Common Metering Profile

IEEE 2030.5 Implementation Guide for Metering

March 3, 2021

Version 1

Status: TEST

Abstract: This document describes how to apply the IEEE 2030.5-2018 server to electrical meters in order to provide IEEE 2030.5-2018 client access from devices such as mobile handsets and laptop computers.

License Agreement and Copyright Notice

Contact Information

SunSpec Alliance

4040 Moorpark Avenue, Suite 110

San Jose, CA 95117

info@sunspec.org

About the SunSpec Alliance

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

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

About the SunSpec Specification Process

SunSpec Alliance specifications are developed by SunSpec member companies seeking to establish industry standards for mutual benefit. Any SunSpec Alliance member can propose a technical work item. Given sufficient interest and time to participate, and barring significant objections, a workgroup is formed. Workgroups meet regularly to advance the agenda of the team.

The output of a workgroup is a SunSpec interoperability specification. SunSpec interoperability specifications 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 SunSpec documents are informative, and provide recommendations regarding best practices, but are not a matter of conformance. Informative documents can be revised more freely and frequently to improve the quality and quantity of information provided.

SunSpec interoperability specifications follow this lifecycle pattern of DRAFT, TEST, APPROVED and SUPERSEDED.

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

Revision History

Revision	Date	Reason
1	03-09-2021	First publication date Status set to TEST PDF generated for review by SunSpec members

Contents

1 Introduction

This guide serves to assist manufacturers, metering system operators, and system integrators to implement an interoperable metering data retrieval system based on IEEE 2030.5, fostering “plug and play” communications-level interoperability between the metering devices and 3rd party smart devices. This guide, along with the IEEE 2030.5 specifications, is also intended to be used to develop an IEEE 2030.5 Client and Server conformance test plans and certification programs. This profile of 2030.5 is designed to meet the needs of metering data retrieval.

2 Guiding Principles

The following principles have been used to help guide the development this profile. From a communications perspective:

1. Establish a complete profile – To achieve complete interoperability a complete profile is required including a data model, messaging model, communication protocol and security. Without a complete profile specification, it would be impossible to achieve communications interoperability without additional systems integration activities.
2. Leverage existing standards and models from the IEEE 2030.5 standard – The development of a new, stand-alone standard would create additional burden on all parties and only serve to raise costs of both development and maintenance.
3. Extensibility of the specification through future revisions is required.
4. Eliminate optionality and keep to a single base specification – Optionality in the specification can serve to hinder interoperability when parties chose to implement.
5. Create a minimal specification – A simple interface serves to lower costs and improve quality.
6. Strictly focus on meter to 3rd party reading device communications. All other communications are out of scope from the perspective of this profile.
7. Implementation of the interface infers no proprietary advantage to any party – communications between the meter and 3rd parties provides a critical, but non-differentiating service. As such, the costs to all parties should be minimized to drive proliferation meter data applications.
8. Provide alternate models of implementation around a single common standard to provide customer choice, 3rd party business models and utility needs.

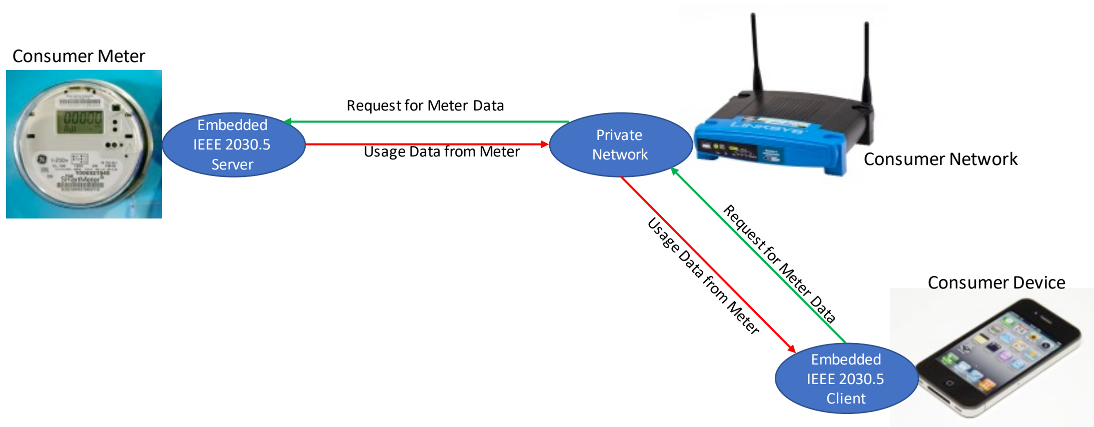
3 Communications Architecture Overview

3.1 Scope of Communications

This profile addresses the communications path between the meter and authorized 3rd party devices.

3.2 Scenarios

The basic scenario envisioned is that of a consumer owned device (Cell Phone, tablet, in home display, etc.) is allowed access to metering data so that it can be displayed to the end-use customer.



Some other use cases that could benefit from this profile:

- An in-home battery controller monitoring consumption to determine when to charge.
- An EVSE system monitoring load to determine when to charge the EV.
- Managing load in light industrial applications to minimize peak demand.
- Adding real time data to Green Button.
- Smart appliances managing their function to operate when demand is low.

All of the use cases rely on simply having access to real time usage data.

4 General Requirements

This section provides general requirements related to implementing 3rd party access to metering data. The related IEEE 2030.5 specific requirements can be found in Section 5.

4.1 4.1 Security Requirements

IEEE 2030.5 security requirements are covered in section 6.1.2. Security includes data in motion (e.g. encryption of communications), data at rest, the authentication of clients and services, as well as the authorization of all requests.

4.2 Registration and Identification of 3rd Party Devices

The registration of 3rd party devices is utility specific and is assumed to be outside the scope of this profile. The registration process may result in the delivery of a globally unique identifier (GUID) associated with a particular 3rd party device. The GUID provides a shared name between the utility and the other parties to ensure that operations and data are routed appropriately. The GUID is used to guarantee its authenticity and uniqueness within the scope of a single utility. For 3rd party devices that have an IEEE 2030.5 certificate, the GUID SHALL be derived from this certificate (see section 5.2.1.2).

4.3 Communication Interactions

To simplify communications, 3rd Party devices SHALL initiate all interactions between the Meter and the 3rd party device.

4.4 Reporting Meter Data

4.4.1 Monitor Data

Meters SHALL, as a minimum, have the capability to report the monitoring data in Table 1. Meters SHALL, as a minimum, have the capability to include the data qualifiers in Table 2.

Table 1 Monitoring Data

Monitoring Data
Demand (kW)
Delivered (kWh)
Received (kWh)

Table 2 - Data Qualifiers

Data Qualifier
Instantaneous (Latest)
Summation

4.4.2 Status Information

Status information is not required to be provided by the metering server.

4.4.3 Alarms

Alarms are not required to be provided by the metering server.

5 IEEE 2030.5 Implementation and Requirements

This section defines IEEE 2030.5 implementation requirements. The specific version of the protocol implemented SHALL be IEEE 385 2030.5-2018. While it is assumed that the reader has a working knowledge of IEEE 2030.5 concepts and operations, a brief overview of IEEE 2030.5 is provided below to help the reader understand the detailed requirements.

5.1 Overview

5.1.1 High-Level Architecture

The IEEE 2030.5 protocol implements a client/server model based on a representational state transfer (REST) architecture utilizing the core HTTP methods of GET, HEAD, PUT, POST, and DELETE. In the REST model, the server hosts resources, and the client uses the HTTP methods to act on those resources. In this guide, the server is implemented at the meter, and the client is then implemented at the 3rd party device. The client typically initiates the action, but the protocol does provide a lightweight subscription mechanism for the server to push resources to the client. This profile SHALL NOT support subscription.

5.1.2 Resources and Function Sets

In IEEE 2030.5, a resource is a piece of information that a server exposes. These resources are used to represent aspects of a physical asset such as a meter, attributes relating to the control of those assets, and general constructs for organizing those assets. IEEE 2030.5 resources are defined in the IEEE 2030.5 XML schema and access methods are defined in the Web Application Description Language (WADL). The schema is generally organized by Function Sets, a logical grouping of resources that cooperate to implement IEEE 2030.5 features. IEEE 2030.5 provides a rich set of Function Sets (e.g. Demand Response

Load Control, Pricing, Messaging, Metering, etc.) to support a variety of use cases. This guide only requires the subset required to meet the required metering support functionality. Metering Servers and Clients SHALL support all IEEE 2030.5 function sets and resources as indicated in Table 7. Any additional function set specific requirements will be detailed in the sections below.

Table 3 - Required Function Sets and Resources

Function Set	Metering Server	Metering Client
Time	MUST	MUST
Device Capability	MUST	MAY
Metering	MUST	MUST
Security	MUST	MUST

5.1.2.1 Time

The metering server uses the Time function set to communicate the current time to clients. Time is expressed in Coordinated Universal Time (UTC). Server event timing is based on this time resource.

5.1.2.2 Device Capability

The metering server uses the DeviceCapability resource to enumerate the function sets it supports. Clients use this function set to discover the location (URL) of the enumerated function sets.

5.1.2.3 Metering

The Metering function set provides the resources needed to support metrology measurements (e.g. Delivered Energy, Received Energy, Demand, etc.).

5.2 IEEE 2030.5 Requirements

3rd Party Metering Clients SHALL meet all IEEE 2030.5 mandatory requirements that are described in the standard for each of these sections/functions.

5.2.1 Security Requirements

HTTPS SHALL be used in all communications scenarios. IEEE 2030.5 defines a specific security framework (i.e. PKI infrastructure). However, this framework may not be compatible with the utility's security and IT infrastructure requirements. 3rd Party Metering Clients SHALL support the required IEEE 2030.5 security framework. In all cases the utility should specify the security framework based on its security and IT requirements. Possible PKI options include:

- Use of the IEEE 2030.5 or SunSpec defined Certificate Authority (CA)
- Contracting with a commercial, third-party certificate authority chain to generate certificates
- Implementing their own private certificate authority chain to generate certificates
- Using self-signed certificates

5.2.1.1 TLS and Cipher Suites

TLS version 1.2 SHALL be used for all HTTPS transactions.

IEEE 2030.5 specifies a single cipher suite for HTTPS communications, namely: TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 using the elliptic curve secp256r1. Servers and Clients SHALL support the IEEE 2030.5 cipher suite.

5.2.1.2 Certificates

Certificates provide a mechanism to authenticate identities during the TLS handshake. All Metering Servers and Clients SHALL have a unique valid certificate. A valid certificate is a certificate that conforms to the IEEE 2030.5 security. A valid certificate SHALL be used in all IEEE 2030.5 TLS transactions. Certificates for Metering Servers and Clients SHALL only be provisioned upon successful completion of Conformance Testing.

The GUID for both Metering Servers and Clients SHALL be the IEEE 2030.5 Long Form Device Identifier (LFDI) which is based on the 20-byte SHA-256 hash of the device's certificate.

5.2.1.3 Authentication

The Metering Servers and Clients perform mutual authentication during the TLS handshake by exchanging and authenticating each other's certificate. The certificates specified by each utility SHALL be used for authentication. Authentication consists of verifying the integrity of the received certificate, checking the certificate has not expired, and verifying the certificate chains back to the correct root certificate authority. If authentication fails, the authenticator SHOULD issue a TLS Alert –Bad Certificate and close the connection.

5.2.1.4 Authorization

The Metering Server will be given a list of authorized devices (i.e. approve 3rd party devices) that are permitted to communicate with the server. For Metering Clients, the authorization list SHALL be based on the LFDI since the SFDI may not provide enough collision protection for a large population (e.g. 1 million) of devices. If the device is not on the authorization list, the Metering server SHOULD return an HTTP error code (e.g. 404 – Not Found) to terminate the transaction.

5.2.1.5 Access Control

Once a device (i.e Metering Client) has been authenticated and authorized, it potentially has access to resources on the Metering server. The Metering server controls access to resources based on Access Control Lists (ACL). In theory, every resource on the Metering server can have its own ACL. The utility SHALL establish the permissions for read, write, control, and other interactions, based on agreements on which interactions are authorized between each 3rd party device and the metering server. For example, role-based access control may be used to establish these permissions for different roles.

Another aspect of Access Control is that the metering server may present different resource information based on the identity of the device making the request. This is done for both efficiency and/or privacy reasons.

5.2.2 Commissioning and Identification of Clients

IEEE 2030.5 uses two identifiers, both of which are hashes of the device certificate. The Short-Form Device Identifier (SFDI) is based on a 36-bit SHA256 hash of the device certificate and is expressed as 12 decimal digits. The Long-Form Device Identifier (LFDI) is the first 20 bytes of the SHA256 hash of the device certificate.

5.2.3 Communication Interactions Requirements

The Metering Server will be hosted on the meter. 3rd party devices, once authenticated and authorized, will request metering data from the metering server. The metering server is not required to support subscription.

5.2.3.1 Monitor Data

Metering Servers and Metering Clients SHALL use the IEEE 2030.5 Metering function set to report metrology data. Each of the monitoring data in Table 4 maps to a MeterReading with a ReadingType specifying the unit of measure (uom) and dataQualifier. All metering servers SHALL support the data shown in table 4 and MAY support other data.

Table 4 - Monitoring Data

Monitoring Data	ReadingType uom
Instantaneous Demand	38 (Watts)
Summation Delivered	72 (WattHours)
Summation Received	72 (WattHours)

6 Metering IEEE 2030.5 Implementation

6.1 General Operation

This section describes the operation of the IEEE 2030.5 metering server and client.

6.1.1 Registration

Metering Servers SHALL register an SVR/TXT record pair for their Usage Point (UPT) sub-type.

Metering Clients SHALL use mDNS to discover the metering servers.

6.1.2 Security, Authentication, and Authorization

Once the Metering Client has determined the location (URL) of the Metering server's *UsagePointList* resource, the Client performs an HTTPS GET of this resource. This action initiates a TLS handshake to establish a secure connection. Certificates are exchanged between the Metering server and client during the handshake. The metering server authenticates the client's certificate and verifies whether it is authorized via the access control list.

Once the metering server authenticates and authorizes the client, it returns the contents of the *UsagePointList* resource with an HTTP response code of 200 – OK. If the Client fails to authenticate or is not authorized, the metering server can abort the TLS connection by sending a TLS Alert message, or it can complete the TLS connection but return an HTTP response code of 403 – Forbidden.

6.1.3 Client Access to Metering Data

Once the Client has the URL of the UsagePointList it uses the procedures outlined in IEEE 2030.5 to navigate the metering server's data to read the requested information. The following sub-sections give an example of the data a metering server would make available.

6.1.3.1 Device Capabilities

The Metering server will host a Device Capabilities resources.


```xml
<DeviceCapability xmlns="urn:ieee:std:2030.5:ns" href="/dcap">
   <TimeLink href="/tm"/>
   <UsagePointListLink href="/upt" all="1"/>
   <SelfDeviceLink href="/sdev"/>
</DeviceCapability>
```


Figure 1 - Example Device Capabilities

6.1.3.2 Time

The Metering server bases many of its measurements on time. It therefore hosts a Time resource containing its time attributes.


```xml
<Time xmlns="urn:ieee:std:2030.5:ns" href="/tm">
   <currentTime>1604963587</currentTime>
   <dstEndTime>1583661600</dstEndTime>
   <dstOffset>3600</dstOffset>
   <dstStartTime>1583661600</dstStartTime>
   <quality>7</quality>
   <tzOffset>-28800</tzOffset>
</Time>
```


Figure 2 - Example Time Resource

6.1.3.3 Self Device

The Metering server hosts a Self Device resource.


```xml
<SelfDevice xmlns="urn:ieee:std:2030.5:ns"     href="/sdev">
  <DeviceInformationLink href="/sdev/sdi"/>
  <sFDI>263739118398</sFDI>
</SelfDevice>
```

Figure 3 - Example Self Device

6.1.3.4 Device Information

The Metering server hosts a Device Information resource describing the given instance of the metering server.

```xml
<DeviceInformation xmlns="urn:ieee:std:2030.5:ns" href="/sdev/sdi">
  <lFDI>62401F51F72EC55E4A00203257859AAB5612089B</lFDI>
  <mfDate>1601539200</mfDate>
  <mfHwVer></mfHwVer>
  <mfID>1233</mfID>
  <mfModel>Itron Meter</mfModel>
  <mfSerNum>ABCD-1234</mfSerNum>
  <primaryPower>1</primaryPower>
  <secondaryPower>0</secondaryPower>
  <swActTime>1601539200</swActTime>
  <swVer>0.1.0</swVer>
</DeviceInformation>
```

Figure 4 - Example Device Information

6.1.3.5 Usage Point List

Figure 5 shows an example of a Usage Point List. The metering client reads this resource from the metering server to determine the URI of the specific Usage Point.

```
<UsagePointList xmlns="urn:ieee:std:2030.5:ns" href="/upt" subscribable="0" all="1"
    results="1" pollRate="900">
   <UsagePoint href="/upt/1">
      <mRID>AAAA0100000000000000000000004D1</mRID>
      <description>Meter Usage Point</description>
      <roleFlags>00</roleFlags>
      <serviceCategoryKind>0</serviceCategoryKind>
      <status>1</status>
      <MeterReadingListLink href="/upt/1/mr" all="3"/>
   </UsagePoint>
</UsagePointList>
```

Figure 5 - Example Usage Point List

6.1.3.6 Meter Reading List

The Meter Reading List contains records describing the different readings this usage point is collecting along with links to the readings.


```xml
<MeterReadingList xmlns="urn:ieee:std:2030.5:ns" href="/upt/1/mr" subscribable="0" all="3"
results="3">
  <MeterReading href="/upt/1/mr/3">
    <mRID>BBBB0300000000000000000000000004D1</mRID>
    <description>Current Summation Delivered</description>
    <ReadingLink href="/upt/1/mr/3/r"/>
    <ReadingTypeLink href="/rt/3"/>
  </MeterReading>
  <MeterReading href="/upt/1/mr/2">
    <mRID>BBBB0200000000000000000000000004D1</mRID>
    <description>Current Summation Received</description>
    <ReadingLink href="/upt/1/mr/2/r"/>
    <ReadingTypeLink href="/rt/2"/>
  </MeterReading>
  <MeterReading href="/upt/1/mr/1">
    <mRID>BBBB0100000000000000000000000004D1</mRID>
    <description>Instantaneous Demand</description>
    <ReadingLink href="/upt/1/mr/1/r"/>
    <ReadingTypeLink href="/rt/1"/>
  </MeterReading>
</MeterReadingList>
```


Figure 6 - Example Meter Reading List

6.1.3.7 Reading Type

The Reading Type record contains the attributes of the associated Meter Readings.

```xml
<ReadingType xmlns="urn:ieee:std:2030.5:ns" href="/rt/1">
  <accumulationBehaviour>12</accumulationBehaviour>
  <commodity>1</commodity>
  <dataQualifier>2</dataQualifier>
  <flowDirection>1</flowDirection>
  <kind>8</kind>
  <powerOfTenMultiplier>0</powerOfTenMultiplier>
  <uom>38</uom>
</ReadingType>
```

6.1.3.8 Reading

The Reading resource contains the actual reading data along with information specific to this reading.

```xml
<Reading xmlns="urn:ieee:std:2030.5:ns" href="/upt/1/mr/1/r">
  <qualityFlags>01</qualityFlags>
  <timePeriod>
    <duration>1</duration>
    <start>1604963861</start>
  </timePeriod>
  <value>-320</value>
</Reading>
```

Figure 8 - Example Reading