SunSpec Test PKI Certificates

Application Note

Abstract

This document describes SunSpec Test PKI certificate creation and usage.

License Agreement and Copyright Notice

Prepared by the SunSpec Alliance

4040 Moorpark Avenue, Suite 110

San Jose, CA 95117

Website: sunspec.org

Email: info@sunspec.org

Revision History

Version	Date	Comments
1.0	04-05-2019	Initial release

About the SunSpec Alliance

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

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

About the SunSpec Specification Process

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

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

SunSpec Interoperability Specifications follow a life cycle pattern of: DRAFT, TEST, APPROVED, and SUPERSEDED.

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

Table of Contents

1 Overview 6

2 Creating Test Certificates 7

2.1 Device Type 7

2.2 Manufacturer Model OID 7

2.3 Device Serial Number 7

3 Using Test Certificates 8

3.1 Test Certificate Package 8

3.1.1 Certificate Package Naming 8

3.1.2 Certificate Authorities 9

4 Getting Test Certificates 10

1 Overview

This application note describes the SunSpec Test PKI functionality and how to get test certificates for use with SunSpec CSIP Test Procedures.

The SunSpec Test PKI is intended to be used to create testing certificates as well as provide information to product developers about the requirements for supporting certificates in the production PKI environment.

The process of creating test certificates gives product developers an opportunity to understand the information necessary for the certificate creation process.

The CSIP specification mandates that TLS be used for all data connections in the system.

Digital certificates are required to perform the CSIP 2030.5 Test Procedures and to participate in a system conforming to the CSIP specification.

2 Creating Test Certificates

Creation of a device certificate package requires three pieces of information:

- Device type
- An object id (OID) corresponding to the manufacturer's model type
- A device serial number

2.1 Device Type

It is desirable for testing purposes for the server and clients to use different intermediate certificates in the certificate chains, so there are two certificate package types: client and server.

The IEEE 2030.5 specification does not make a distinction between certificates associated with client and server devices but the SunSpec test PKI uses this convention to ensure different certificate chains for clients and servers.

2.2 Manufacturer Model OID

The IEEE 2030.5-2018 specification requires that the Subject field of a device certificate be left empty and that the device identification be provided in the X509v3 Subject Alternative Name field as a combination of manufacturer model OID as hwType and device serial number as hwSerialNum.

The combination of manufacturer model OID and device serial number must be unique.

Example of the X509v3 Subject Alternative Name contents in a device certificate:

```
X509v3 Subject Alternative Name:
    othername: hwType=1.3.6.1.4.1.99999.13.1, hwSerialNum=1234
```

The manufacturer OID consists of an IANA PEN with an additional numbering hierarchy added to represent each different model id. For more information of PEN, see *https://en.wikipedia.org/wiki/Private_Enterprise_Number*.

The management of the model id is left to each manufacturer but it must satisfy the requirement that the combination of model OID and device serial number is unique.

Some manufacturers may already have a PEN allocated with an existing hierarchy within the organization and others may need to request a PEN from IANA. The process of acquiring a PEN is easy and free.

The OID example used in the IEEE 2030.5 specification:

1.3.6.1.4.1.99999.13.1.1

Where 1.3.6.1.4.1.99999 is the manufacturer PEN and 13.1.1 represent the model id in the manufacturer hierarchy.

2.3 Device Serial Number

The device serial number can be any string of characters. The IEEE 2030.5 specification requires the serial number be represented as an ASN.1 DER encoded OCTET STRING. By convention, the serial number string provided by the manufacturer will be placed in the OCTET STRING as a utf-8 encoded string allowing support for any sequence of characters. This convention allows a deterministic usage and display of the serial number in a human readable form of the certificate.

3 Using Test Certificates

Each request for a device test certificate results in a package of multiple certificates.

The testing environment consists of a device that is being testing and a framework that is creating the testing conditions. The testing framework emulates the functionality of the peer of the device under test and creates the required test conditions.

In this environment, the device under test is expected to have the same behavior as it would in a production environment and is configured with a single certificate chain that is used throughout testing. In the case the additional certificates in the certificate package are not used.

The testing framework can be configured and updated to suit the requirements of the test procedures and uses multiple certificate chains to create the security related conditions specified in the test procedures.

3.1 Test Certificate Package

A certificate package for a device is distributed as a single directory in zip file format.

A test certificate package contains three valid device certificates, the device private key, the root certificate and device certificates with errors for error testing. The device certificate files include all intermediate CA certificates in the certificate chain and the device private key. The files are provided in PEM (.pem), PKCS 7 (.p7b), and PKCS 12 (.p12) formats. The .p12 files are encrypted with a password of: password. The private key file is in PKCS 8 format and is PEM encoded.

It is desirable for testing purposes for the server and client clients to use different intermediate certificates in the certificate chains, so there are two certificate package types: client and server.

Test frameworks should get a full set of server and client certificate packages and use the appropriate set based on the device under test. Test frameworks can install a certificate set once and reuse the same certificates for testing with different devices.

Devices being tested should get an appropriate test certificate package based on the device type (client or server) and use the mca-mica-dev certificate chain for testing as this most complex chain option and should as the best validation of compliant chain support.

The test certificate package is generated based on the device type, manufacturer model OID, and serial number of the device.

For a device under test, only three files are required: the root certificate, the device private key, and the device certificate. The root certificate and the device private key are located in the top level directory. The device certificate is located in the directory corresponding to the format used by the device: pem, p7b, or p12. The certificate directories also contain folders with additional valid certificates of different chain lengths and certificates containing errors. These can be used by a testing framework for more comprehensive testing.

3.1.1 Certificate Package Naming

All directory and file names in the certificate package follow the following format:

`sat-<type>_<chain>_<model>_<serial number>`

The following table describes the file name elements.

File Name Element	Description
sat	SunSpec Alliance Test
<type>	‘cli’ - client certificate ‘svr’ - server certificate ‘key’ - private key
<chain>	‘dev’ - signed by root ‘mica-dev’ - signed by MICA signed by root ‘mca-mica-dev’ - signed by MICA signed by MCA signed by root
<model>	Unique portion of the model OID that comes after the IANA PEN prefix. For example a model OID of 1.3.6.1.4.1.53630.2.10 would be represented as ‘53630_2_10’.
<serial number>	Serial number of the device.

3.1.2 Certificate Authorities

The three valid device certificates consist of certificates with different certificate chain lengths. The IEEE 2030.5 specification specifies three certificate authority types: Smart Energy Root CA (SERCA), Manufacturer CA (MCA), Manufacturer Issuing CA (MICA). A MICA issues the device certificates associated with a manufacturer. A MICA certificate can be issued by the SERCA or an intermediate manufacturer CA (MCA). A MCA certificate is always issued by the SERCA. The SERCA can also issue a device certificate but this is not standard practice. The valid certificates consist of the three following certificate chains: serca-device, serca-mica-device, and serca-mca-mica-device.

The certificate authority certificates consist of the SERCA, MCA, MCA signed MICA, and SERCA signed MICA.

The error certificates consist of device certificates based on the serca-mica-device chain with errors to be used for error testing.

4 Getting Test Certificates

SunSpec test PKI certificate packages are available on the SunSpec website at https://sunspec.org/sunspec-public-key-infrastructure-pki-program/.

The following information must be provided for certificate generation:

- Company
- Contact name and email
- Device type (server or client)
- Manufacturer model OID
- Device serial number
- Number of certificate packages (defaults to 1)

If the number of certificate packages is more than one, a set of certificate packages are generated. In this case, the serial number must be a numeric value and is incremented by one for each certificate package created.