CitiPower and Powercor Utility Interconnection Handbook

CitiPower Pty Ltd and Powercor Australia Ltd
CPPAL-GU-0004

Disclaimer
The master document is controlled electronically.
Ensure latest version prior to use.

Table of Contents

List of Figures

List of Tables

1. Purpose

To address the growing minimum demand risks, the Victorian Government has introduced new legislation that require all new, upgrading and replacement rooftop solar systems to be remotely turned down or switched off in an emergency. For more information, refer to: [Victoria's Emergency Backstop Mechanism for rooftop solar | Engage Victoria].

This requires all new, upgraded and replaced solar sites of capacity less than or equal to 200kVA to be capable of receiving and adhering to CSIP-AUS for all applications from 1 October 2024[1]. The Low Voltage (LV) Distributed Energy Resource Management System (DERMS) forms one of the systems that will enable CitiPower and Powercor (CPPAL) to connect and manage these installations.

CSIP, and by extension CSIP-AUS, regularly refer to a utility interconnection handbook to provide additional detail that may be utility-specific. This document aims to provide supplementary information for technology providers, including original equipment manufacturers (OEM's), who are developing technology compatible with the CPPAL LV DERMS and utility server.

Additionally, this document describes the process by which a Software Communications Client(SCC) and inverter series can connect to the LV DERMS production systems.

This document serves as a supplementary document alongside IEEE 2030.5:2018, SA HB-218:2023, CSIP and CSIP-AUS communications client test procedures to assist with interfacing with the Utility Server.

Other relevant information for service providers can be found in the associated documents available on request:

- Interoperability Quick Start Guide and Test Procedure: Guide to connect to CPPAL test environment and steps to onboard OEM systems to CPPAL systems including interoperability test procedure.
- LV DERMS CSIP AUS External Party API: Detailed description of Application Programming Interface (API) and Public Key Infrastructure (PKI) requirements to integrate with CPPALs utility server.

This document will be reviewed regularly and amended as required to reflect changes in standards, the application of new technologies, changes to procedures and field experience.

All enquiries relating to this document shall be directed to the email address shown below.

Email: oem_onboarding@powercor.com.au

2. Document Scope

The scope of this document is limited to:

- The requirements expected of software communications clients to connect to the CPPAL utility server and expected functionality in production.
- The registration, connection, and capability testing steps required to connect to our LV DERMS Production systems.
- Connection requirements for connecting to customer site devices.
- OEM troubleshooting and error codes.

Out of scope:

- OEM onboarding and testing process.

For any new OEM that requires guidance on Onboarding to LV DERMS Utility Server refer to the document "LV DERMS Interoperability Quick Start Guide and Test Procedure".

[1] Embedded networks must only comply from 1 January 2025.

3. LV DERMS Communication Models

3.1 Introduction

This section outlines the available communication models that are in scope for the CPPAL LV DERMS. Four communication models are possible between the Utility Server and the DER End Device as illustrated below. In all cases communications between the Utility Server and the Software Communications Client shall be via the internet and shall comply with *IEEE 2030.5:2018*.

3.2 Direct to Inverter Communications Model

For a small DER installation such as residential rooftop solar with a single inverter one method to be CSIP-AUS compliant is to incorporate the Software Communications Client in the inverter enabling direct communications between the Utility Server and the DER. Fail-safe operating modes shall be implemented at each site at the end device.

Figure 1: Direct to Inverter Communications Model

3.3 Gateway/GFEMS Communications Model

Rather than having direct communications between the Utility Server and the inverter, it is possible to communicate to a Gateway which in turn communicates with the inverter. This option may be used if the inverter is not capable of acting as the Software Communications Client. The Gateway can be used for larger or more complex installations with multiple End Devices such as solar inverters, battery energy storage, and electric vehicle charging or Vehicle to Grid (V2G) technology. When used this way the Gateway is referred to as the Generating Facility Energy Management System (GFEMS). The Gateway acts to collect data from and control the various End Devices and may be seen as a single DER device to the Utility Server. In this configuration fail-safe operating modes shall be implemented at each site (either in the End Device or within the local Gateway/GFEMS).

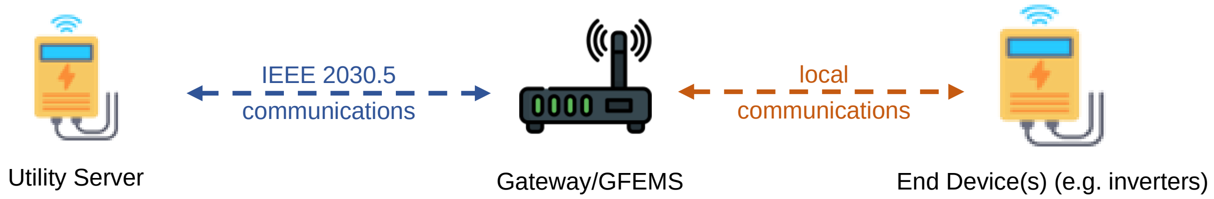


Figure 2: Gateway/GFEMS Communications Model

3.4 Aggregator Communications Model

The Utility Server can communicate with an Aggregator Platform which acts as the Software Communications Client. The Aggregator Platform then communicates with the various End Devices via a range of other communications technologies. The End Devices need not be located within one electrical installation and can be distributed across a large geographic area but aggregated together by a single entity. It remains necessary for the Utility Server to be able to identify each individual DER as an IEEE 2030.5 End Device so that each End Device can be monitored and controlled individually. Furthermore, fail-safe operating modes shall be implemented at each site (such as in the End Device), so that fail-safe export limits will operate correctly if there is a failure of the Aggregator Platform.

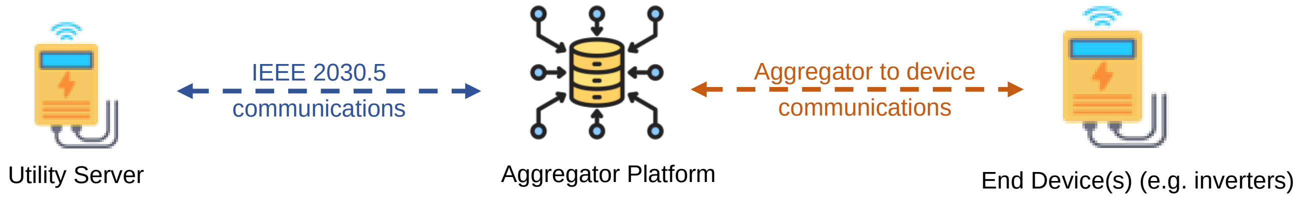
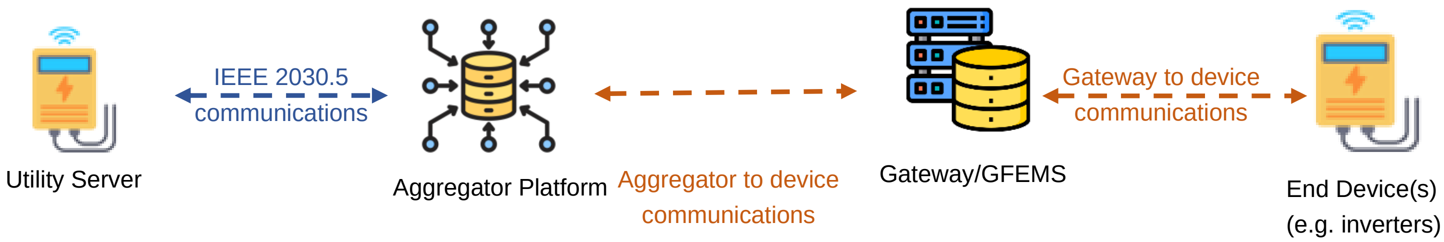


Figure 3: Aggregator/Proxy Communications Model

3.5 Aggregator Gateway Communications Model

The Utility server can communicate to end devices through a combination of the Gateway and Aggregator Communication Models. In this model, the Utility Server communicates to an Aggregator Platform as the Software Communications Client. The Aggregator Platform can then communicate with a combination of End Devices and/or Gateway devices. As with the previously described Aggregator Communications Model, the End Devices and Gateways need not be located within one electrical installation and can be distributed across a large geographic area but aggregated together by a single entity. It remains necessary for the Utility Server to be able to identify each individual site as an IEEE 2030.5 End Device so that each End Device can be monitored and controlled individually. Furthermore, fail-safe operating modes shall be implemented at each site (either in the End Device or within a local Gateway/GFEMS) so that fail-safe export limits will operate correctly if there is a failure of the Aggregator Platform.



Note

Default settings or modes for autonomous functions shall not be changeable by IEEE2030.5. The autonomous functions should be configured per existing national standards or comply with jurisdictional requirements.

4. Site Registration Process

4.1 Purpose

Registration is the process through which a new SCC representing a site is made known to the CPPAL Utility Server. This process is completed upon installation and is required to implement the Victorian Emergency Backstop Mechanism. There are multiple ways in which registration can be achieved in CSIP-AUS, this section defines the supported registration method for CPPAL Utility Server.

4.2 Technology Selection and Onboarding

From 1st February 2025, only approved inverters and software communication devices that can communicate with our systems will be able to be installed on our network.

If a device is not approved and listed on our website, it won't be possible to select it as part of an alteration request. If the inverter is not on the list, please check with your inverter supplier they have engaged with us. The list on our website will continue to be updated as new devices are tested and approved. Please check the list regularly to remain up to date.

4.3 NMI Whitelisting

In addition, prior to device registration a National Meter Identifier (NMI) must first be whitelisted in our systems. This process ensures that only valid Distributed Energy Resources (DER) requiring emergency backstop enablement are connected to our systems.

Before registering a DER system with our server, you must have a valid and approved Solar Pre-Approval (SPA) (applied for after 1 October 2024).

4.4 Implementation

Once the inverter(s) and export meter is installed on site, the installer must ensure to have the inverter(s) or the communication gateway connected to the internet. **For sites <30kVA[2], if the site cannot practically connect to the internet, a static zero export limit must be applied on site.**

Once connected the installer will have to follow steps defined by the OEM to register the device. In most cases, by following steps defined by the OEM, the communications software client will register itself to the Utility Server. This process is defined as In-Band Registration. CPPAL currently only supports in-band registration for aggregator based communications models.

In some circumstances the communication software client will fail to register into the utility server and an Out-of-Band registration will be required. Both methods of registration are described below.

4.4.1 In-Band Registration

During In-Band registration, the installer will have to follow below steps:

1. Install inverter(s) and export meter on site.
2. Use OEM app/portal to connect the EndDevice to the internet.
3. **Follow instructions provided by the OEM** to register the device (this may include providing the 11 character site NMI).
4. Once completed, depending on the communication model as described in section 0, the EndDevice or it's aggregator will generate a 40 character Long Form Device Identifier (LFDI) and automatically publish this code along with the NMI to the CPPPAL utility server (find more about LFDI in section 7 of this document).
5. Once the LFDI is published to the server, the End Devices will be authorised to initiate communications with the Utility Server by posting to the End Device endpoint as described in section 6.1.4 of CSIP-AUS.
6. Once client is registered via the OEM portal/app, the installer (on site) shall use one of the following portals to commence the New Alteration Request, verify the registration success and finalise the commissioning process.

- For installations within CitiPower and Powercor distribution network use eConnect

[2] Sites >30kVA must practically connect under emergency backstop mechanism.

For in-band registration the communications software client must post the NMI to the CPPAL Utility Server. This is achieved utilising the Connection Point registration extension described in CSIP-AUS (Annex E). If successful, communications to the site will commence.

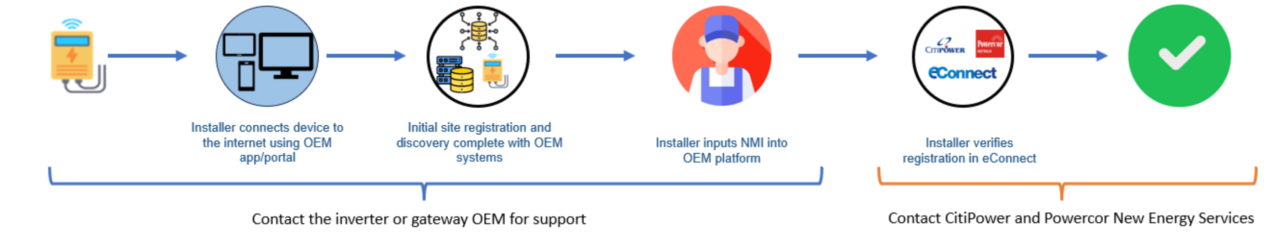


Figure 5: End Device In-Band registration process

4.4.2 Out-of-Band Registration

During Out-of-Band registration, the installer will have to follow below steps:

1. Install inverter(s) and export meter on site.
2. Use OEM app/portal to connect the EndDevice to the internet.
3. **Follow instructions provided by the OEM** to register the device (this may include providing the site NMI).
4. Once completed, depending on the communication model as described in section 0, the EndDevice or it's aggregator will generate a 40 character LFDI. During Out-band registration the LFDI **will not automatically** publish to CPPPAL utility server (Find more about LFDI in section 7 of this document).
5. Installer **must copy** the generated LFDI from the OEM or the aggregators app/portal and manually provide to CPPAL. Devices will be authorised as they initiate communications with the Utility Server by posting to the End Device endpoint as described in section 6.1.4 of CSIP-AUS

1. Once the EndDevice is registered and LFDI generated, the installer (on site) shall use one of the following portals to commence the New Alteration Request to **provide the LFDI**, verify the registration success and finalise the commissioning process.

- For installations within CitiPower and Powercor distribution network use eConnect.

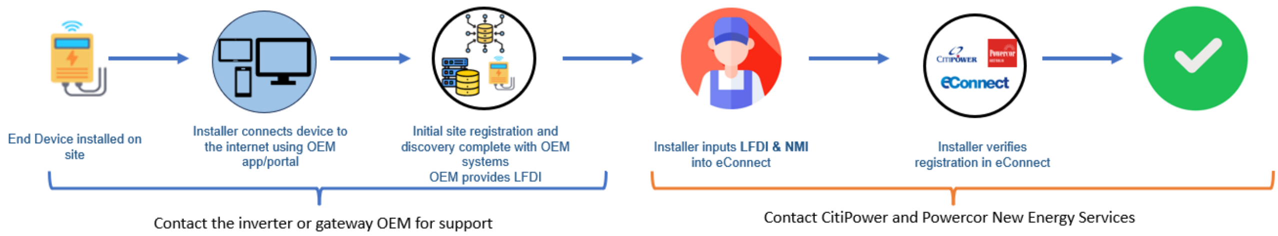


Figure 6: End Device Out-of-Band registration process

5. Capability Test

5.1 Purpose

The Capability Test is required to validate site connectivity with the Utility Server and ensure the site is compliant with the Victoria Government Emergency Backstop requirement. For more information, please refer to Victoria's Emergency Backstop Mechanism for rooftop solar | Engage Victoria.

This section is included to inform technology providers on how the capability test will operate from a functional perspective. Further materials will be developed to assist solar installers in executing the test and made available at https://www.powercor.com.au/emergency-backstop.

5.2 Process

The capability test is intended to be completed by the installer to ensure the system is compliant before leaving site. The test shall be completed via eConnect.. Upon completion of the test, approved record for the corresponding site, and test progress, meter readings and results will be displayed against this record.

Further information including solar installer resources can be found at https://www.powercor.com.au/emergency-backstop

The capability test is designed to validate remote communications and site setup. The test has been designed to minimise additional time and effort during installation and should take on average 5-10 minutes to complete. Prior to test commencement the site must be commissioned and registered with CPPAL per the Registration Specification defined in section 0.

After registration of the site has occurred, system parameters will be configured with a 1-minute poll/post rate and be set to a default export limit of 0kW.

The faster poll/post rate will enable the system to complete the capability test quicker which will minimise additional time required for installers onsite.

CPPAL will utilise the default export limit of 0kW which will apply to the site whenever the connection is lost to the utility server. **Note that the site will not start receiving its approved export limit (i.e. it will stay on its default export of 0kW) until after the capability test and alteration request has been successfully closed out.**

The high-level installation to capability test process is shown in Figure 7 below. Upon successful completion of the capability test the site will be re-configured with a poll/post rate of 5 minutes to be used under system normal operations.

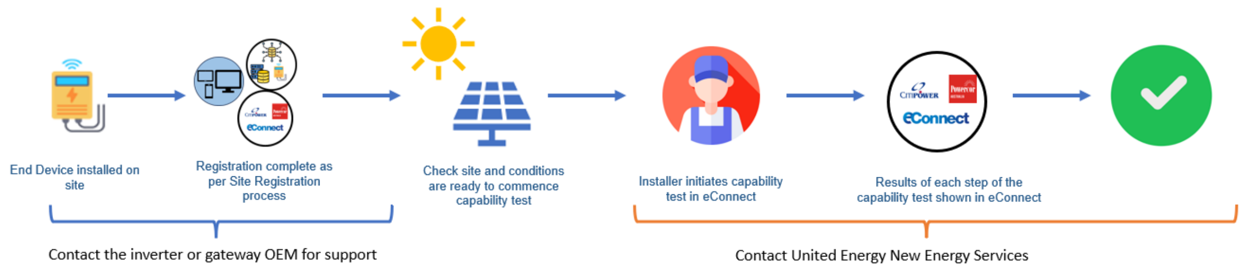


Figure 7: Installation to capability test process

Once a solar installer selects Run Test they'll see a list of four tests. Upon execution of the test, CPPAL connection portals will display the progress and result of the tests (pass or fail) and provide reasons for failure where appropriate so the solar installers can track the progress of each test.

The DER must be generating at least 1kW during the test in order to pass (i.e. the test will fail at night or if insufficient sunlight). Given that the successful test would require solar generation (sunlight), the test can be executed remotely even after the installer has left the site.

Also, depending on the site setup, any battery storage may need to be disabled to complete the capability test step 3.

5.3 Test Details

The diagram below outlines capability test which comprises 4 steps. Further detail is then provided on each step in the subsequent sections.

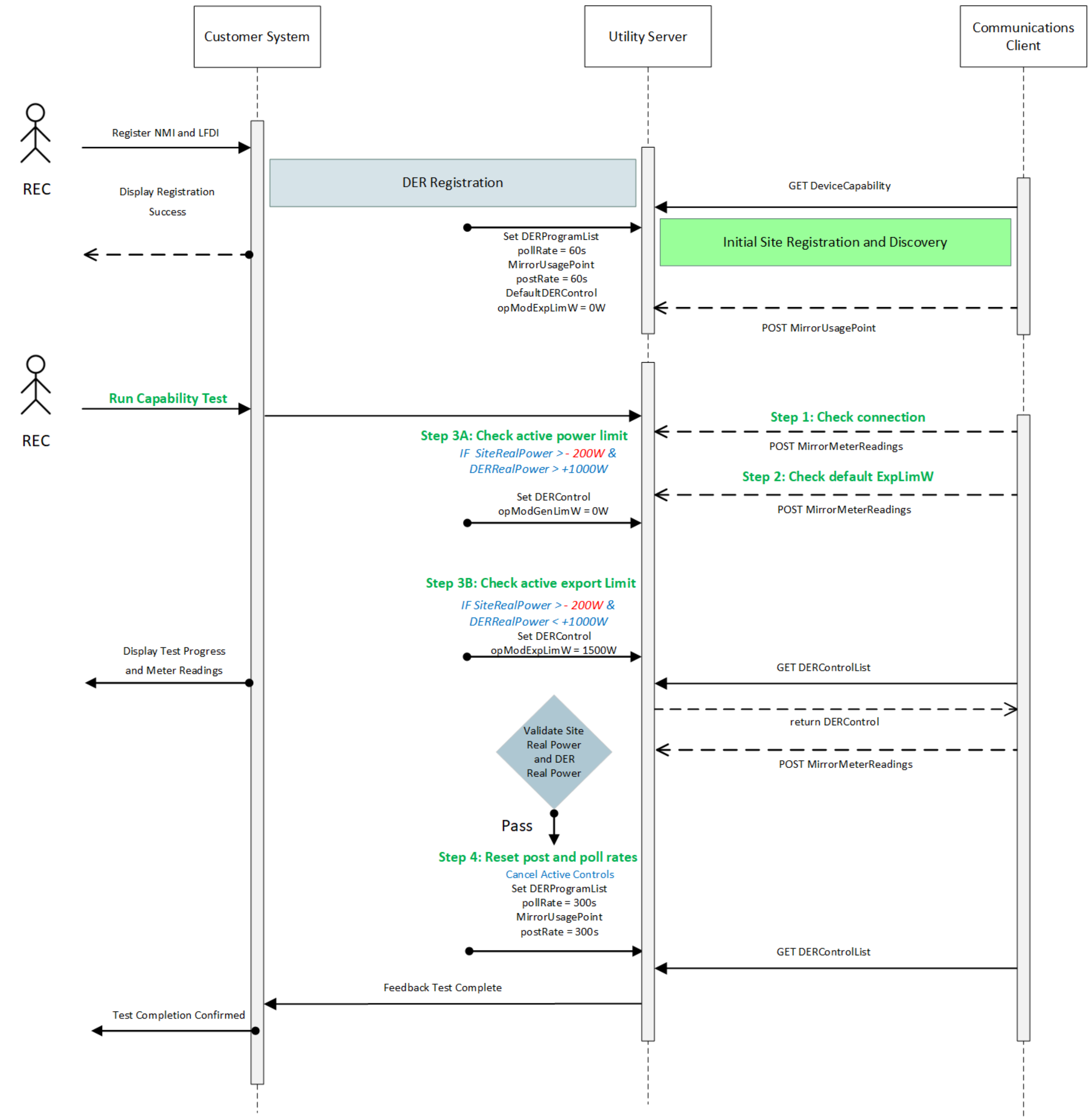


Figure 8: Capability Test Integration Steps

Step 1 - Confirm connection has been made:

- At the start of this test a 1-minute poll/post rate and a default export limit of 0kW will be set (the "DefaultDERControl") will be re-sent to ensure that it has been received.
- This step then checks the network connection status to make sure the rooftop solar system is connected to the internet and can communicate with our network. Once real power telemetry is received from the DER and Site the test will pass. If no telemetry is received within 10 minutes the test will fail.[3]

Step 2 - Confirming adherence to default export 0kW:

- Step 2 checks to ensure that the device is adhering to the default export of 0kW is applied to the site. To do this it waits for a post of the DER and Site Real Power and confirms that the site is not exporting.
- If no telemetry is received within 3 minutes or the site is exporting the test will fail.

Step 3 - Confirming adherence to active power limit:

- This step confirms that the rooftop solar system can receive a control and is able to action it.
- Depending on the DER real power registered in step 2, either an active gen limit or an active export limit will be applied as described below.

Table 1: Capability Test Step 3 Pathways

Pathway 3A - DER real power **>1kW**: • This pathway is designed to cater for sites with a large load that may not export. • An active **generation** limit control of **0kW** will be issued upon commencement. • The test then ensures that the control is received, and that the generation reduces in response to the control. It also confirms that the site does not start exporting (i.e. the export meter is not incorrectly wired). • If no telemetry is received within 4 minutes or the site is not adhering to the above condition the test will fail.
Pathway 3B - DER real power **<1kW**: • This pathway is designed to cater for sites with a low load. • An active **export** limit control of **1.5kW** will be issued upon commencement. • The test then ensures that the control is received, and that the DER real power increases to >1kW and that the site export remains below 1.5kW. • If no telemetry is received within 4 minutes or the site is not adhering to the above condition the test will fail.

Step 4 – Resets poll/post rate to 5 mins

- The final step of this test resets the poll/post rate of the end device to 5 minutes ready for BAU operations.
- This step will pass once the utility server has confirmed the poll/post rate PUT request.
- Upon successful completion of this step 4 the installer will be able to proceed to the next step of the alteration request. **Note that the site will not start receiving its approved export limit (i.e. it will stay on its default export of 0kW) until after the alteration request has been successfully closed out.**

[3] The 10 minute timeout is designed for a test run immediately after registration to allow for end device list poll, mirror usage point creation and first post time. In reality, if these steps are completed prior to the capability test initiation then this step will take upto 1 minute.

6. Public Key Infrastructure (PKI)

6.1 PKI Structure and Certificate Provisioning

The communications model utilised directly impacts the device certificate and LFDI generation requirements for connecting to the Utility Server. This section outlines the certificate generation requirements for different communication models.

The Utility Server supports three distinct levels of certificate chain verification. This means it can validate certificates issued by different authorities within the same hierarchical structure.

- SERCA: Smart Energy Root Certificate Authority
- MCA: Manufacturing Certificate Authority
- MICA: Manufacturing Intermediary Certificate Authority
- Device Certificate: The client certificate applied to the end device or aggregator

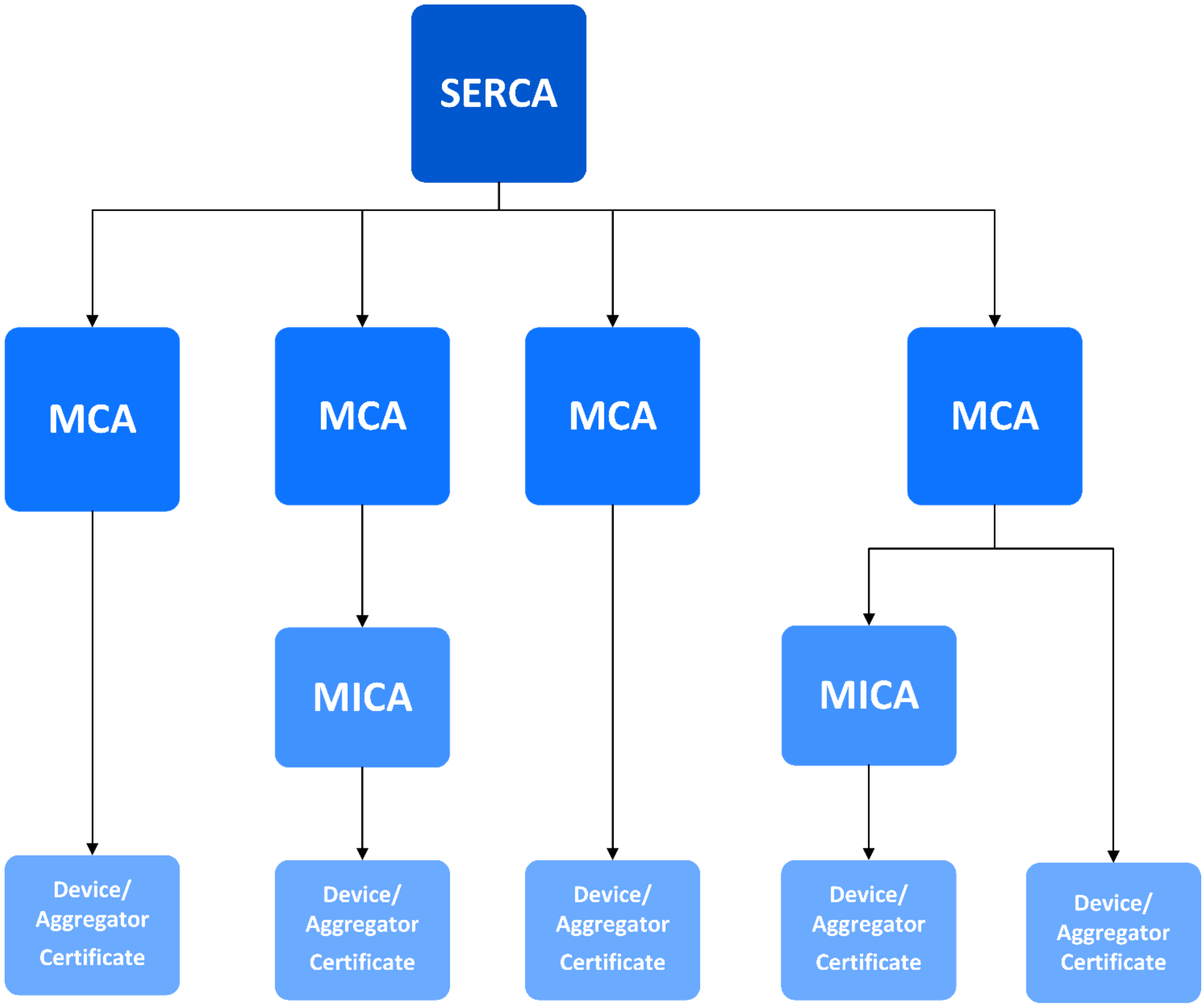


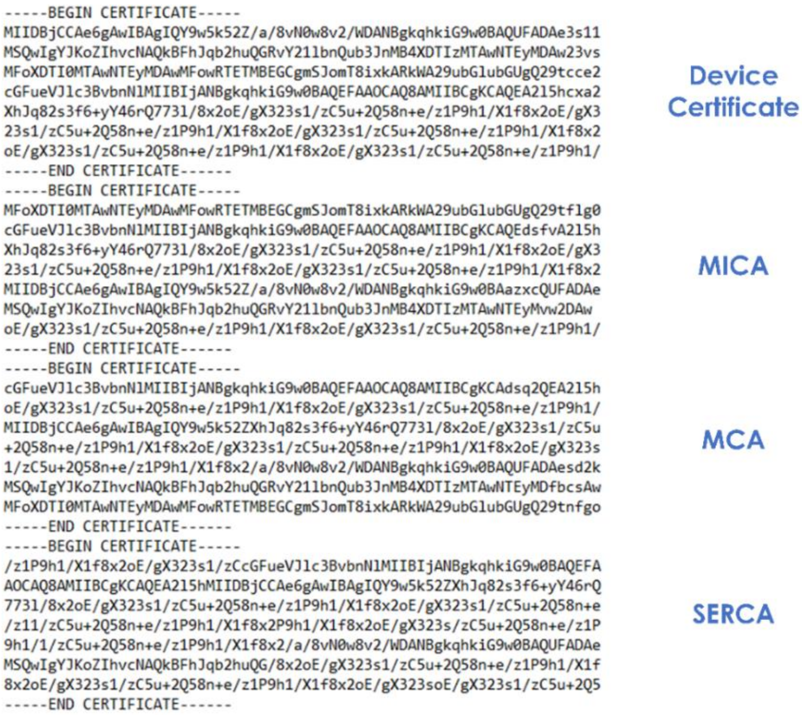
Figure 9: Example PKI Structure

The Utility Server employs a unique SERCA, separate from those used by other DNSPs. This ensures secure and controlled access to the server's services. The Utility Server requires a device certificate that is issued by and chained to our organisation's designated SERCA. Certificates issued by other SERCAs will not be accepted. Additionally, our production and non-production environments utilise distinct SERCAs. Device certificates must be issued by and chained to the appropriate SERCA for the intended environment.

The following certificate paths are accepted:

- SERCA > MCA > Device Certificate
- SERCA > MCA > MICA > Device Certificate

All certificate files must include the full certificate chain of trust. Refer to Figure 10 For example end device certificate file.



```
-----BEGIN CERTIFICATE-----
MIIDBjCCAe6gAwIBAgIQY9w5k52Z/a/8vN0w8v2/WDANBgkqhkiG9w0BAQUFADAe3s11
MSQwIgYJKoZIhvcNAQkBFhJqb2huQGRvY21lbnQub3JnMB4XDTIzMTAwNTEyMDAw23vs
MFoXDTI0MTAwNTEyMDAwMFowRTETMBEGCgmSJomT8ixkARkWA29ubGlubGUgQ29tcce2
cGFueVJlc3BvbnNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA215hcxa2
XhJq82s3f6+yY46rQ7731/8x2oE/gX323s1/zC5u+2Q58n+e/z1P9h1/X1f8x2oE/gX3
23s1/zC5u+2Q58n+e/z1P9h1/X1f8x2oE/gX323s1/zC5u+2Q58n+e/z1P9h1/X1f8x2
oE/gX323s1/zC5u+2Q58n+e/z1P9h1/X1f8x2oE/gX323s1/zC5u+2Q58n+e/z1P9h1/
-----END CERTIFICATE------
-----BEGIN CERTIFICATE-----
MFoXDTI0MTAwNTEyMDAwMFowRTETMBEGCgmSJomT8ixkARkWA29ubGlubGUgQ29tf1g0
cGFueVJlc3BvbnNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEdsfvA215h
XhJq82s3f6+yY46rQ7731/8x2oE/gX323s1/zC5u+2Q58n+e/z1P9h1/X1f8x2oE/gX3
23s1/zC5u+2Q58n+e/z1P9h1/X1f8x2oE/gX323s1/zC5u+2Q58n+e/z1P9h1/X1f8x2
MIIDBjCCAe6gAwIBAgIQY9w5k52Z/a/8vN0w8v2/WDANBgkqhkiG9w0BAazxcQUFADAe
MSQwIgYJKoZIhvcNAQkBFhJqb2huQGRvY21lbnQub3JnMB4XDTIzMTAwNTEyMvw2DAw
oE/gX323s1/zC5u+2Q58n+e/z1P9h1/X1f8x2oE/gX323s1/zC5u+2Q58n+e/z1P9h1/
-----END CERTIFICATE------
-----BEGIN CERTIFICATE-----
cGFueVJlc3BvbnNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAdsq2QEA215h
oE/gX323s1/zC5u+2Q58n+e/z1P9h1/X1f8x2oE/gX323s1/zC5u+2Q58n+e/z1P9h1/
MIIDBjCCAe6gAwIBAgIQY9w5k52ZXhJq82s3f6+yY46rQ7731/8x2oE/gX323s1/zC5u
+2Q58n+e/z1P9h1/X1f8x2oE/gX323s1/zC5u+2Q58n+e/z1P9h1/X1f8x2oE/gX323s
1/zC5u+2Q58n+e/z1P9h1/X1f8x2/a/8vN0w8v2/WDANBgkqhkiG9w0BAQUFADAesd2k
MSQwIgYJKoZIhvcNAQkBFhJqb2huQGRvY21lbnQub3JnMB4XDTIzMTAwNTEyMDfbcsAw
MFoXDTI0MTAwNTEyMDAwMFowRTETMBEGCgmSJomT8ixkARkWA29ubGlubGUgQ29tnfgo
-----END CERTIFICATE------
-----BEGIN CERTIFICATE-----
/z1P9h1/X1f8x2oE/gX323s1/zCcGFueVJlc3BvbnNlMIIBIjANBgkqhkiG9w0BAQEFA
AOCAQ8AMIIBCgKCAQEA215hMIIDBjCCAe6gAwIBAgIQY9w5k52ZXhJq82s3f6+yY46rQ
7731/8x2oE/gX323s1/zC5u+2Q58n+e/z1P9h1/X1f8x2oE/gX323s1/zC5u+2Q58n+e
/z11/zC5u+2Q58n+e/z1P9h1/X1f8x2P9h1/X1f8x2oE/gX323s/zC5u+2Q58n+e/z1P
9h1/1/zC5u+2Q58n+e/z1P9h1/X1f8x2/a/8vN0w8v2/WDANBgkqhkiG9w0BAQUFADAe
MSQwIgYJKoZIhvcNAQkBFhJqb2huQG/8x2oE/gX323s1/zC5u+2Q58n+e/z1P9h1/X1f
8x2oE/gX323s1/zC5u+2Q58n+e/z1P9h1/X1f8x2oE/gX323soE/gX323s1/zC5u+2Q5
-----END CERTIFICATE------
```


Figure 10: Example End Device Certificate File

6.1.1 Aggregator/Proxy Certificate Provisioning

It is preferred that Aggregator/Proxy OEMs handle their own offline MCA requests and management. By handling their own offline MCA, Aggregator/Proxy OEMs can directly provision certificates for their end devices and, if needed, MICA certificates. However, if Aggregator/Proxy OEMs do not have the capability to manage an offline MCA, CPPAL can directly provision Aggregator/Proxy device CSRs from a CPPAL managed MCA. Refer to Figure 12 below for example Aggregator/Proxy MCA structure and see section 9.2 for MCA CSR and end device CSR guidance.

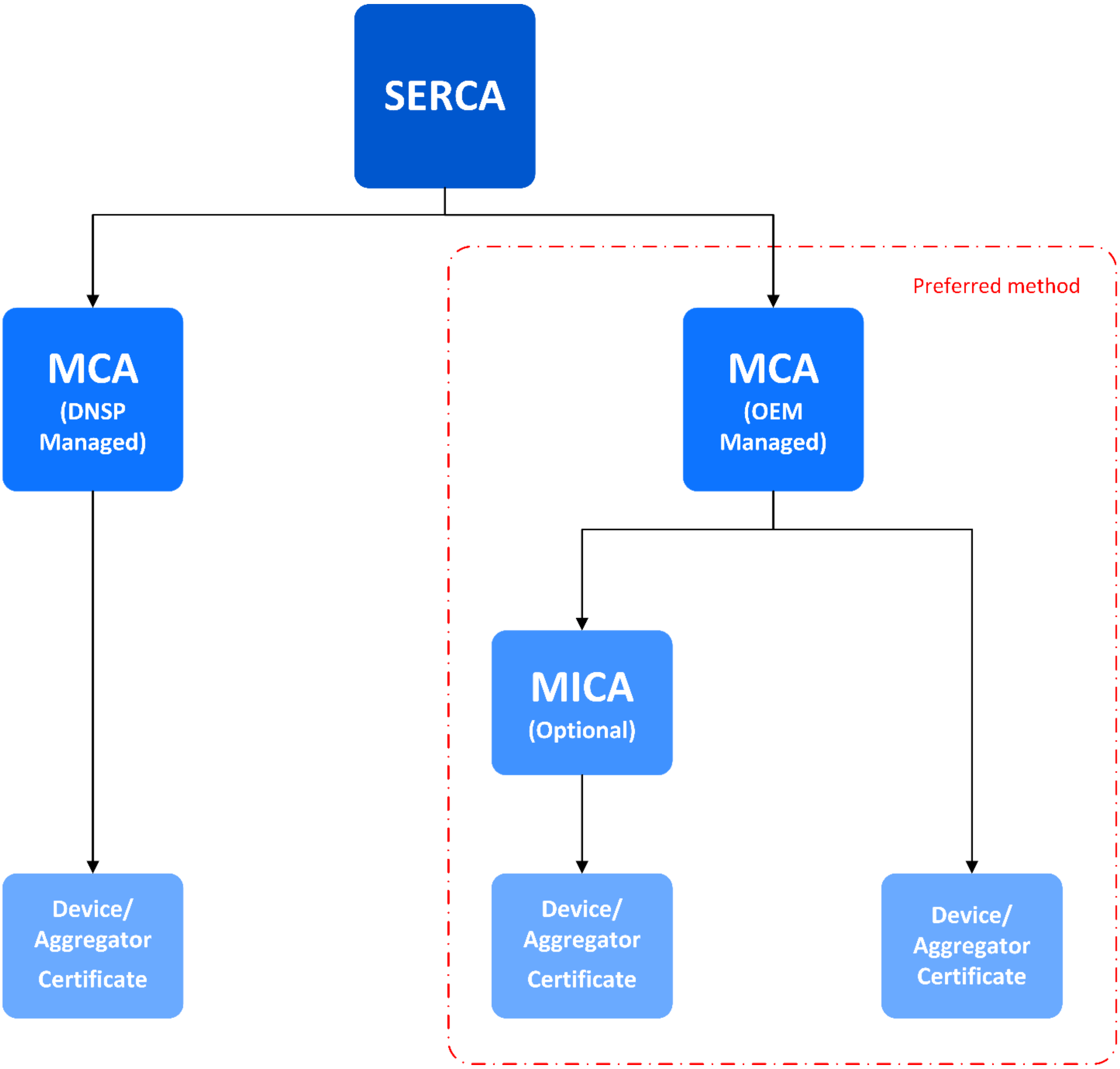


Figure 11: Aggregator/Proxy OEM PKI Structure

6.1.2 Direct Device Certificate Provisioning

Direct device OEMs will be provided an offline MCA. This MCA, provisioned directly from the SERCA, will enable OEMs to manage the issuance of end device certificates, and, if needed, MICA certificates. OEMs can provision end device certificates directly from the MCA, or from MICAs under the main MCA. Refer Figure 11 below for example Direct Device OEM MCA structure and see Section 9.2 for MICA CSR guidance.

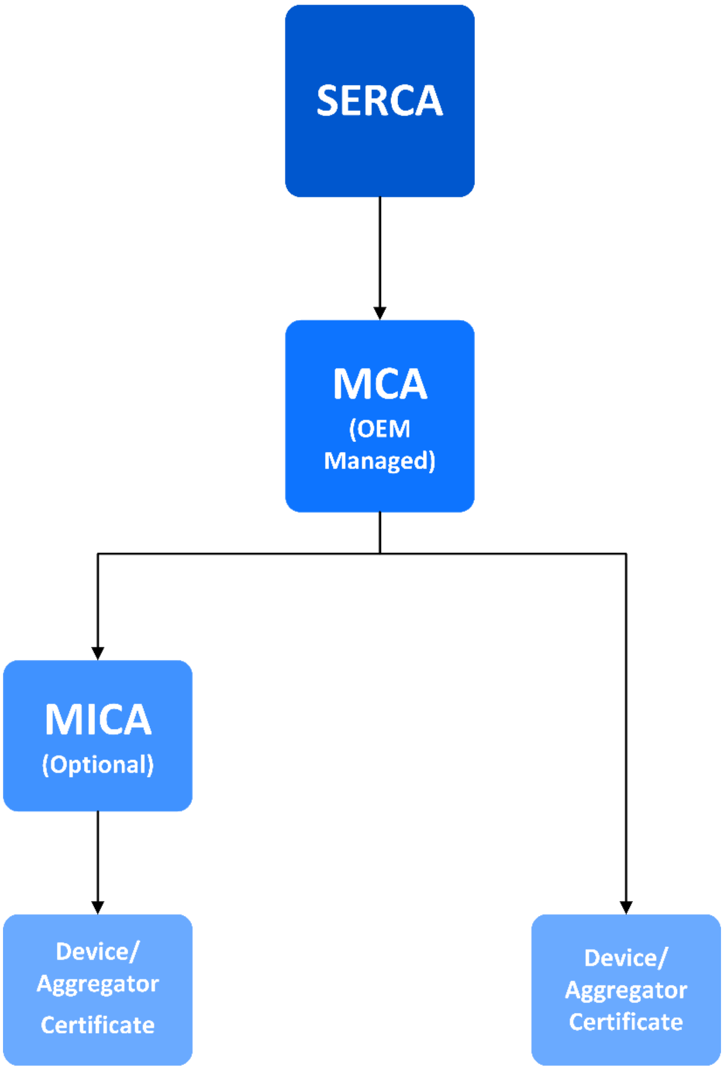


Figure 12: Direct Device OEM PKI Structure

6.2 Requesting a Certificate

To request an MCA or end device Certificate, you must generate a private key and Certificate Signing Request (CSR). Once you have generated a private key and CSR, please email the CSR to OEM_Onboarding@powercor.com.au as part of the Application process.

6.2.1 Requesting an end device certificate

IEEE2030.5 requires that any Elliptic Curve Cryptography (ECC) cipher suite used to generate a private key must use a specific mathematical formula called the "secp256r1 elliptic curve". This curve is also sometimes referred to as "prime256v1" or "NIST P-256". Here's an example of how to generate a key using this curve with OpenSSL.

1. Create new openssl.cnf file and enter the following:

```
[ req ]
req_extensions = req_ext

[ req_ext ]
subjectAltName = otherName:1.3.6.1.5.5.7.8.4;SEQ:hwmodulename

[ hwmodulename ]
# this is where you enter Manufacturer Device Type/Model OID number e.g. 1.3.6.1.4.1
hwType = OID:1.3.6.1.4.1

# this is where you enter Device unique serial number using Octet String value e.g.
4444...Octet String must be an even amount of digits
hwSerialNum = OctetString:4444
```

OIDs (Object Identifiers) for hwType:

- OEMs may use their IANA assigned PEN as the OID
- IANA OID Prefix: All IANA OIDs for PENs share a common prefix: 1.3.6.1.4.1.
- Full OID for hwType: To identify your device type using your IANA PEN, the full OID would be constructed as follows:

```
1.3.6.1.4.1.<your_iana_pen>
```

- (Replace <your_iana_pen> with your actual PEN number.)
- Optional Child Suffix: You can optionally add a child suffix to your PEN OID to further categorize different device models or versions within your organization. Here's the format:

```
1.3.6.1.4.1.<your_iana_pen> <child_suffix>
```

(The <child_suffix> can be any numerical or alphanumeric string that helps differentiate devices.)

Example: If your PEN is 123 and you want to identify a specific model with version 1.1.1, the OID would be:

```
1.3.6.1.4.1.123.1.1.1
```

- Relevance for Aggregator Solution Providers: This child suffix approach might be less relevant if you provide aggregation solutions for devices from various vendors, as using vendor-specific PENs is more appropriate in such cases.

hwSerialNum:

- This field is intended to uniquely identify a particular device instance.
- Ideal Data: The best value for hwSerialNum would be a manufacturer-assigned serial number or a version number associated with the device.
- Alternative Options: If a dedicated serial number or version number isn't available, you can:
  - Reuse PEN: Use your IANA PEN as the hwSerialNum.
  - Subset of Device SFDI: If you have a longer identifier like a Short Form Device Identifier (SFDI), you can use a relevant portion of it for hwSerialNum.
- Even Length Requirement: The hwSerialNum field must have an even number of characters (e.g., "1234", "ABCDEF").

- Odd-Length Handling: If your source identifier (PEN or SFDI subset) has an odd number of characters, simply add a leading zero (e.g., "0123" for a PEN of "123").

2. Create keypair using OpenSSL command:

```
openssl genpkey -genparam -algorithm ec -pkeyopt ec_paramgen_curve:P-256 -out "CPPAL -
csr.pem"
```

The private key you generate is extremely sensitive. It acts like a master password for your certificate, so treat it with the utmost care. It should never be shared with anyone.

Once you've created your secure private key, you can move on to generating a Certificate Signing Request (CSR). Unlike traditional internet certificates that require information like your website's domain name, *IEEE2030.5* certificates do not. In fact, these fields should be left blank during CSR creation. To avoid OpenSSL prompting you to fill in these empty fields, you'll need to include them upfront as blank values when generating the CSR.

3. Create CSR file using OpenSSL command:

```
openssl req -new -nodes -newkey ec:"CPPAL-csr.pem" -sha256 -utf8 -subj "/" -config
openssl.cnf -extensions req_ext -keyout "CPPAL.privatekey" -out "CPPAL.csr"
```

6.2.2 Requesting an MCA Certificate

MCA certificates do not require the same IEEE2030.5 OpenSSL Configuration changes.

1. Generate private key using OpenSSL command:

```
./openssl ecparam -out DERMSPIEEE2030_5MICA.pkey -name prime256v1 -genkey
```

2. Generate MCA CSR file using OpenSSL command:

```
./openssl req -new -key DERMSPIEEE2030_5MICA.pkey -nodes -
out DERMSPIEEE2030_5MICA.csr -subj "/C=AU/ST=/L=/O={YOUR ORG NAME}/CN=DERMSP IEEE
2030.5 MICA"
```

7. LFDI Generation

7.1 Introduction

The communications model utilised directly impacts the device certificate and LFDI generation requirements for connecting to the Utility Server. This section outlines the certificate and LFDI generation requirements for different communication models.

7.2 LFDI: Direct Device and Aggregators

LFDIs for direct connected devices and for aggregator instances must be generated as a hash of the device's X.509 certificate. It must adhere to the following formatting specifications:

- Character set: Hexadecimal characters only (0-9, A-F)
- Length: 40 characters

The LFDI for a given device certificate can be generated with the following openssl command:

```
openssl x509 -outform der -in client.pem | sha256sum | head -c 40 | tr '[a-f]' '[A-F]'
```

Alternatively, the LFDI for a given device certificate can be generated with the following PowerShell commands:

```
openssl x509 -outform der -in client.pem -out client.der
(Get-FileHash client.der).Hash.Substring(0, 40)
```

7.3 LFDI: Aggregator Mediated Device

Aggregators and software clients can represent multiple downstream sites or devices while communicating to the Utility Server as a single communicating client. These aggregators require a single certificate regardless of how many downstream devices it might represent. However, all downstream devices require their own LFDI to identify each site. To generate a LFDI for the downstream devices follow below steps.
NOTE: to generate LFDI for Direct devices or Aggregators follow steps illustrated in section 13.1

Downstream devices LFDIs shall be generated by the aggregator using the aggregator manufacturer's Private Enterprise Number (PEN). The PEN shall be used as the last 8 digits of the LFDI with leading zeroes.
If your organisation does not have a PEN, you can request on for free from IANA.
Aggregator Mediated Device LFDIs must adhere to the following formatting specifications:

- Character set: Hexadecimal characters only (0-9, A-F)
- Length: 40 characters

An example LFDI is as follows where [1234] is the PEN:

4B1AFA32312D2AA600ACF57E76FEBEDA00001234

8. Utility Server Details

8.1 Utility Server Environment Details

Table 2: Utility Server Environment Details

Environment Name	URL
PROD	https://dermsp.powercor.com.au:30101
SIT/Test	https://dermst.powercor.com.au:30101

9. IP Whitelisting

The CPPCUE utility server implements geo blocking of IPs to restrict access to IP addresses within Australia only. Where an aggregator solution is based outside of Australia, the IP address will need to be provided so that it can be whitelisted. Both individual IP addresses and reasonable IP ranges are acceptable for IP whitelisting.
Therefore, if an aggregator or their service provider changes IP addresses, at least 20 business days notice is required to maintain un-interrupted connectivity. To inform CPPCUE of a planned change, please email oem_onboarding@powercor.com.au

10. Client-Server Interactions

This section provides a summary of DER Client requests that are expected by the Utility Server.

Figure 13 demonstrates the workflow of DER Client requests that are submitted to the Utility Server during the initial device connection and discovery.

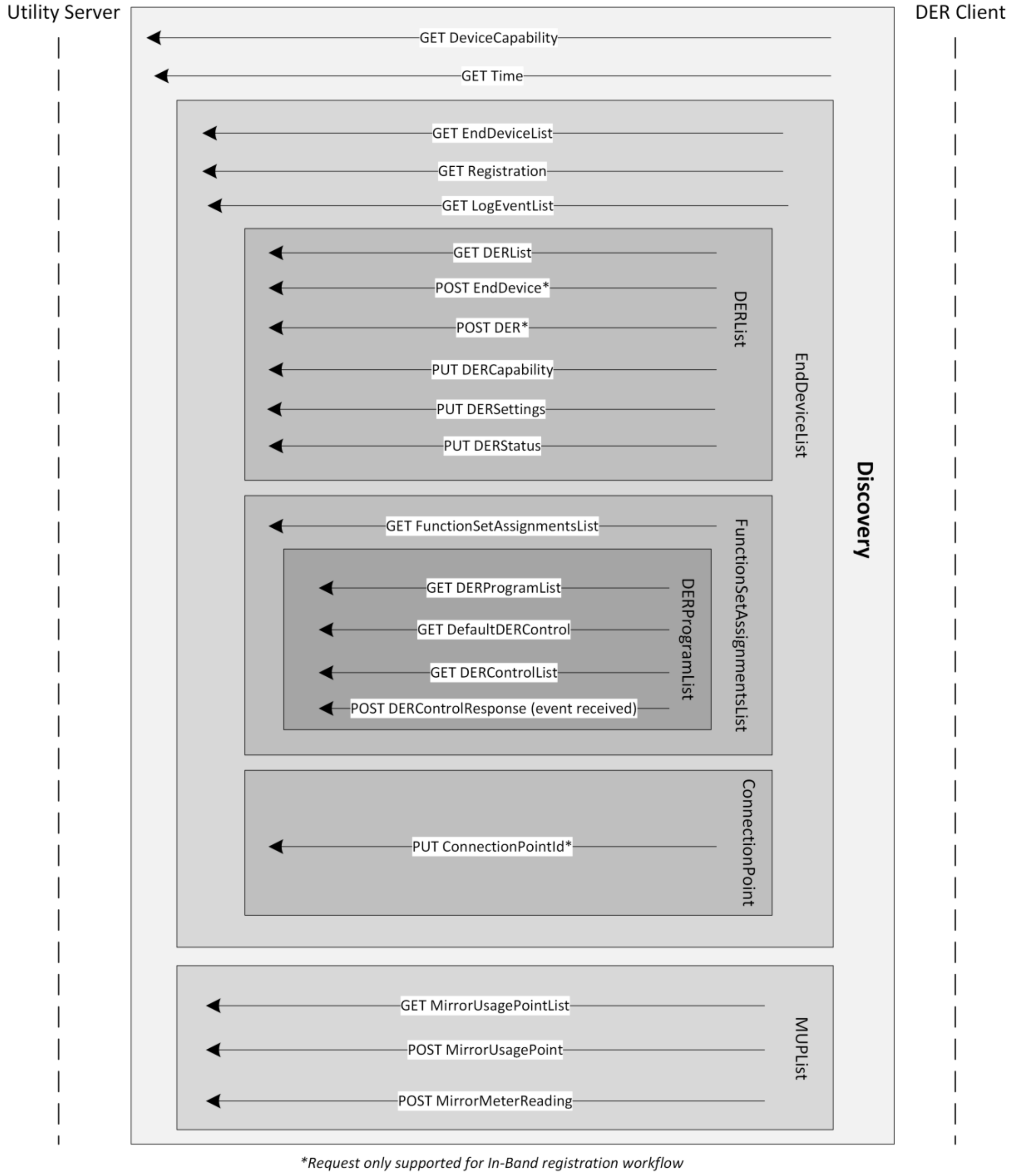


Figure 13: DER Client-Server Interactions - Discovery

Figure 14 demonstrates the workflow of DER Client ongoing requests that are submitted to the Utility Server Important to note that the utility server expects post on change for:

- DERControl Responses (Received, Started, Completed, Cancelled/Superseded)
- DERSettings
- DERCapabilities

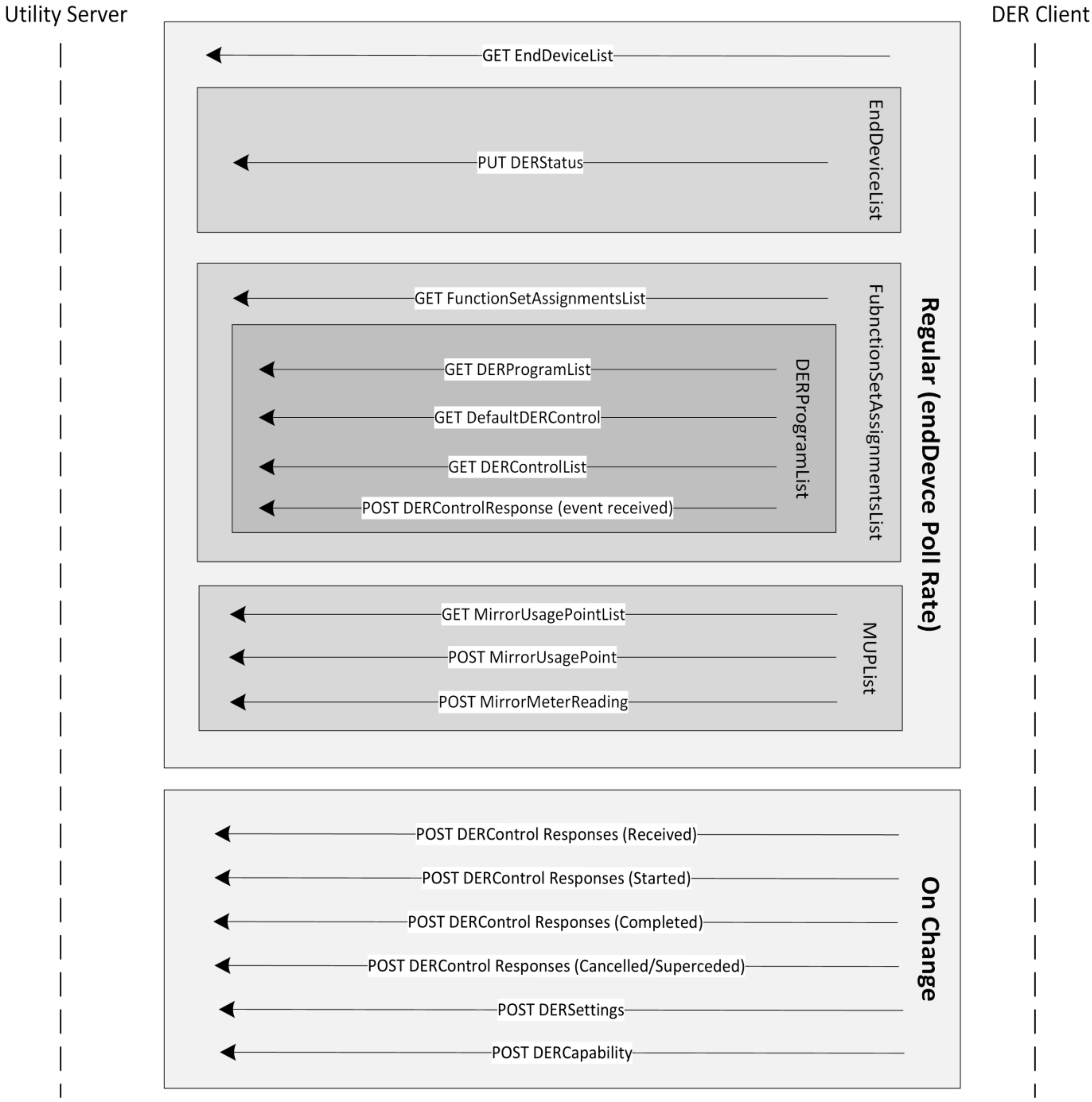


Figure 14: Client-Server interactions - Ongoing

11. Telemetry and Alarm Requirements

11.1 Monitoring

Under any scenario (aggregator-mediated or otherwise), End Devices shall be able to report the following monitoring information. This information shall be reported for the connection point. The following average readings are required through the Mirror Metering function set:

- Site Real Power.
- Site Reactive Power.
- DER Real Power.
- DER Reactive Power.
- Site Voltage (DER voltage can be provided if site is unavailable). Per phase for three phase devices.

Where applicable, data intervals shall be aligned to **regular boundaries** (for example, 1/5/30 minute boundaries). By default, EndDevices shall report monitoring information every 5 minutes (aligned to 5-minute boundaries). Devices shall support reporting intervals up to 1 minute.

Refer to Annex A of CSIP-AUS for further information on these reading types.

11.2 Supported Functions

The below functions from *CSIP-AUS* and *IEEE 2030.5:2018* are required to be supported in addition to any other common functionality required to support the following:

- DeviceCapability
- Time
- EndDevice
- FunctionSetAssignments
- DER
  - DERList
  - DERSettings
  - DERStatus
  - DERCapability
  - DERProgram
  - DERControlList
  - DefaultDERControl
- Randomisation
- Scheduling
- Response
  - DERControlResponse
- Metering Mirror
  - MirrorUsagePoint
  - MirrorMeterReadingList
  - MirrorMeterReading
  - MirrorReadingSet
  - Reading
- Subscription/Notification
- ConnectionPoint Extension

11.2.1 Multiple FSA, multiple programs and overlapping controls

CPPAL requires support for multiple FSAs and multiple programs as per CSIP. For further information please email oem_onboarding@powercor.com.au to request a copy of Interoperability Quick Start Guide and Test Procedure for further details on implementation.

11.3 Poll and Post Rates

For steady state operation the Utility Server will configure the following poll and post rates for resources as per the table below.

Table 3: Default Poll and Post Rates

Resource	Type	Value (secs)
Device Capability	Poll	300
EndDeviceList	Poll	300
FunctionSetAssignmentList	Poll	300
DERProgramList	Poll	300
DERList • DERStatus • DERSettings • DERCapability	Post	300
MirrorUsagePoint	Post	300
EndDevice	Post	300

Note that as above the Utility Server will configure the following poll and post rates during the on-site capability test to allow for quicker polling of controls and posting of telemetry.

Table 4: Capability Test Poll and Post Rates

Resource	Type	Value (secs)
Device Capability	Poll	300
EndDeviceList	Poll	300
FunctionSetAssignmentList	Poll	300
DERProgramList	Poll	60
DERList • DERStatus • DERSettings • DERCapability	Post	300
MirrorUsagePoint	Post	60
EndDevice	Post	60

11.4 Device Status

The required DERStatus objects are listed below:

Table 5: DER Status Objects Required

DERStatus objects	Requirement
OperationalModeStatus	Required for all implementations
GenConnectStatus	Required for all implementations
inverterStatus	Not required
alarmStatus	Not required
storConnectStatus and stateofchargestatus	Required for communications software communication clients that can control energy storage

11.5 DER Capability

DERCapability resource is the posting of the nameplate ratings to the utility server as per Table 6.

Table 6: Settings and Capabilities

DERSettings	DERCapabilities	Aggregation
setMaxVA	*rtgMaxVA*	Total
setMaxVAr	*rtgMaxVAr*	Total
setMaxVArNeg	*rtgMaxVArNeg*	Total
setMaxW	*rtgMaxW*	Total

CPPAL requires clients to post:

- What modes are supported for the modesSupported bitmap such as opModEnergize
- What CSIP-AUS controls have been implemented via the csipaus:doeModesSupported as per Section 9 of SA HB218:2023

11.6 Aggregations for Multi-Inverter Sites

When multiple DER are being represented by one LFDI as a Generating Facility Energy Management System (GFEMS) the Software Communications Client shall provide a representative value for the whole site as below:

Table 7: Aggregated Settings and Capabilities

DERSettings	DERCapabilities	Aggregation
setMaxVA	*rtgMaxVA*	Total
setMaxVAr	*rtgMaxVAr*	Total
setMaxVArNeg	*rtgMaxVArNeg*	Total
setMaxW	*rtgMaxW*	Total

11.7 Control Response Requirements

The communications software client shall support the following control responses from IEEE 2030.5 Table 27. All other responses are excluded. Control response is expected on change as per section 10.

Table 8: Control Responses

Enumeration Value	Description
1	Event Received
2	Event Started
3	Event Completed
6	The event has been cancelled
7	The event has been superseded

11.8 Ramp Rates

It is expected that if setGradW or rampTms has not been specified by the utility server, then the ramp rates should be as per AS 4777.2:2020.

The gradient of power rate limit of 16.67% of rated power per minute applies when ramping to a default control.

The soft limit for generation and export control applies for ramping when an active control is in place.

12. Failure Modes

The following requirements are important to consider as they ensure that widespread impacts to the network do not occur because of the following uncommon but expected events:

- Utility Server Outages.
- Widespread Communication Outages.
- Power Outages.

12.1 Loss of Communications

Following a connection point power outage, the client MUST remove all existing DERControls, revert to the DefaultDERControl and re-poll all associated DERPrograms to establish if any DERControl events have been added or changed whilst offline.

This is in addition to the connection and reconnection procedure outlined in AS/NZS 4777.2:2020. Note that this scenario applies to a lack of grid supply, and not to a communications outage.

12.2 Re-establishment of Communications Following Power Outage

Following a connection point power outage, the client MUST remove all existing DERControls, revert to the DefaultDERControl and re-poll all associated DERPrograms to establish if any DERControl events have been added or changed whilst offline.

This is in addition to the connection and reconnection procedure outlined in AS/NZS 4777.2:2020. Note that this scenario applies to a lack of grid supply, and not to a communications outage.

13. OEM Troubleshooting

OEM devices could present useful troubleshooting information to the customer depending upon what error is faced:

Timeout error
A timeout error is expected if connecting from a non-Australian IP address. Alternatively, if connecting from within Australia, the timeout period of the client may be set too low.
Remote end closed connection without response error
This error is expected when you have not provided a valid PKI certificate as part of the request.
404 (Not Found) error for a valid URL
The SEP2 Utility Server returns a 404 (Not Found) error for pages that do not exist and also when it does not want to confirm the pages existence (what would normally be a 401 (Unauthorized) error). As such, an unexpected 404 (Not Found) is most likely because the certificate is not authorised for that resource.
429 Client Error: Too Many Requests error
If the server receives too many simultaneous requests from a client, it will return this error. A client should be capable of retrying with exponential backoff after a short period of time.
404 (Not Found) error for a newly created resource

If the resource has been recently created (such as a new MUP), it may take a few seconds for the resource to become available. The client should retry after a few seconds.

400 “Failed to create endDevice due to duplicate key edevId” error during In-Band registration

If an OEM is conducting an in-band registration with an LFDI that is already registered in the Utility Server, the Utility Server will reject the registration. In such case, the OEM or installer should contact the DNSP to request manual termination of the existing LFDI from the Utility Server. Once terminated, the OEM/installer can then retry the in-band registration.

400 "Unable to update the ConnectionPointId in endDevice, the ConnectionPointId doesn't exist in the registration database" error during In Band registration

If an OEM or installer attempts to In Band register a device with an invalid NMI or without a valid Solar Pre-Approval (SPA), the registration will fail with this error message. To resolve this, please ensure that the correct NMI is used and that a corresponding SPA has been approved. If an SPA has not yet been approved, please submit an SPA application before attempting to register the device.

14. Referenced Documents

14.1 Australian Standards and Handbooks

Table 9: External References

Title	Standard/Reference
Common Smart Inverter Profile – Australia with test procedures store.standards.org.au/reader/sa-hb-218-2023	SA HB 218:2023
CSIP-AUS Communications Client Test Procedures v1.0 https://bsgip.com/wp-content/uploads/2023/09/CSIP-AUS-Comms-Client-Test-Procedures-v1.0-final.pdf	CSIP-AUS Communications Client Test Procedures v1.0
CitiPower, Powercor and United Energy LV DERMS DER Client Integration Guide for API Implementation Available on request	LV DERMS CSIP AUS External Party API
Guide to connect to CPPAL test environment and steps to onboard OEM systems to CPPAL systems including interoperability test procedure Available on request	Interoperability Quick Start Guide and Test Procedure
Grid connection of energy systems via Inverters Part 2: Inverter requirements	AS4777:2020

Standards listed have been developed for use in Australia and may be based on international standards and are not Australian Standards branded unless prefaced with the letters "AS" or "AS/NZS".

14.2 International Standards and References

Table 10: International Standards

Title	Document No.
IEEE Standard for Smart Energy Profile Application Protocol	IEEE 2030.5:2018
Common Smart Inverter Profile CSIP Implementation Guide v2.0 (sunspec.org)	SunSpec CSIP Implementation Guide

15. Definitions

Table 11: Terms and Definitions

Term	Definition
Communications Software Client	IEEE 2030.5 client to receive commands and send measurements
CSIP	Common Smart Inverter Profile
CSIP-AUS	Common Smart Inverter Profile – Australia (A companion document to CSIP describing the changes to support Australian use cases.)
DER	Distributed Energy Resource (Electricity generating and storage devices connected to the distribution network including rooftop solar, batteries and electric vehicles and other smart electrical devices.)
Direct Device	DER with embedded Communications Software Client such that the DER directly communicates with the Utility Server
DOE	Dynamic Operating Envelope (An operating profile that defines the upper and lower limits of power export or import in each time interval for each DER or connection point.)
End Device	Individual DER, often an inverter (including bi-directional inverter used with a battery
Flexible Exports	Optional DER connection type provided by the Utility that permits the maximum power exported to the network to be limited by a DOE issued by the Utility
Gateway	A hardware device located on site with the DER to provide communications (control and metering) functionality for DER acting as a Direct Device Client and may also be known as the GFEMS
GFEMS	Generating Facility Energy Management System (GFEMS) as defined in CSIP
Utility Interconnection Handbook	A document outlining the technical requirements and processes for connecting a customer's software communications client to the utility server. This document.
LFDI	Long Form Device Identifier as defined in IEEE2030.5:2018
NMI	National Metering Identifier
OEM	Original Equipment Manufacturer (Including the manufacturers of solar inverters, managed batteries and other DER equipment and integration systems.)
PCC	Point of Common Coupling
PKI	Public Key Infrastructure
SCC	Software Communications Client
Technology provider	Entity providing a communications software client implementation, can either be an OEM or another party responsible for the integration
Utility	CitiPower, Powercor and United Energy distribution networks
Utility Server	Computer server as defined in CSIP-AUS
V2G	Vehicle to Grid (Technology available in some electric vehicles to permit the battery vehicle to store energy that can be used within an electrical installation or exported to the electrical distribution network.)