SunSpec Alliance Public Key Infrastructure

PKI Scope and Certificate Profiles

April 30, 2019

Document Identifier: 1.3.6.1.4.1.52424.1.100.1

Table of Contents

1 Introduction 2
1.1 Overview 2
1.2 References 2
1.3 Document Name and Identification 3
2 System Architecture 3
3 CA Hierarchy 4
4 Deviations from Core CP 5
5 Certificate Profiles 6
5.1 CA Certificates 6
5.1.1 Root CA Certificate Profile 6
5.1.2 Intermediate CA Certificate Profile (MCA) 7
5.1.3 Intermediate CA Certificate Profile (MICA) 8
5.2 End-entity Certificates 9
5.2.1 Device Certificate Profile 9

1 Introduction

1.1 Overview

This document describes the scope for the SunSpec Alliance (“Owner”) public key infrastructure (PKI). It includes system architecture, CA hierarchy, certificate deployment, and certificate validation requirements. Additionally, this document defines profiles for the different types of certificates in the SunSpec Alliance public key infrastructure (PKI). It includes details on the subject name attributes, validity period, key algorithm, and extensions. Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) profiles are also defined. SunSpec PKI Participants MUST support the requirements and the profiles in this document as well as the requirements defined in the Kyrio Core Certificate Policy documents.

Throughout this document, the words that are used to define the significance of particular requirements are:

“must”	This word, or the word “require”, means that the definition is an absolute requirement of this document.
“must not”	This phrase means that the definition is an absolute prohibition of this document.
“should”	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
“should not”	This phrase means that there may exist valid reasons in particular circumstances when the listed 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 word “optional”, means that an item is truly discretionary.

1.2 References

This document uses the following references:

Ref #	Doc Number	Reference Title
[1]	RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, IETF (Myers, Ankney, Malpani, Galperin, Adams), June 1999.
[2]	RFC 5280	Internet X.509 PKI Certificate and Certification Revocation List (CRL) Profile, IETF (Cooper, Santesson, Farrell, Boeyen, Housley, and Polk), May 2008.

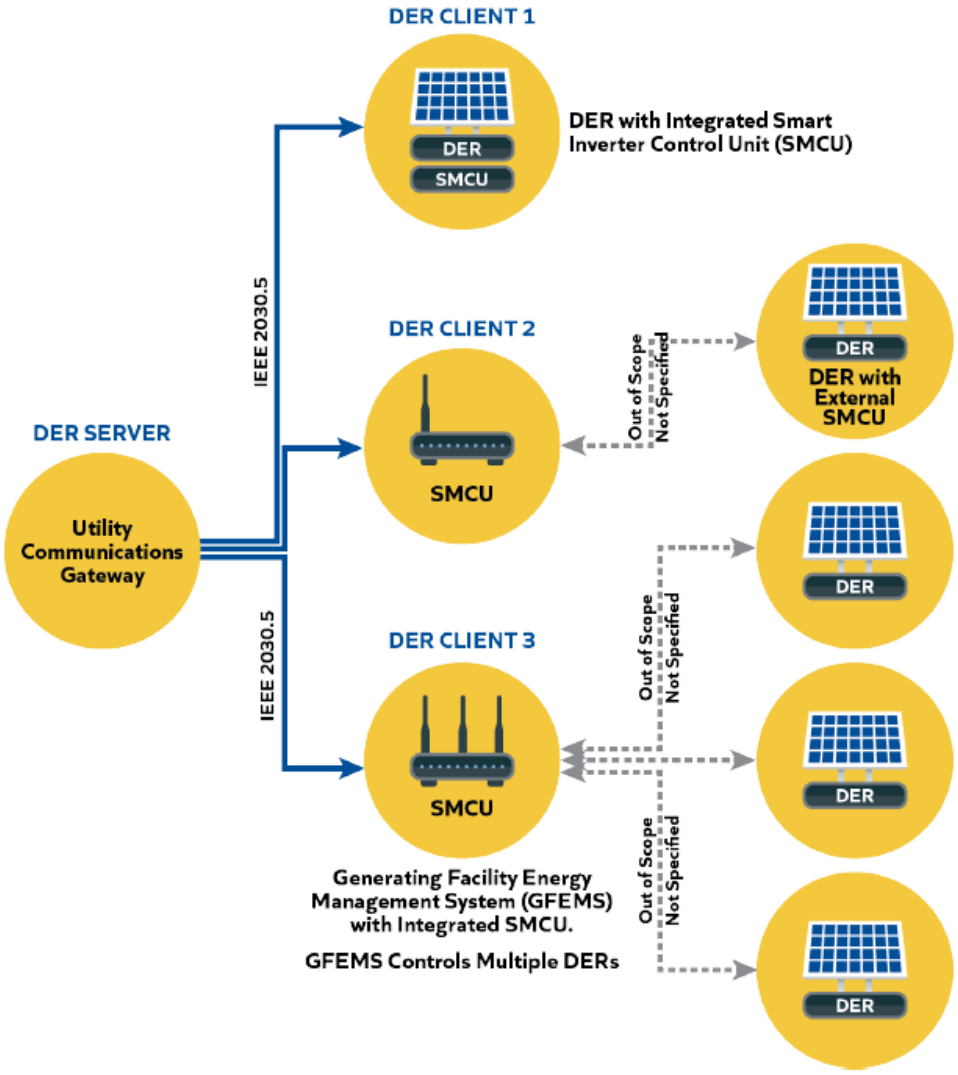
1.3 Document Name and Identification

This document is named SunSpec Alliance PKI Scope and has the following policy object identifier:

OID above. 1.3.6.1.4.1.52424.1.100.1

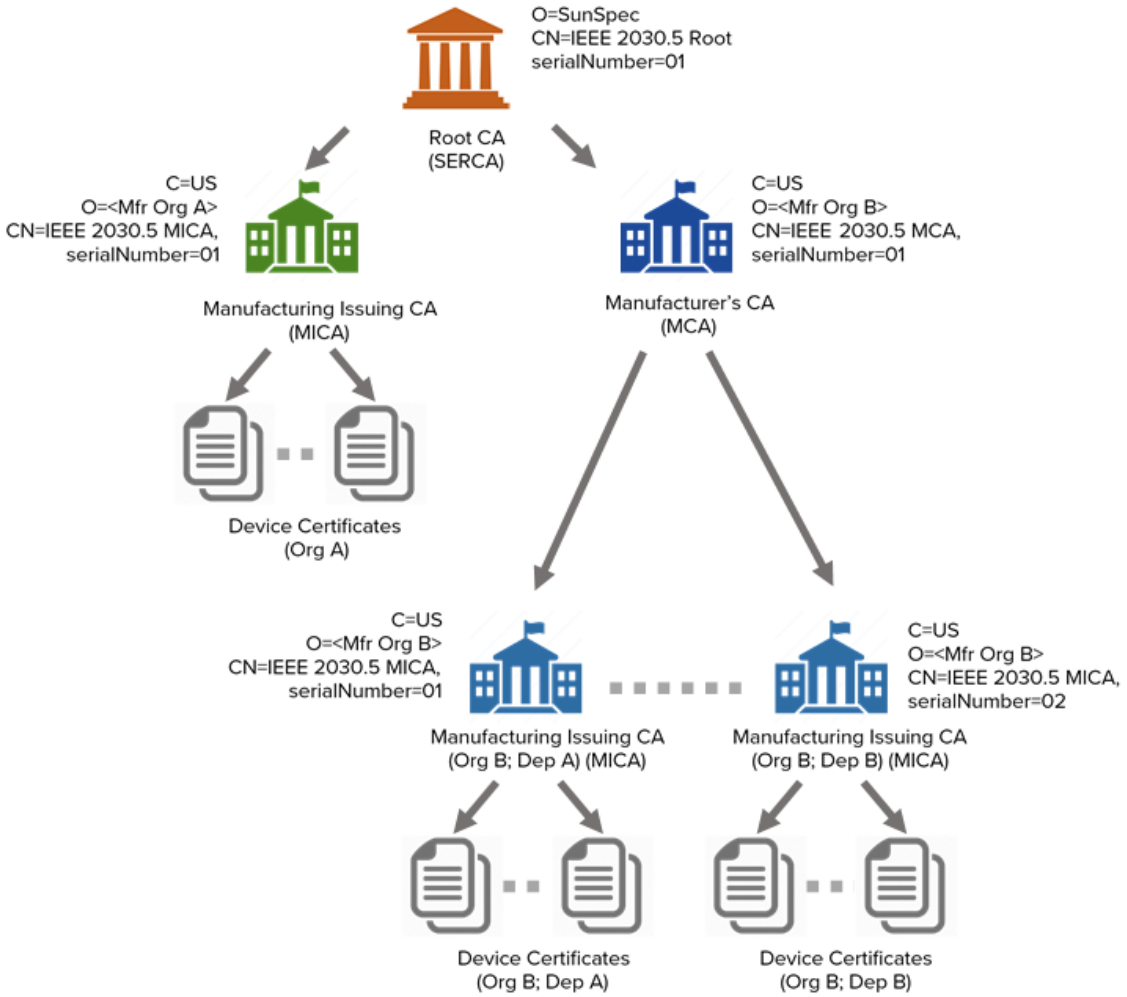
2 System Architecture

The overall network consists of a connected system of Distributed Energy Resources (DER) which are power generation and storage devices that communicate via IP-based networks using the IEEE 2030.5 protocol. All gateways, aggregators, or devices that communicate directly with a Utility Communication Gateway require digital certificates to complete TLS mutual authentication.



3 CA Hierarchy

The SunSpec ecosystem utilizes a PKI hierarchy as described in the IEEE 2030.5 specification. The hierarchy comprises a Root CA (SERCA), directly managed by Kyrio on behalf of SunSpec, that issues Intermediate CAs to manufacturers. Manufacturers will be responsible for requesting and setting up their own Manufacturer's CAs (MCAs) or Manufacturing Issuing CAs (MICAs). In particular, for manufacturers that do not require per-department CAs, the SERCA will issue MICA Sub CAs. For manufacturers that might require intermediate Sub CAs to handle different production lines, the SERCA will issue MCA Sub CAs for the qualifying organizations. At this time there is no distinction between devices or servers with all elements of the ecosystem receiving the same type of End Entity Certificates.



4 Deviations from Core CP

SunSpec Alliance PKI does not require support for revocation checking as defined in Section 4.9 of the Kyrio Core CP document (OID: 1.3.6.1.4.1.52424.1.1.1), as it is not currently supported by the IEEE 2030.5 specification. Additionally, the SunSpec Alliance PKI does not require support for Online Certificate Status Protocol (OSCP) for the same reason.

5 Certificate Profiles

This section defines profiles for the different types of certificates in the PKI. Certificates MUST be compliant to RFC 5280 and have the settings defined in this section.

5.1 CA Certificates

5.1.1 Root CA Certificate Profile

Certificate Details

Version	v3
Serial number	Unique Positive Integer assigned by the CA
Subject DN	O=SunSpec Alliance CN=IEEE 2030.5 Root serialNumber=<001>
Issuer DN	O=SunSpec Alliance CN=IEEE 2030.5 Root serialNumber=<001>
notBefore	<Issuing Date>
notAfter	Dec 31, 9999 23:59:59Z [99991231235959Z]
Signature Algorithm	☒ Sha256
Key size and type	ECC 256 (secp256r1)

Certificate Extensions

Extension Identifier	OID	Criticality	Value
keyUsage	{id-ce 15}	**TRUE**	
keyAgreement			Set
cRLSign			Set
basicContraints	{id-ce 19}	TRUE	
cA			Set (TRUE)
pathLenConstraint			Not Set
subjectKeyIdentifier	{id-ce 14}	FALSE	OPTIONAL
keyIdentifier			Calculated per Method 2 [RFC 5280; Section 4.2.1.2]
certificatePolicies	{id-ce 32}	**TRUE**	
policyIdentifier			anyPolicy {id-ce- 32 0}
policyQualifiers			Not Set

5.1.2 Intermediate CA Certificate Profile (MCA)

Certificate Details

Version	v3
Serial number	Unique Positive Integer assigned by the CA
Subject DN	C=<Country> O=<Manufacturing Org> CN=IEEE 2030.5 Root serialNumber=<001>
Issuer DN	O=SunSpec Alliance CN=IEEE 2030.5 Root serialNumber=<001>
notBefore	<Issuing Date>
notAfter	Dec 31, 9999 23:59:59Z [99991231235959Z]
Signature Algorithm	☒ Sha256
Key size and type	ECC 256 (secp256r1)

Certificate Extensions

Extension Identifier	OID	Criticality	Value
keyUsage	{id-ce 15}	**TRUE**	
keyCertSign			Set
basicContraints	{id-ce 19}	TRUE	
cA			Set (TRUE)
pathLenConstraint			Set (1)
authorityKeyIdentifier	{id-ce 35}	FALSE	
keyIdentifier			Calculated per Method 2 [RFC 5280; Section 4.2.1.2]
subjectKeyIdentifier	{id-ce 14}	FALSE	OPTIONAL
keyIdentifier			Calculated per Method 2 [RFC 5280; Section 4.2.1.2]
certificatePolicies	{id-ce 32}	**TRUE**	
policyIdentifier			<At Least One IEEE 2030.5 Device Type Identifier>
policyQualifiers			Not Set

5.1.3 Intermediate CA Certificate Profile (MICA)

Certificate Details

Version	v3
Serial number	Unique Positive Integer assigned by the CA
Subject DN	C=<Country> O=<Manufacturing Org> CN=IEEE 2030.5 Root serialNumber=<001>
Issuer DN	O=SunSpec Alliance CN=IEEE 2030.5 Root serialNumber=<001>
notBefore	<Issuing Date>
notAfter	Dec 31, 9999 23:59:59Z [99991231235959Z]
Signature Algorithm	☒ Sha256
Key size and type	ECC 256 (secp256r1)

Certificate Extensions

Extension Identifier	OID	Criticality	Value
keyUsage	{id-ce 15}	**TRUE**	
keyCertSign			Set
basicContraints	{id-ce 19}	TRUE	
cA			Set (TRUE)
pathLenConstraint			Set (0)
authorityKeyIdentifier	{id-ce 35}	FALSE	
keyIdentifier			Calculated per Method 2 [RFC 5280; Section 4.2.1.2]
subjectKeyIdentifier	{id-ce 14}	FALSE	OPTIONAL
keyIdentifier			Calculated per Method 2 [RFC 5280; Section 4.2.1.2]
certificatePolicies	{id-ce 32}	**TRUE**	
policyIdentifier			<At Least One IEEE 2030.5 Device Type Identifier>
policyQualifiers			Not Set

5.2 End-entity Certificates

5.2.1 Device Certificate Profile

Certificate Details

Version	v3
Serial number	Unique Positive Integer assigned by the CA
Subject DN	Not Set
Issuer DN	<Issuing CA: MCA or MICA>
notBefore	<Issuing Date>
notAfter	Dec 31, 9999 23:59:59Z [99991231235959Z]
Signature Algorithm	☒ Sha256
Key size and type	ECC 256 (secp256r1)

Certificate Extensions

Extension Identifier	OID	Criticality	Value
keyUsage	{id-ce 15}	**TRUE**	
keyAgreement			Set
digitalSignature			Set
subjectKeyIdentifier	{id-ce 14}	FALSE	OPTIONAL
keyIdentifier			Calculated per Method 2 [RFC 5280; Section 4.2.1.2]
authorityKeyIdentifier	{id-ce 35}	FALSE	
keyIdentifier			Calculated per Method 2 [RFC 5280; Section 4.2.1.2]
certificatePolicies	{id-ce 32}	**TRUE**	
policyIdentifier			<Exactly One IEEE 2030.5 Device Type Identifier>
policyQualifiers			Not Set
subjectAltName	{id-ce 17}	**TRUE**	
otherName: HardwareModuleName: hwType hwSerialNum			 Set (<OID VALUE>) Set (<OCTET STRING VALUE>)