Status: Approved

Version: 1.0

Secure SunSpec Modbus Specification

Abstract

This document specifies the requirements for Secure SunSpec Modbus TCP.

License Agreement and Copyright Notice

Prepared by the SunSpec Alliance

Website: sunspec.org

Email: info@sunspec.org

Revision History

Version	Date	Comments
0.1	08/18/2025	Initial release
0.2	08/26/2025	Workgroup updates and removal of RTU requirements
0.3	09/05/2025	Updated role requirements, added appendix with typical use cases, and expanded the development description.
0.4	11/05/2025	Promoted several SHOULD requirements to MUST.
1.0	12/10/2025	Promoted from TEST to Approved.

.

About the SunSpec Alliance

The SunSpec Alliance is a California-based non-profit trade alliance that develops open information standards to support Distributed Energy Resource (DER) interoperability, cybersecurity, and grid resiliency. With over 180 member organizations from North America, Europe, Asia, Australia, and the Middle East, SunSpec serves manufacturers, software developers, utilities, and service providers across the DER industry.

SunSpec standards enable seamless integration of DER systems at residential, commercial, and utility scales, helping reduce cost, ensure compliance, and accelerate innovation. Membership is open to corporations, non-profits, and individuals.

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 work group 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 recommendations with regard to best practices, but are not a matter of conformance. Informative documents can be revised more freely and more frequently to improve the quality and quantity of information provided.

SunSpec Interoperability Specifications follow a lifecycle pattern of: DRAFT, TEST, APPROVED, and SUPERSEDED.

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

Table of Contents

1 Introduction

Modbus, defined by Modbus.org, was designed for use in isolated, "air-gapped" industrial networks where physical access was the primary security measure. In modern DER and industrial internet of things (IIoT) environments, it is necessary to provide additional security features in the communication protocol. For this reason, the SunSpec Alliance initiated an effort to establish a secure implementation of Modbus based on contemporary security practices. Secure SunSpec Modbus provides a standardized set of requirements for implementing a secure implementation of Secure SunSpec Modbus TCP, particularly for grid control applications such as those described in the IEEE 1547-2018 standard. The Secure SunSpec Modbus TCP implementation incorporates mutual TLS with an X.509 extension to provide confidentiality, integrity, authentication, and authorization based on the MODBUS/TCP Security Protocol Specification.

1.1 Security Principles

Secure SunSpec Modbus TCP provides the following security features:

- **Confidentiality:** TLS encrypts all data transmitted between the client and server, preventing eavesdropping and data exposure.
- **Authentication:** TLS uses digital certificates (Public Key Infrastructure) to provide mutual authentication, ensuring that both the client and the server are who they claim to be.
- **Integrity:** TLS provides data integrity checks to ensure that the message has not been altered during transmission.
- **Anti-Replay Protection:** TLS is designed to prevent replay attacks by using session-specific keys and sequences.
- **Authorization:** The protocol can also use information embedded in the certificates (such as user and device roles) to implement role-based access control (RBAC), allowing for more granular authorization in DER grid control environments.

1.2 Document Organization

Chapter 2 includes the normative references that provide links to the specifications mentioned in this document.

Chapter 3 covers the Secure SunSpec Modbus TCP Developments.

Chapter 4 discusses considerations for Secure SunSpec Modbus RTU.

Chapter 5 covers the Secure SunSpec Modbus TCP Requirements.

Appendix A describes possible use cases for this communication protocol.

Appendix B describes the possibility of running a secure and traditional SunSpec Modbus server on the same product.

1.3 Glossary

Device	A device is an entity that exchanges data across communications interfaces. A device has a data set, modeled by Device Information Models, that describes physical and state information about the device. The device data set is the set of logically related data points specific to the device type. The collection of Device Information Models that describe the data set corresponds to the full set of device data points supported by the device.
mbaps	Modbus Security Application Protocol
MBR	Modbus Requirement. This reflects the requirement number in the Modbus/TCP Security Protocol Specification.
Modbus	Modbus is a communication protocol for transmitting information between devices using a serial or TCP/IP communication interface. This document specifies Modbus encoding for Device Information Model instances. The official Modbus protocol is defined by modbus.org
MUST, MUST NOT, REQUIRED, MUST, MUST NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL	The keywords "MUST", "MUST NOT", "REQUIRED", "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification, are to be interpreted as described in IETF RFC 21

2 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, https://www.rfc-editor.org/info/rfc2119.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, DOI 10.17487/RFC2279, January 1998, https://www.rfc-editor.org/info/rfc2279.

[RFC4492]. Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., Moeller, B., Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), May 2006, https://www.rfc-editor.org/info/rfc4492

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., Polk, W., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008, https://www.rfc-editor.org/info/rfc5280.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014, https://www.rfc-editor.org/info/rfc7159.

[MODBUS] Modbus IDA, MODBUS Application Protocol Specification v1.1b3, North Grafton, Massachusetts, www.modbus.org/specs.php, April 26, 2012.

[MODBUS/TCP Security] MODBUS/TCP Security Protocol Specification v36, North Grafton, Massachusetts, https://modbus.org/docs/MB-TCP-Security-v36_2021-07-30.pdf, July 30, 2021.

3 Secure SunSpec Modbus TCP Development

The SunSpec Modbus workgroup gathered weekly for several months to select the requirements for the Secure SunSpec Modbus Specification. During those conversations, there were many difficult decisions regarding the security requirements and use cases of the SunSpec specification. The following sections describe many of the critical decisions and why the SunSpec implementation deviates from the modbus.org MODBUS/TCP Security specification.

3.1 Cipher Suites Selection

The MODBUS/TCP Security specification, last updated by Modbus.org in 2021, permits weak cipher suites that use outdated encryption algorithms, short key lengths, vulnerable modes (e.g., Cipher Block Chaining)[1], and absent Perfect Forward Secrecy (PFS). As a result, the SunSpec working group modernized the cipher suite options while allowing for additional ciphers to be added as standardized cryptography evolves. The group selected ciphers that were widely available and lightweight for the embedded systems.

Devices must support the following TLSv1.2 cipher suites:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8

and if the device supports TLSv1.3, they must provide the following cipher suites:

- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

The list of required ciphers was kept to a minimum to improve interoperability. Further, IEEE 2030.5—specified as a standard interface in the IEEE 1547 standard like SunSpec Modbus—requires TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8, so it was included because many DER devices may already have software libraries and hardware components that support it.

3.2 Authorization and Mandatory Roles

SunSpec adopted the MODBUS/TCP Security authorization approach to address the grid operator use case—and took things further by mandating the X.509v3 certificate must include a role. MODBUS/TCP Security states the role in the X.509v3 certificate MUST use ASN.1:UTF8String encoding. There must only be one role defined per certificate and the entire string is treated as a single role. SunSpec adopted this same approach and embedded the role in the X.509v3 certificate with the Modbus.org Private Enterprise Number (PEN) OID 1.3.6.1.4.1.50316.802.1.

To encourage standardization across industry, the SunSpec Alliance also created a set of required roles with these general permissions.[2] All roles include read access to the SunSpec Modbus points, but write access is limited based on the role:

- **ReadOnlySunSpec** - Read access to all data. No write permissions. This role may be

[1] P.G. Sarkar, S. Fitzgerald, Attacks On SSL: A Comprehensive Study of BEAST, CRIME, TIME, BREACH, Lucky 13 & RC4 Biases, iSEC Partners, Inc, Aug 2013.

[2] Roles were discussed previously in the SunSpec/Sandia DER Cybersecurity Workgroup, wherein a working group establishing a set of recommendations around role-based access control. See: J. Johnson, Recommendations for Distributed Energy Resource Access Control, Sandia Report SAND2021-0977, January 2021.

used by DER owners for monitoring production data or DER vendors for monitoring, diagnostics, and/or prognostics.

- **GridServiceSunSpec** - Read access to all data. Write access to commanded and autonomous functions. No access to networking or protection functions.
- **NetworkAdministratorSunSpec** - Read access to all data. Write access to SunSpec network holding registers.
- **SuperAdministratorSunSpec** - Full read/write access to all SunSpec points. This role may be used by (a) the grid operator, (b) the system installer, (c) the DER vendor for repairs, or (d) a DER owner in situations where they are operating a microgrid.

A full role-to-rights mapping reference implementation for SunSpec Modbus models is provided on GitHub[3].

There was also a desire to align, where possible, with the IEC 62351-8 "Role-based access control for power system management" standard. Therefore, it is noted the device vendor may add additional roles from IEC 62351-8 that include:

- VIEWER
- OPERATOR
- ENGINEER
- INSTALLER
- SECADM: Security administrator
- SECAUD: Security auditor
- RBACMNT: RBAC management

An example X.509v3 certificate with the role extension is shown in Fig. 1.

[3] https://github.com/sunspec/rbac

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            09:b2:2a:2e:75:00:40:a2:90:1e:3d:92:68:86:04:fe:89:dd:76:83
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = STATE, L = LOCAL, O = ORG, OU = SUBORG, CN = INTER-CA-CLIENT
        Validity
            Not Before: Sep  5 20:51:32 2025 GMT
            Not After : Sep  3 20:51:32 2035 GMT
        Subject: C = US, ST = STATE, L = LOCAL, O = ORG, OU = CLIENTORG, CN = SunSpecModbusSecurityClient
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d5:8a:3f:02:96:f2:fd:bb:4b:87:db:ae:d2:6c:
                    37:ce:af:ef:22:f2:79:27:93:75:eb:0c:07:3b:6b:
                    de:fc:0c:b7:62:bb:c9:d6:df:31:93:06:e8:80:c4:
                    3f:b7:28:96:64:5b:cc:e3:52:40:07:57:c6:62:3f:
                    92:5e:6d:62:44:1b:0c:21:b1:3e:9a:8d:dd:1d:08:
                    a9:9d:2e:d6:3a:f3:a1:36:79:57:a2:7e:e7:60:73:
                    28:d3:b2:dc:c7:6b:92:ae:75:68:bd:d8:22:2c:cb:
                    9a:8f:08:76:2b:ed:57:6f:d3:d5:ca:3c:4a:df:15:
                    28:3b:99:f4:2d:1d:9f:19:72:b9:12:2d:8d:ca:ae:
                    5d:1c:60:56:73:2e:97:6b:27:75:d4:9e:5c:a7:df:
                    94:79:15:22:1c:68:01:61:b6:fe:9d:71:98:50:43:
                    32:cc:0d:77:c6:10:ce:43:a2:6c:48:00:a3:1b:7b:
                    47:31:4b:69:b8:0d:ed:b7:13:c3:07:ca:bd:12:95:
                    11:ed:5e:8b:35:71:d2:a0:84:6a:cc:fe:6a:a3:a8:
                    45:11:66:20:af:c2:6e:d0:10:b8:fd:6a:fb:cf:9b:
                    39:8e:3b:d4:a4:3c:90:af:f0:a0:75:8a:c3:59:16:
                    1a:89:b6:2b:54:e8:ab:16:3e:4e:1c:ac:e5:89:7e:
                    76:f5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment
            1.3.6.1.4.1.50316.802.1:
                ..ReadOnlySunSpec
            X509v3 Subject Key Identifier:
                94:B0:5A:93:2A:C5:A7:C8:82:6E:67:E6:45:F5:B7:CE:AC:E3:6E:15
            X509v3 Authority Key Identifier:
                DirName:/C=US/ST=STATE/L=LOCAL/O=ORG/OU=SUBORG/CN=ROOT-CA
                serial:2E:28:DD:9B:0E:CA:8F:A9:0A:0C:1B:D7:05:D7:BF:E5:75:B0:29:E0
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        32:f4:f1:46:df:96:38:26:cb:15:88:e7:1f:63:a6:3e:99:e2:
        5a:f7:94:56:c2:f1:cf:e5:7b:69:db:5f:38:e8:c8:03:1f:53:
        3c:01:65:28:f1:b5:91:fd:c3:49:dd:80:10:f1:4e:b7:b2:a4:
        9d:bf:9e:b2:8c:05:fe:40:d0:62:de:dd:29:d5:90:c8:ce:10:
        fa:4b:7a:f5:1c:bd:c9:9c:55:d6:9d:2c:c1:f3:f5:55:6d:1e:
        a7:7e:b5:c2:de:08:9b:13:55:ef:07:58:d5:9f:c1:b2:3b:47:
        03:e2:0c:5e:4b:d2:10:bd:43:d1:eb:33:b8:89:57:1f:38:a8:
        b8:36:eb:91:82:5f:89:a6:7d:d8:d2:f8:6c:4d:54:3d:03:16:
        35:8f:9c:5b:e2:c1:9e:52:75:b2:28:7b:1e:6e:ac:4f:6b:ca:
        9c:81:09:ca:12:a6:e3:5a:92:53:c8:a8:56:22:d2:cf:b6:63:
        44:8e:47:e9:46:1a:a2:48:c9:50:66:09:77:a5:93:36:48:dc:
        53:83:c5:47:63:fe:11:33:dc:2f:9d:a0:93:92:f6:e0:64:d8:
        d2:87:36:f0:e2:65:66:2e:5b:e9:8b:2b:d3:9b:b9:a4:c9:05:
        8f:ba:07:99:40:76:d7:71:cc:8b:90:23:ef:bf:02:21:b2:14:
        09:5e:e3:93
```

Example X.509v3 Certificate with Role Encoded as a Certificate Extension

- Example Role is ReadOnlySunSpec
- The OID for the Role is defined in the Modbus.org Private MIB whose PEN (Private Enterprise Number) is 50316.
- The “..” at the beginning of the Role field are the non-printable ASN.1 UTF8String type (e.g., 0x0C) and byte length values (e.g., 0x0F for 15 bytes).

Figure 1: X.509 Certificate with the Role OID extension.

3.3 PKI Design

The PKI architecture is outside the scope of this document, but it's likely to align with the IEEE 2030.5 implementation wherein there's three tiers (a root CA, intermediate CA, and leaf certificates). A national or jurisdictional root CA will be established and intermediate CAs established for corporations operating within the PKI ecosystem. Client and server certificates would then be signed by the intermediate CAs, which will enforce the appropriate role requirements.

The requirements in Section 5 do not prohibit the use of self-signed certificates in the DER equipment if the owner would like local encryption, authentication, and authorization. Any internet-routed Modbus communications MUST be tied back to an appropriately secured root of trust. Self-signed certificates are allowed but not recommended for internet-routed communications.

3.4 Server Certificate Lifecycles

It is anticipated that DER products will be shipped with some root and server certificates, especially if a national or international root CA is established. In addition, the products should include the ability to add new CA chains and server certificates. These MUST be added either a) through a local out-of-band mechanism like a website hosted on the product or via a vendor's cloud management portal or b) through a secured in-band Modbus interface that MUST push the necessary files to the DER device's secure store.

3.5 Authorization Enforcement

DER products with the SunSpec Modbus Server are responsible for authorization enforcement. All products MUST enforce the SunSpec roles, but additional roles can be added as necessary. These roles may limit what registers can be read. For example, roles could be created that only allow access to the measurement data included in Models 701 (DERMeasureAC) and 714 (DERMeasureDC).

For a given role, the SunSpec Modbus holding register map is likely to include many data regions that do not permit read or write access. As a result, the Modbus Client must be programmed to only make read or write operations on the registers which are permitted by the Server. Otherwise, the Modbus Server will return exception code 01 – Illegal function code. This will require additional programming logic on the part of SunSpec Modbus implementors.

4 Secure SunSpec Modbus RTU Development

There have been concerns within the standards community that SunSpec Modbus RTU could pose a cybersecurity risk. While the risk is arguably much lower as compared to an Internet-routable communication protocol like SunSpec Modbus TCP, the working group investigated options for securing these serial communications that could be routed over twisted pair cable (e.g., RS-485 or RS-232), radio frequency, fiber optic, or other media. One proposal was to adopt the technology from the KNX Data Secure protocol for the Modbus serial bus.

While this proposal has merit, the working group decided to defer the work of defining security requirements for Modbus RTU to a future revision of this document.

5 Secure SunSpec Modbus TCP Requirements

5.1 Transport Layer Security

SunSpecTCP-1. Port 802 **SHOULD** be used for the mbaps protocol.

SunSpecTCP-2. mbaps device **MUST** support at least 10 root certificates.

SunSpecTCP-3. mbaps device **MUST** include a secure method of adding and removing root certificates and server certificates. The mbaps device **MUST** consider all stored certificates when processing authentication requests.

SunSpecTCP-4. The TLS Protocol v1.2 as defined in [RFC5246] **MUST** be supported as a secure transport protocol to an mbaps Device. (modified from MBR-01[4])

SunSpecTCP-5. The TLS Protocol v1.3 as defined in [RFC 8446] **MAY** be supported as a secure transport protocol to an mbaps Device.

SunSpecTCP-6. Secure communications to an mbaps Device **MUST** use mutual client/server authentication as provided by the TLS Handshake Protocol. (MBR-02)

SunSpecTCP-7. X.509v3 Certificates as defined in [RFC5280] **MUST** be used as mbaps device credentials for Identity/Authentication by the TLS protocol. (MBR-03)

SunSpecTCP-8. The Authorization function **MUST** use the role transferred via X.509v3 certificate extensions. (modified from MBR-04)

SunSpecTCP-9. There **MUST** be no change to the mbap protocol because of it being encapsulated by secure transport. (MBR-05)

SunSpecTCP-10. mbaps end devices **MUST** provide mutual authentication when executing the TLS Handshake Protocol to create the TLS session. (MBR-06)

SunSpecTCP-11. The TLSServer **MUST** send the CertificateRequest message during the TLS handshake. (MBR-07)

SunSpecTCP-12. The TLSClient **MUST** send a ClientCertificate message upon receiving a request containing the Client Certificate Request. (MBR-08)

SunSpecTCP-13. If the TLSClient does not send a ClientCertificate message, then the TLSServer **MUST** send a ‘fatal alert’ message to TLSClient and terminate the connection. (MBR-10)

SunSpecTCP-14. Per RFC5246-7.2.2, the TLS connection **MUST NOT** be resumed after a ‘fatal alert’. (MBR-11)

5.2 Cipher Suite Selection

SunSpecTCP-15. Cipher suites used with TLS for mbaps **MUST** be listed at the IANA Registry found at http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml (MBR-12)

SunSpecTCP-16. The cipher allowed for TLS with mbaps **MUST** accommodate the use of X.509v3 certificates. (MBR-13)

[4] MBR is the Modbus Base Requirement from [MODBUS/TCP Security].

SunSpecTCP-17. mbaps Devices **MUST** provide at minimum the following TLS v1.2 cipher suites: (modified from MBR-14)

1. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
2. TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
3. TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8

SunSpecTCP-18. If supporting TLSv1.3, mbaps Devices **MUST** provide at minimum the following TLSv1.3 cipher suites:

1. TLS_AES_128_GCM_SHA256
2. TLS_CHACHA20_POLY1305_SHA256
3. TLS_AES_128_CCM_SHA256

SunSpecTCP-19. In the TLS handshake, the mbaps Devices **MUST** present the cipher suite order as listed in the requirements SunSpecTCP-17 and SunSpecTCP-18.

SunSpecTCP-20. mbaps Devices **MUST** include the ability to disable cipher suites that are discouraged by IANA (https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml)

5.3 Role-Based Client Authorization

SunSpecTCP-21. A mbaps Server Device **MUST** provide the role-based client AuthZ as described in Section 8.4 of [MODBUS/TCP Security]. (modified from MBR-16, 17)

SunSpecTCP-22. A mbaps Devices **MUST** support the roles of ReadOnlySunSpec, GridServiceSunSpec, NetworkAdministratorSunSpec, and SuperAdministratorSunSpec.

SunSpecTCP-23. A mbaps Device **MAY** support additional roles including the IEC 62351-8 mandatory roles of VIEWER, OPERATOR, ENGINEER, INSTALLER, SECADM, SECAUD, and RBACMNT.

SunSpecTCP-24. A mbaps Device vendor **MUST** provide the Roles-to-Rights Rules Database for all roles for all supported SunSpec points.

SunSpecTCP-25. For the mandatory roles listed in SunSpecTCP-21, the mbaps Device **MUST** incorporate the roles-to-rights map provided by the SunSpec Alliance at https://github.com/sunspec/rbac.

SunSpecTCP-26. To provide mbaps role-based client authorization capability the following elements are **REQUIRED**: (MBR-18)

- X.509v3 client domain certificate ‘Role’ extension,
- mbaps server AuthZ algorithm,
- mbaps server Roles-to-Rights Rules Database.

SunSpecTCP-27. The mbaps client device **MUST** be provisioned with its X.509v3 domain certificate. (MBR-19)

SunSpecTCP-28. The X.509v3 client domain certificate **MUST** include the Role extension. (modified from MBR-20) The role extension is not required on the server certificate.

SunSpecTCP-29. The Role in the X.509v3 certificate **MUST** use the Modbus.org PEN OID 1.3.6.1.4.1.50316.802.1 (MBR-21)

SunSpecTCP-30. The Role in the X.509v3 certificate **MUST** use ASN1:UTF8String encoding (MBR-22)

SunSpecTCP-31. There **MUST** only be one role defined per certificate. The entire string will be treated as one role. (MBR-65)

SunSpecTCP-32. If no Role is specified in the X.509v3 certificate, the mbaps server **MUST** return the exception code 01 – Illegal function code (modified from MBR-23)

SunSpecTCP-33. The mbaps AuthZ Algorithm **MUST** be defined and provided by the device vendor. (MBR-24)

SunSpecTCP-34. The Roles-to-Rights Rules Database design, both syntax and semantics, **MUST** be defined by the device vendor. (MBR-25)

SunSpecTCP-35. The Roles-to-Rights Rules Database for a particular application **MUST** be configured according to the device vendor's design. (MBR-26)

SunSpecTCP-36. The Roles-to-Rights Rules Database for a particular application **MUST** be configurable. (MBR-27)

SunSpecTCP-37. The Roles-to-Rights Rules Database for a particular application **MUST NOT** have hardcoded default roles that are unchangeable. (MBR-28)

SunSpecTCP-38. The Role values used in the X.509v3 client domain certificates **MUST** be consistent with the device vendor's design of the Roles-to-Rights Rules Database. (MBR-29)

SunSpecTCP-39. The mbaps server **MUST** extract the client Role from the received X.509v3 client domain certificate. (MBR-30)

SunSpecTCP-40. If the MBAP protocol handler for authorization rejects a request it **MUST** use the exception code 01 – Illegal function code. (MBR-31)

SunSpecTCP-41. If any portion of the MBAP request is rejected because of authorization, the Device **MUST** return an exception and no additional information.

5.4 Public Key Infrastructure

5.4.1 TLS Key Exchange

SunSpecTCP-42. mbaps Devices using ECC technology **MUST** support at least P-256 NIST curve. (MBR-61)

SunSpecTCP-43. mbaps Devices using ECC technology **MUST** specify the curves used in their 'Client Hello' using the Supported Elliptic Curves extension in [RFC4492]. (MBR-63)

SunSpecTCP-44. mbaps Devices using ECC technology **MUST** specify the point format used in their 'Client Hello' using the Supported Point Format extension in [RFC4492]. (MBR-64)

5.4.2 TLS Authentication

SunSpecTCP-45. A mbaps Device **MUST** support the TLS Client-Server Mutual Authentication Handshake. (MBR-41)

SunSpecTCP-46. mbaps Device **SHOULD** support the TLS Resumed Session Handshake on Client and Server. (MBR-42)

SunSpecTCP-47. mbaps Device **MAY** support the TLS Session Ticket resumption on Client and Server. (MBR-43)

SunSpecTCP-48. mbaps Servers **MUST** reject a TLS Handshake where the Client has not responded to a Client Certificate request with certificate. (MBR-44)

SunSpecTCP-49. mbaps Devices X.509v3 **MAY** use self-signed certificates. The private key **SHOULD** follow the certificate lifecycle defined in the NIST Special Publication (SP) 800-57.

SunSpecTCP-50. For communications routed on a public network, mbaps Devices **MUST** provide X.509v3 Certificates signed by a Certificate Authority.

SunSpecTCP-51. mbaps Devices **MUST** send the entire certificate chain down to the root CA when sending their certificate. (MBR-46)

SunSpecTCP-52. X.509v3 Certificates provided by mbaps Devices **MUST** conform to the requirements of [RFC5280]. (MBR-47)

SunSpecTCP-53. If a mbaps Device is to be used in a scenario where encryption is required, then a cipher suite with the required encryption indicator **MUST** be chosen from the list at IANA’s TLS Cipher Suite Registry in the [TLS-PARAMS]. (MBR-48)

5.4.3 TLS Cryptography

SunSpecTCP-54. mbaps Devices **MUST NOT** use: (MBR-50,51,53)

- HMAC-MD5 hash algorithm
- HMAC-SHA-1 hash algorithm
- NULL HMAC hash algorithm

SunSpecTCP-55. mbaps Devices **MUST** provide the HMAC-SHA-256 hash algorithm. (MBR-52)

SunSpecTCP-56. mbaps Devices **MUST NOT** provide the HMAC-SHA-1 hash algorithm for use in the PRF function to calculate the key block as defined in [RFC5246] sections 5, 6.3 and 8.1. (MBR-54)

SunSpecTCP-57. mbaps Devices **MUST** provide the HMAC-SHA-256 hash algorithm for use in the PRF function to calculate the key block as defined in [RFC5246] sections 5, 6.3 and 8.1. (MBR-55)

SunSpecTCP-58. As early as possible in their development cycle, mbaps devices **MUST** determine that they comply with the import/export conformance policies of their respective countries for the cryptography they provide. (MBR-56)

5.5 Packet and Session Requirements

SunSpecTCP-59. mbaps devices **MUST** provide the Maximum Fragment Length Negotiation Extension as defined in [RFC6066]. (MBR-57)

SunSpecTCP-60. mbaps devices **MUST** provide the ability to negotiate a Maximum Fragment Length of 2^9 (512) bytes as defined in [RFC6066]. (MBR-58)

SunSpecTCP-61. mbaps devices **MUST** set the TLS CompressionMethod field of the ClientHello message to the value of NULL. (MBR-59)

SunSpecTCP-62. mbaps devices **MUST** provide the TLS Renegotiation Indication Extension defined in [RFC5746] to provide the secure renegotiation of TLS sessions. (MBR-60)

Appendix A (informative) Example Use Cases

A.1. Utility Control of DER Devices

In a situation where a utility would like direct control over DER devices, possibly over the public internet, the DER and utility DERMS would be commissioned with certificates with the same root of trust. The root of trust may be a national PKI Root CA or a utility owned Root CA. The Utility would use a certificate with a SuperAdministratorSunSpec Role to read and write the SunSpec Modbus holding registers.

A.2. VPP or Aggregator Control of DER Devices

Grid service providers like virtual power plant operators and aggregators need the ability to read measurements and control active and reactive power controls in the equipment. They do not need to adjust any of the protection settings, such as over/under voltage and over/under frequency trip settings. These entities will get a certificate from a certificate authority with the GridServiceSunSpec role.

A.3. DER Vendor Diagnostics Tracking for DER Operations

DER vendors typically have alternative communication channels to their equipment (HTTPS APIs, SSH, MQTT, etc.) but they may use the Modbus interfaces on the equipment to also gather telemetry data. In this case they will use the ReadOnlySunSpec role and read that data. They may also have their own PKI implementation in place for their products and embed the CA cert in the product at the time of manufacture. In some cases, DER vendors may be acting on behalf of grid operators or aggregators, in which case they would connect to the equipment using a certificate with the SuperAdministratorSunSpec or GridServiceSunSpec roles. If they needed to modify the networking configuration of the equipment, they could do with using the NetworkAdministratorSunSpec role.

A.4. DER Control for Home or Campus Microgrid Operator

The Secure SunSpec Modbus Specification has been designed such that self-signed certificates can be used for local, encrypted communications to the equipment. In those cases, the user would generate certificates and load the root CA and server CA on the product. Then using the appropriate role (e.g., GridServiceSunSpec), they would communicate with the equipment using an encrypted Modbus connection.

A.5. Homeowner DER Access

Some homeowners may only like to access the measurement data of the system while others would like to have full control over the system. Depending on the needs of the homeowner, they will get certificates that include ReadOnlySunSpec, NetworkAdministratorSunSpec, or SuperAdministratorSunSpec role either from an intermediate CA or self-provision the certs or PKI ecosystem. This will enable the user to modify all the settings on the equipment locally using an encrypted connection.

Appendix B (informative) Implementation Example

It is possible to run both a Secure SunSpec Modbus Server on port 802 and a traditional Modbus Server on port 502 on the same product. The secure interface would be used for communications routed on a public network, and the unencrypted interface could be used for local interactions. This may represent a good stopgap solution as the industry adjusts to the added complexity of the TLS requirement for Secure SunSpec Modbus.

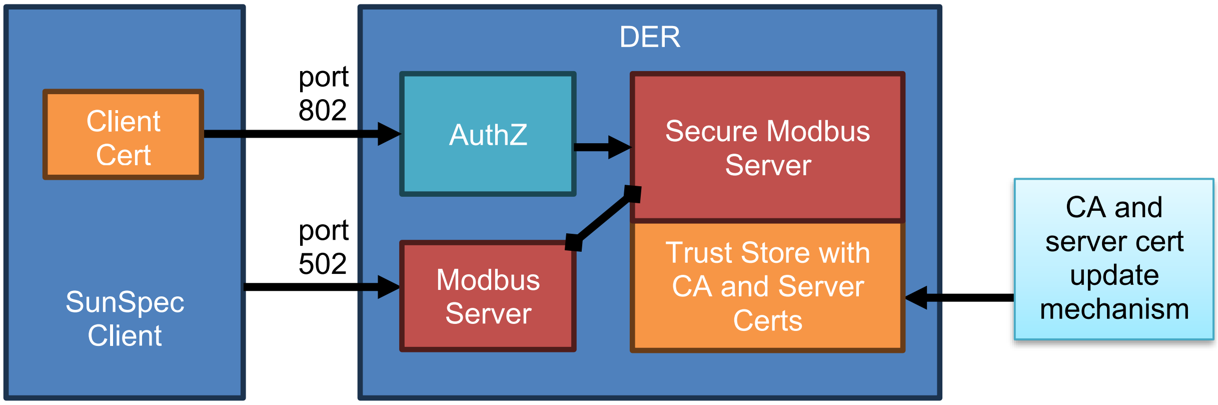

Figure 2: DER implementation example.