SunSpec Official PKI Provider Request for Proposal

September 18, 2018

Abstract This Request for Proposal is an offer to qualified Public Key Infrastructure (PKI) service partners to engage with the SunSpec Alliance to establish a high quality digital certificate provisioning service for the Distributed Energy Resources (DER) industry. The objective of this program is to increase stakeholder confidence in DER communication solutions, including those enabling smart inverters, smart PV modules, EV charging, and energy storage. Market demand for this service is immediate. The program's initial focus is to enable California Rule 21 compliance and the rollout of IEEE 1547-2018.

Legal Disclaimer

NOTHING CONTAINED IN THIS DOCUMENT SHALL BE DEEMED AS GRANTING YOU ANY KIND OF LICENSE IN ITS CONTENT, EITHER EXPRESSLY OR IMPLIEDLY, OR TO ANY INTELLECTUAL PROPERTY OWNED OR CONTROLLED BY ANY OF THE AUTHORS OR DEVELOPERS OF THIS DOCUMENT. THE INFORMATION CONTAINED HEREIN IS PROVIDED ON AN "AS IS" BASIS, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE AUTHORS AND DEVELOPERS OF THIS DOCUMENT HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, STATUTORY OR AT COMMON LAW, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE SUNSPEC ALLIANCE FURTHER DISCLAIMS ANY AND ALL WARRANTIES OF NON-INFRINGEMENT, ACCURACY OR LACK OF VIRUSES.

Trademarks and Copyrights

Table of Contents

Definitions and Abbreviations

Acronym	Meaning
CA	Certificate Authority
CSIP	Common Smart Inverter Profile
CP	Certificate Policy
CPS	Certificate Policy Statement
CRA	Certificate Requesting Account
DER	Distributed Energy Resources
ECC	Elliptic Curve Cryptography
EV	Electric Vehicle
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Standards Organization
PICS	Protocol Implementation Conformance Statement
PKI	Public Key Infrastructure
PV	Photovoltaic
RA	Registration Authority
RFP	Request For Proposal
TLS	Transport Layer Security

1. Introduction and Background

Distributed Energy Resources (DER), including solar, energy storage, and electric vehicle (EV) charging infrastructure, are revolutionizing how electricity is generated and consumed across the globe. California is leading the energy revolution and has policies in place that require 100% of energy generated in California come from renewable sources by the year 2045. A significant portion of this capacity will come from DER installed on homes, commercial buildings, and campuses.

To achieve state DER deployment goals, the state of California modified its interconnection rule (California Rule 21) to require that all systems installed after February 22, 2019 be capable of communicating with the host utility. The default DER-to-utility communication standard is IEEE 2030.5. Configuration options stipulated the Common Smart Inverter Profile (CSIP) document refine California requirements. California Rule 21 states that products using the communication standard shall be evaluated against the SunSpec Alliance compliance criteria.

Approximately 250,000 DER systems per year will require SunSpec Certification to the IEEE 2030.5/CSIP standard in California by 2020. The IEEE 2030.5 standard includes a requirement for Transport Level Security (TLS), implying the use of cryptographic keys installed on communication devices. Other standards specified by U.S. federal regulations (Energy Act of 2005 and the IEEE 1547-2018 standard) similarly require cryptographic keys. Millions of systems must comply to these standards. To address these critical needs, the SunSpec Alliance is seeking to partner with a qualified provider to deliver Public Key Infrastructure (PKI) services.

2. RFP Timeline and Submission Requirements

To apply, companies should respond to the RFP Questionnaire in Section 0 and email your response, in PDF format, to certification@SunSpec.org . The deadline for submission is October 15, 2018.

Applicants meeting minimum requirements will be notified by October 22, 2018 and asked to meet with SunSpec to discuss their bids. The winning bidder will be notified during the week of November 5, 2018.

2.1 General Conditions

This RFP is not an offer to enter into a contract. Unless stated otherwise in writing, any and all costs associated with response to this RFP are the responsibility of the responder and are not billable to the SunSpec Alliance. Submitted proposals must include project and budget breakdowns as well as estimated schedules. The proposal must also include ongoing costs of maintenance and operation of the PKI service.

2.2 Proposal Content

To respond to this RFP request, please provide a concise response to each of the items in the RFP Questionnaire found in Section 0.

3. Participartion Requirements

To qualify for participation in the program, applicants must demonstrate:

- Company is experienced with PKI programs such as the one offered by SunSpec.
- Company has record keeping, security, and confidentiality procedures that are adequate.
- Company PKI resources and infrastructure are available to implement the SunSpec program.
- The PKI platform is capable of supporting manufacturers that will play a key role in administering security certificates.
- Personnel performing and administering the PKI procedure are technically competent.
- Company agrees to the SunSpec Official PKI Provider program business terms.

4. Terms of the SunSpec Official PKI Provider Program

The SunSpec Official PKI Provider program is designed to operate at high efficiency in order to minimize operational impact on participants and maximize program value and ROI for all stakeholders. SunSpec encourages program participants to integrate the program into their normal business processes and practices. Accordingly, the SunSpec Official PKI Provider must abide by these terms:

- Maintain membership in the SunSpec Alliance.
- Pay annual program fees to cover the costs of onboarding, training, technical support, and administrative compliance.
- Demonstrate that the company’s PKI platform can serve the needs of the SunSpec ecosystem of equipment manufacturers, software providers, system integrators, electric utilities, and independent power producers.
- Participate actively in the promotion of this progam to the DER industry.
- Collect SunSpec digital certificate issuance fees at time of customer engagement.
- Remit SunSpec digital certicate issuance fees to SunSpec at time of issuance.

The pricing of SunSpec digital certificate issuance fees is to be determined. The RFP questionnaire asks for your input on this topic.

5. Applicable Specifications

5.1 IEEE 2030.5 and Common Smart Inverter Profile

The initial standard to secure is IEEE 2030.5-2018 as stipulated in California Rule 21 interconnection requirements. The IEEE 2030.5-2018 specification is available for purchase from IEEE.org. Information about California Rule 21 can be found at http://www.cpuc.ca.gov/Rule21/.

The Common Smart Inverter Profile (CSIP) is the other source of criteria for California Rule 21 communication interface compliance. This document is available for free download at SunSpec.org.

5.2 SunSpec CSIP Test Procedures

The SunSpec Common Smart Inverter Profile (CSIP) Conformance Test Procedures are used to evaluate products for compliance to SunSpec certification criteria for California Rule 21. This document is also available for free download at SunSpec.org.

6. Other SunSpec Standards Requiring PKI Services

In addition to providing PKI services for California Rule 21 compliance, SunSpec plans to offer similar services for communication standards required by the IEEE 1547-2018 standard (IEEE 1815 and SunSpec Modbus) and for SunSpec information models transmitted over SunSpec Device/WS. Demand for these services is anticipated within the first half of 2018.

7. Working With SunSpec

7.1 Business Relationship

SunSpec Alliance is a non-profit trade alliance dedicated to expanding the market for Distributed Energy by establishing information and communication standards. To give the program the opportunity to develop and mature, SunSpec and the SunSpec Official PKI Provider will enter into an exclusive, two (2) year agreement that will allow the parties to establish a high-quality program in the market. Whether SunSpec offers exclusivity after that period is to be determined.

7.2 SunSpec Official PKI Provider Program Principles

Expertise, record keeping, and data management are essential requirements of the SunSpec Official PKI Service Provider program. SunSpec anticipates that the primary business of a typical program applicant is that of information security services. We assume that many applicants are compliant with International Standards Organization (ISO) standards given the use of ISO standards in industries that use PKI services.

The ability to work with hardware manufacturers is essential. Manufacturers play a key role in administering the chain of trust. The SunSpec Official PKI Service Provider is a key link between the SunSpec Certified communication standards compliance program and the manufacturer. Accordingly, the SunSpec Official PKI Service Provider serves as a guardian for the SunSpec Certified program and the SunSpec Alliance itself.

8. SunSpec Official PKI Provider Requirements

Public Key Infrastructure is becoming the preferred method of authentication for networked ecosystems due to its strength and scalability. In addition, advances in the hardware and semiconductor industries have allowed for strong authentication using ECC and PKI to be implemented in small devices very economically.

PKI is specified as the method of authentication used for IEEE 2030.5 and is therefore the method to be used for authenticating and securing communications for SunSpec Certified products and services.

There are two main aspects to providing a production PKI for the SunSpec Alliance that are covered by this RFP, the Registration Authority and the Certificate Authority.

8.1 Registration Authority Requirements

The Registration Authority (RA) is the gatekeeper for companies that wish to create accounts and be permitted to request and download SunSpec certificates. The RA authenticates member entities and their designated users who will have access to the system that requests and permits download of digital certificates to be implemented by members in their hardware and systems.

The RA works in concert with SunSpec certification testing to ensure that only entities that have passed compliance testing are permitted to download SunSpec certificates. Upon entry to the program, entities that have not passed SunSpec compliance testing can create accounts, but cannot download certificates until certification is completed and verified.

The RA is required to have an official agreement with a Certificate Authority (CA) who handles the operations and security around the PKI.

8.1.1 RA Responsibilities

- The RA shall manage the CA under partnership or contract with them for service
- The RA shall authenticate all entities that request a Certificate Requesting Account (CRA) via the SunSpec Alliance
- The RA shall coordinate with the SunSpec Certified program to verify that entities requesting certificates are eligible to receive them
- The RA shall ensure that auditable records are kept as per the SunSpec Certificate Policy (CP) and that all activities involving the SunSpec PKI conform to the SunSpec CP requirements
- The RA shall work with the SunSpec Security Working Group to update the SunSpec CP as needed by the SunSpec Alliance

8.2 Certificate Authority Requirements

The CA manages the operational security around the SunSpec Root and certificiate-issuing sub-CA(s). The CA is responsible for ensuring that the handling of all secrets and private keys is done in conformance to the approved certificate policy of the SunSpec Alliance. In addition, the CA is responsible for providing a Certificate Policy Statement (CPS) that clearly defines all procedures that will be followed to conform to the SunSpec CP.

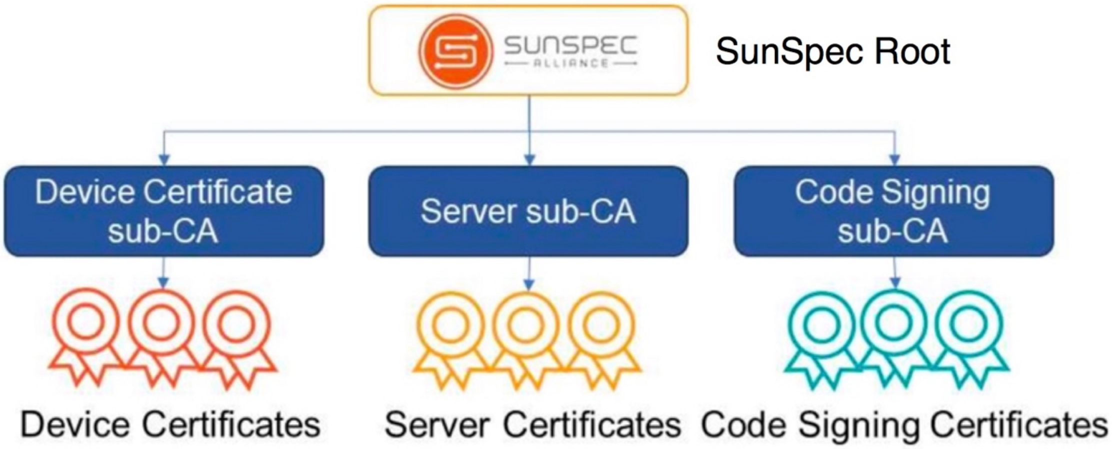
8.2.1 CA Responsibilities

- The CA physically hosts and operates the PKI elements for RA and SunSpec (i.e. Root and sub-CAs)
- The CA implements the security policies defined in the CP consistent with its CPS
- The CA shall maintain all necessary documentation for all operations involving the offline Root and hosted sub-CAs
- The CA shall maintain backups of the Root and sub-CAs in a geographically-separate location
- The CA shall have a disaster recovery plan to recreate the Root or sub-CAs in the event of hardware failure or other situation resulting in the loss of the primary copy of the Root and sub-CA private keys

PKI Hierarchy and Structure

PKIs are generally segregated into branches according to the type of element and the security properties characteristic of elements of that type. Each type of element is grouped under a separate sub-CA that issues certificates with data and properties appropriate for those element types. For example, end device elements might have a very long certificate validity period if they are deployed in the field and are difficult to update. Servers on the other hand, might have shorter life certificates because they are easier to update and are also potentially more vulnerable due to their dependency on software for key storage.

A possible PKI hierarchy for SunSpec could be as follows:



9. RFP Questionnaire

In your written response to this Open RFP, please answer all the questions in this section and provide responses numbered and ordered as presented here. Responses should be in PDF format and should be emailed to certification@SunSpec.org.

9.1 Corporate Overview

Success of the SunSpec certification process depends on the financial success of the PKI Service Provider. Please provide details about the company and the nature of its business.

	Requested Information
1	Corporate Overview:
2	Headquarters location:
3	Company web site:
4	Company locations (city, state, country):
5	How many total employees does the company have?
6	Describe the primary nature of your company's business.
7	Who are your key customers and where are they located?
8	How many years has your company been in operation?
9	What is the name, title, phone number, and email address of the person who is responsible for making the decision to participate in the SunSpec Official PKI Provider program?
10	Describe previous projects that your company has delivered that demonstrate your understanding of cybersecurity, hardware manufacturing and embedded systems.
11	Please provide three customer references.

9.2 Execution and Delivery

Given the changes occurring in the Distributed Energy Resources industry, timely execution is essential. Please provide information about your service locations and ability to execute the program.

	Requested Information
12	List location(s) where SunSpec PKI services will be performed (city, state, country):
13	What other types of projects are handled at each location?
14	What are your staffing levels at each location?
15	Which markets, applications, and standards do you address?
16	How do you protect customer confidentiality?
17	Describe your data backup and archiving process.
18	Describe your data retention policy.
19	Are you willing to designate a program manager for this program? (Yes/No)
20	Are you prepared to administer SunSpec Certified branding requirements? (Yes/No)
21	Provide a bullet list of your estimated deliverables and schedules to deploy a PKI for the SunSpec Alliance.
22	What pertinent experience makes your company exceptionally qualified to provide SunSpec certification testing?

9.3 Business Model

Crafting a mutually-beneficial model is essential. Please describe how your company proposes to do business with SunSpec.

	Requested Information
23	Describe any SunSpec PKI set up services and associated costs.
24	Describe any “per manufacturer” set up services and associated costs.
25	Describe typical digital certificate issuance services and fees (by volume).
26	Describe any other services and fees involved in your service.
27	What is your proposal for supporting SunSpec Official PKI Provider ecosystem marketing program?
28	How do you propose to bring additional value (customers, sponsorship dollars, etc.) to the SunSpec Alliance and its members?
29	Are you willing to cooperate with SunSpec, at no added cost, to produce online training that can be disseminated by SunSpec through is education distribution channels?

9.4 Certificate Issuance Fees

Certificate Issuance fees allow the SunSpec Alliance to provide, maintain, and enhance this valuable service. Our objectives are to keep costs low, generate enough money to continually improve the program, and stay in line with other successful programs. To that end, we seek your input.

	Requested Information
30	Do you offer Certificate Issuance Fee sharing for alliances like SunSpec? (Yes/No)
31	List the names of the other alliances for which you offer certification:
32	What percentage of the fee typically goes to the PKI service provider vs. to the alliance?
33	In your experience, what is a typical fee for products like those used in the DER industry?
34	For a given certification program, do fees vary by product type? If so, how do they vary?

10. Thank You

The SunSpec Alliance appreciates the opportunity to work with your organization on this important initiative. If you have any questions or suggestions about how to improve this program, please contact us at any time.