived.

The PA, MA, and CA Operator retains business contact information about the Authorized Applicant. If a party collects, transmits or stores Personal Information, its practices will comply with all applicable laws.

9.4.1 Privacy Plan

All parties ensure their privacy plan describes the process to manage relevant information.

9.4.2 Information Treated as Private

An Authorized Applicant's business contact information, which at a minimum includes name, organizational affiliation, email address, and phone number is treated as Personal Information.

9.4.3 Information Not Deemed Private

The SunSpec Alliance CP and issued Certificates are not considered private information.

9.4.4 Responsibility to Protect Private Information

The Root CA, Intermediate CA, and Subscribers will protect private information when it is within their control.

9.4.5 Notice and Consent to use Private Information

Notice and consent practices regarding private information complies with any applicable law.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

Disclosure in response to a valid judicial or administrative order is permitted.

9.4.7 Other Information Disclosure Circumstances

Except as required for operation of the PKI system, as expressly permitted or required under this CPS, or any agreements between the PA and Intermediate CA, or as permitted under applicable law, no private information will be disclosed without the express written consent of the party to which that private information pertains.

9.5 Intellectual Property Rights

The SunSpec Alliance CP, this CPS, and all Certificates issued by the Root CA or Intermediate CA and all documentation on the SunSpec Alliance PKI are the property of the SunSpec Alliance.

No party will use any intellectual property of SunSpec Alliance, including, without limitation, any trademark, copyright, trade secret or other proprietary right of the SunSpec Alliance, unless the SunSpec Alliance has licensed that use.

No party will infringe the intellectual property rights of any third party participant in the SunSpec Alliance PKI. Without limitation, except as the SunSpec Alliance can expressly authorize in writing, it is prohibited to:

- Reverse engineer, translate, disassemble, decompile the whole or any part of any software or system or any part therefore;
- Attempt to access any software source code embedded in or operating using any system;
- Attempt to access any proprietary or protected information embedded in or operating using any system, including without limitation, any cryptographic access data or keying material of any kind;
- Remove or alter any trademark or any copyright or other proprietary notice on any software, system or any other materials;
- Distribute, create derivative works of or modify any materials, software or system or any part thereof in any way, or use, copy, duplicate or display same on a commercial or development basis.
- Provide any service using a Certificate provided under the SunSpec Alliance CP except as authorized and provided in the SunSpec Alliance CP and this approved CPS.

These restrictions can not be construed in a manner that would violate any applicable law.

9.6 Representations and Warranties

The obligations described below pertain to the PKI Participants. The obligations applying to CAs pertain to their activities as issuers of Certificates.

9.6.1 PA / SunSpec

The SunSpec Alliance and the PA make no representations and disclaim all warranties except as noted in Section 9.6.2, however characterized, to the maximum extent permitted by law.

9.6.2 CA Representations and Warranties

The SunSpec Alliance warrants that:

- There are no material misrepresentations of fact in the Certificate known to be or originating from the PA or a CA Operator;

- There are no errors in the information in the Certificate that were introduced by the PA or CA as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate;
- The Certificates issued meet all material requirements of the SunSpec Alliance CP and this CPS;
- Revocation services and use of the Repository conform to all material requirements of the SunSpec Alliance CP and this CPS in all material aspects; and
- It will perform all services in a professional and workmanlike manner and in conformity with standards that equal or exceed industry norms for the services that it is providing.

9.6.3 RA Representations and Warranties

No stipulation.

9.6.4 Subscriber Representations and Warranties

Subscribers use Certificates in accordance with the SunSpec Alliance CP and this CPS; see Section 1.4. Subscriber Agreements stipulate additional requirements for Subscriber representations and warranties.

9.6.5 Relying Party Representations and Warranties

RPs use the Root CA and Intermediate CA Certificate in accordance with the SunSpec Alliance CP and this CPS; see Section 1.4. Relying Party Agreements stipulate additional requirements for RP representations and warranties.

9.6.6 Representations and Warranties of Other Participants

Other Participant agreements will stipulate representations and warranties.

9.7 Disclaimers of Warranties

Except for the representations and warranties contained herein, the SunSpec Alliance and the PA disclaim all warranties. No disclaimer contradicts a required express warranty.

9.8 Limitations of Liability

The limitations of liability are approved by the PA. Limitations of liability are stipulated in Relying Party Agreements.

9.9 Indemnities

The indemnities are approved by the PA.

9.10 Term and Termination

9.10.1 Term

The SunSpec Alliance CP and this CPS becomes effective when the PA approves it and continues until the PA terminates it.

9.10.2 Termination

Termination of this CPS is at the discretion of the PA. This CPS remains in force until such time as the PA terminates it.

9.10.3 Effect of Termination and Survival

9.10.3.1 CPS

The provisions found in Section 5.8 of this CPS shall survive termination.

9.10.3.2 Other Agreements

The provisions found in the following sections shall survive termination: 5.5 (to the extent required pursuant to Sections 5.5.2 and 9.10.3.1), 9.3, 9.4, 9.5, 9.7, 9.8, 9.9, and 9.10.3.1.

9.11 Individual Notices and Communications With Participants

The provisions found in Section 5.8 of this CPS shall survive termination.

9.12 Amendments

9.12.1 Procedure for Amendment

9.12.1.1 CP

No stipulation.

9.12.1.2 CPS and Participant Agreements

The PA will approve amendments to the SunSpec Alliance PKI CPS and Participant agreements.

9.12.2 Notification Mechanism and Period

Any subsequent changes are made publicly available as soon as reasonably possible.

9.12.3 Circumstances Under Which OID Must Be Changed

If the PA determines that an amendment necessitates a change in an OID, then the revised version of the SunSpec Alliance CP will identify that a new OID is required and will specify a revised OID.

9.13 Dispute Resolution Provisions

Any dispute arising with respect to this CPS or any Certificates issued under this CPS is addressed by the PA. All determinations of the PA are final.

9.14 Governing Law

Subject to any limits appearing in applicable law, the federal laws of the United States and/or the laws of the Commonwealth of Delaware shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in the Commonwealth of Delaware. This governing law provision applies only to this CPS. Agreements incorporating the CPS by reference may have their own governing law provisions, provided that this Section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the terms of such other agreements.

9.15 Compliance with Applicable Law

This CPS complies with the laws of the Commonwealth of Delaware and the United States of America.

9.16 Miscellaneous Provisions

9.16.1 Document Incorporated into CPS

The SunSpec Alliance PKI Profiles are incorporated into this CPS by reference.

9.16.2 Entire Agreement

This Agreement contains the entire understanding of the Parties in respect of its subject matter and supersedes all prior agreements and understandings between the Parties with respect to such subject matter. Each representation and warranty contained in this Agreement is independent of each other representation and warranty, and each shall survive Closing notwithstanding any investigation, audit or review made at any time by any Party to this Agreement and notwithstanding the delivery of any documents, Schedules or Certificates pursuant to this Agreement.

9.16.3 Assignment

No party to this Agreement may assign its rights or delegate its duties under this Agreement without the prior written consent of the SunSpec Alliance. Any attempted assigned or delegation without such consent will be void.

9.16.4 Severability

A determination that any provision of this CPS is invalid or unenforceable shall not affect the validity or enforceability of any other provision hereof. If it shall be determined by any court or applicable governmental or regulatory authority that any provision of this Agreement is invalid for any reason, such provision shall be considered to be reduced to the extent required to cure such invalidity.

9.16.5 Waiver

This CPS may not be modified, amended, supplemented, cancelled or discharged, except by a written instrument executed by each of the Parties. No failure to exercise, and no delay in exercising, any right, power or privilege under this Agreement shall operate as a waiver, nor shall any single or partial exercise of any right, power or privilege preclude the exercise of any other right, power or privilege. No waiver of any breach of any provision shall be deemed to be a waiver of any preceding or succeeding breach of the same or any other provision, nor shall any waiver be implied from any course of dealing between the Parties. No extension of time for performance of any obligations or other acts under this or any other related agreement shall be deemed to be an extension of the time for performance of any other obligations or any other acts.

9.16.6 Attorneys' Fees

In the event that any arbitration, suit or action is instituted to enforce any provision in this CPS, the prevailing Party in such dispute shall be entitled to recover from the losing Party all fees, costs and expenses of enforcing any right of such prevailing Party under or with respect to this CPS, including without limitation, such reasonable fees and expenses of attorneys and accountants, which shall include, without limitation, all reasonable fees and costs.

9.17 Force Majeure

To the extent permitted by applicable law, Relying Party Agreements shall include a force majeure clause protecting SunSpec and CA Operators for a delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by an event beyond their control.

9.18 Arbitration

Any dispute, controversy or claim arising under or related to this CPS, or the SunSpec Alliance CP, regardless of the legal theory upon which it is based, will be settled by final, binding arbitration pursuant to the U.S. Federal Arbitration Act, 9 U.S.C. Section 1 et seq., in accordance with the American Arbitration Association Commercial Arbitration Rules. Nothing herein will, however, prohibit a Party from seeking temporary or preliminary injunctive relief in a court of competent jurisdiction. In any arbitration, the number of arbitrators will be three. Each Party shall have the right to appoint one arbitrator, who will together appoint a third neutral arbitrator within thirty (30) days after the appointment of the last party-designated arbitrator. All arbitration proceedings will take place in San Jose, California. The arbitrators will be entitled to award monetary and equitable relief, including specific performance and other injunctive relief; provided, however, that only damages allowed pursuant to this CPS may be awarded. Except as otherwise expressly provided in this Section 9.18, each Party will bear the expenses of its own counsel and will jointly bear the expenses of the arbitrators. The arbitrators will allocate the remaining costs of the arbitration proceeding. The Parties agree that the arbitrators will include, as an item of damages, the costs of arbitration, including reasonable legal fees and expenses, incurred by the prevailing Party if the arbitrators determine that either (a) the non-prevailing Party did not act in good faith when disputing its liability hereunder to the prevailing Party or when initiating a claim against the prevailing Party; or (b) the prevailing Party has had to resort to arbitration with respect to a substantially similar claim more than twice in any thirty-six (36) month period. If the court directs or otherwise requires compliance herewith, then all costs and expenses, including reasonable attorneys' fees incurred by the Party requesting such compliance, will be reimbursed by the non-complying Party to the requesting Party.

Section 10 Bibliography

FIPS 140-2, “Security Requirements for Cryptographic Modules”, March 2019.

FIPS 186-4, “Digital Signature Standard”, July 2013.

IEEE Std 2030.5-2018, “IEEE Standard for Smart Energy Profile Application Protocol”, May 2018

RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels”, March 1997.

RFC 3647, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, November 2003.

RFC 4108, “Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages”, August 2005

RFC 5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, May 2008.

RFC 6960, “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”, June 2013.

RFC 8174, “Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words”, May 2017.

Section 11 Acronyms & Abbreviations

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DER	Distributed Energy Resource
DN	Distinguished Name
DoS	Denial of Service
FIPS	Federal Processing Information Standard
HSM	Hardware Security Module
HTTP	Hypertext Transmission Protocol
I&A	Identification and Authentication
IETF	Internet Engineering Task Force
MCA	Manufacturer's Certificate Authority
MICA	Manufacturing Issuing Certificate Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure using X.509
RP	Relying Party
RA	Registration Authority
SERCA	Smart Energy Root Certificate Authority
TA	Trust Anchor
URI	Uniform Resource Identifier

Section 12 Glossary

Access	The ability and means to communicate with or otherwise interact with a system to use system resources either to handle information or to gain knowledge of the information the system contains.
Access Control	Protection of system resources against unauthorized access.
Activation Data	Secret data, other than keys, that is required to access a cryptographic module.
Applicant	The entity that applies to a CA for a Certificate, but before the Certificate issuance procedure is completed.
Archive	Long-term, physically separate storage.
Archive Facility	The offsite facility used by a CA to store archive data.
Administrator	A trusted role that installs, configures, and maintains the CA.
Audit	An independent review and examination of a system's records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Auditor	A trusted role that performs the Audit.
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
Authenticate	Verify (i.e., establish the truth of) an attribute value claimed by or for a system entity or system resource.
Authentication	The process of verifying a claim that a system entity or system resource has a certain attribute value.
Authorized Applicant	An Authorized Applicant is a company that has had its products certified, by the SunSpec Alliance, to the IEEE 2030.5/CSIP standard and profile.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Backup Facility	The offsite facility used by a CA to store backup data.
Certificate	A digital representation of information which at least (1) identifies the CA issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the CA issuing it.
Certificate Validation	An act or process by which a Certificate user establishes that the assertions made by a digital Certificate can be trusted.
CA (Certification Authority)	The CA is responsible for all aspects of the issuance and management of a Certificate including: registration, identification and authentication, issuance, and ensuring that all aspects of the CA services and CA operations and infrastructure related to Certificates issued under the CP are performed in accordance with the requirements, representations, and warranties of their CPS.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a CA to perform Certificate issuance and revocation.
CA Operator	The legal entity responsible for all aspects of the issuance and management of a Certificate. In this CPS, there are two types: (1) Root CA Operator, (2)

	Intermediate CA Operator. The Root CA Operator and Intermediate CA Operator in this CPS is SecureG.
CP (Certificate Policy)	A CP is a specialized form of administrative policy tuned to electronic transactions performed during Certificate management. A CP addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of Certificates. Indirectly, a CP can also govern the transactions conducted using a communications system protected by a Certificate-based security system. By controlling critical Certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
CPS (Certification Practice Statement)	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing Certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
CRL (Certificate Revocation List)	A list maintained by a CA of the Certificates that it has issued that are revoked prior to their stated expiration date.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module; from FIPS140-2, or later.
CSR (Certificate Signature Request)	A digitally signed message associates the subject, the public key, and any attributes together and provided to the CA during the certification request process,
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a RP can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital Certificate; and (2) whether the message has been altered since the transformation was made.
Integrity	Protection against unauthorized modification or destruction of information.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and that may have one or more CAs subordinate to itself and may have issued Subscriber Certificates.
Issuance (of a Certificate or a CRL)	Generate and sign a digital Certificate or a CRL and, usually, distribute it and make it available to potential RPs.
Key Escrow	A deposit of the private key of a Subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the Subscriber, the terms of which require one or more agents to hold the Subscriber's private key for the benefit of the Subscriber, an employer, or other party, upon provisions set forth in the agreement.

Key Pair	Two mathematically related keys having the properties that (1) one (public) key can be used to encrypt a message that can only be decrypted using the other (private) key, and (2) even knowing the public key, it is computationally infeasible to discover the private key.
MCA	An Intermediate Certificate issued by the Root CA for manufacturers that might require Intermediate CA Certificates per-department to handle different production lines. The MCA issues MICA Certificates to different departments within the same organization.
MICA	An Intermediate CA Certificate for manufacturers that do not require an Intermediate CA Certificate per-department. The MICA issues Certificates to Subscribers.
Modification (of a Certificate)	The act or process by which data items bound in an existing Certificate, especially authorizations granted to the subject, are changed by issuing a new Certificate.
Non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.
OCSP (Online Certificate Status Protocol) server	A server that process OCSP requests and returns OCSP responses on behalf of a CA.
OID (Object Identifier)	A specialized formatted number that is registered with an internationally recognized standards organization to reference a specific object.
PA (Policy Authority)	The individual or group that is responsible for the creation and maintenance of CPs and CPSes, and for ensuring that all PKI components (e.g., CAs, RAs) are audited and operated in compliance with the entity PKI CP. The PA evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI CPs.
Privacy	Restricting access to Subscriber or RP information in accordance with Federal law.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is normally made publicly available in the form of a Certificate.
PKI (Public Key Infrastructure)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering Certificates and public/private key pairs, including the ability to issue, maintain, and revoke Certificates.
RA (Registration Authority)	An entity that is responsible for identification and authentication of Certificate subjects, but that does not sign or issue Certificates (i.e., a RA is delegated certain tasks on behalf of an authorized CA).
Re-key (a Certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new Certificate that contains the new public key.
RP (Relying Party)	An entity that relies on the validity of information signed by a digital Certificate.

RP Agreement	An agreement between a CA and relying party that typically establishes the rights and obligations between those parties regarding the verification of digital signatures or other uses of Certificates.
Renew (a Certificate)	The act or process of extending the validity of the data binding asserted by a Certificate by issuing a new Certificate.
Repository	A database containing information and data relating to Certificates as specified in this CP.
Revoke (a Certificate)	To prematurely end the operational period of a Certificate effective at a specific date and time.
Root CA	An established point of trust from which a Certificate user begins the validation of a certification path.
SERCA	See Root CA.
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a Certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the Certificate, and (3) does not itself issue Certificates to another party.
Subscriber Agreement	An agreement between a CA and a subscriber that establishes the right and obligations of the parties regarding the issuance and management of Certificates.
SunSpec Repository	See Repository
Trust Anchor	See Root CA.
Trusted Role	Entity who performs CA-related functions that can introduce security problems if not carried out properly, whether accidentally or maliciously, that would adversely affect the basis of trust for all RPs. In this CP, there are four: (1) Administrator, (2) Officer, (3) Auditor, (4) Backup Operator.
Two-Party Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements.
Web Portal	A web interface which the Authorized Applicant uses to order Certificates for the Subscriber.