SwitchDin

Detailed Design

Interim PKI – IEEE 2030.5

Prepared by
SwitchDin Pty Ltd

Suite 101, Level 1, 426 King Street
Newcastle West, 2302, NSW, Australia

Table Of Contents

Document Revision History

ID	Title	Date	Revision
A	First Release	03/07/2025	1.0
B	MInor update - ID Check Process and AUS SERCA inclusion	16/10/2025	1.1
C	Minor update - Utility Server / Aggregator Cert Profile; and ID Check Process	4/02/2026	1.2

1. Solution Context

This document outlines the detailed design for the Interim Public Key Infrastructure (PKI) service for coordinated Distribution Network Service Providers (DNSPs), provided by SwitchDin in partnership with DigiCert. This service is a key component for implementing Emergency Backstop mechanisms for Consumer Energy Resources (CER) in alignment with CSIP-AUS (Common Smart Inverter Profile – Australia) and IEEE 2030.5 2018 standards.

Coordinated DNSPs have opted for a shared Smart Energy Root CA (SERCA) and other PKI processes. This shared service model is closely aligned with the national PKI concepts and architecture envisioned for a national solution. The solution aims to provide the required PKI capability until a national solution is available, offering an easy transition path.

The PKI components and processes have been informed by the Gatekeeper Public Key Infrastructure Framework published by the Australian Government, Department of Finance.

1.1. Changes to this document

Changes to the document will be made from time to time. The latest version will be made available via the SwitchDin Support Portal. Significant changes will be raised for discussion and final decision at the Policy Steering Committee meetings.

1.2. Roles and responsibilities

Interim PKI Service Operators

Service Operator	Overview and Responsibilities
SwitchDin	Responsible for the overall operation of the Interim PKI service. Responsibilities include maintaining a PKI service as outlined in this document. This includes but is not limited to: • First and second line technical support for the service. • Ensuring a CA hierarchy aligned to the IEEE 2030.5 standard. • Maintaining a repository of all relevant information, accessible to Interim PKI Consumers, relating to the service. • Completing OEM identity checks. • Chairing the Policy Steering Committee.

DigiCert	DigiCert operates the PKI platform that the Interim PKI runs on top of. Responsibilities include: • Third line technical support for the service. • Operating a reliable and secure platform in line with industry practices.

Interim PKI Service Consumers

Consumer Type	**Overview and Responsibilities**
DNSPs	DNSPs manage registered CER connected to their network via a Utility Server. Utility Server Device certificates are hosted on the DNSP Utility Server. Responsibilities include: • Approve any certificate requests related to their network (e.g. DNSP MICA and Utility Server Device certificates). • Authorise OEMs (Aggregators and Direct Connect) to request PKI services related to their DNSP network.
OEMs (Aggregators)	OEMs manufacture CER. OEM Aggregators act as a proxy/gateway for a fleet of CER to the DNSP Utility Server. Aggregator Device Certificates are hosted on the Aggregator infrastructure. Responsibilities include: • Completing appropriate OEM Identity Checks. • Adhering to the obligations outlined in the OEM Certificate Practice Requirements signed during the OEM Identity Check process.
OEMs (Direct Connect)	OEMs manufacture CER. OEMs which operate in a Direct Connect architecture have deployed CER directly connecting to the DNSP Utility Server. Device Certificates are installed directly onto these CER devices. Responsibilities include: • Completing appropriate OEM Identity Checks. • Adhering to the obligations outlined in the OEM Certificate Practice Requirements signed during the OEM Identity Check process.

2. Solution Overview

2.1. Certificate Authority (CA)

Test and Production Environments

Separate test and production CA environments are configured.

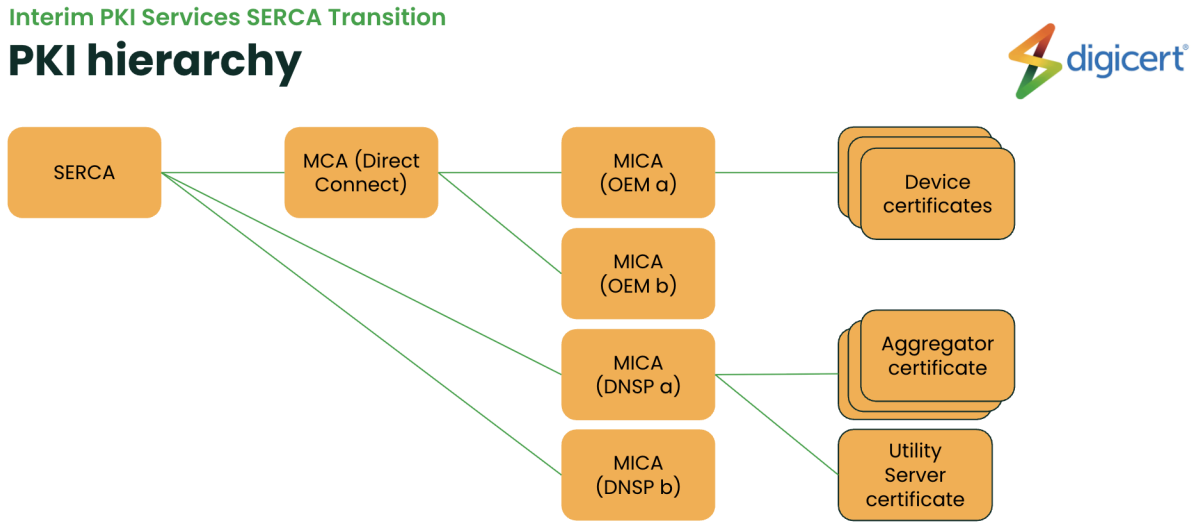
- The test environment manages certificates for pre-production test environments.
- The production environment manages certificates for the live emergency backstop or other CSIP-AUS based services.
- There are currently two production environments. One hosted in the United States and one in Australia.

Prior to issuing Production Certificates:

- It is expected that all DNSP and OEM configuration and certificates are tested in an appropriate Test environment and approved by the DNSP; and
- OEM identification checks must be completed.

Certificate Authority Trust Hierarchy

The following Certificate Hierarchy is configured in the Test and Production environments.



Notes on hierarchy:

- The hierarchy makes use of the four levels available from the IEEE 2030.5 standard.
- The Smart Energy Root CA (SERCA) is maintained offline and subject to strict procedures for its protection and use.

- A Manufacturer CA (MCA) is used for Direct Connect OEM's. The Direct Connect MCA is online and can only be used by interacting with the DigiCert PKI hosting platform. A Direct Connect MCA was established to improve the onboarding speed of OEM MICAs as these are signed by the online MCA (as opposed to requiring a key ceremony requiring physical access to HSMs).
- Manufacturer Issuing CA's (MICA) are used for DNSP (Aggregator and Utility Server device certificate) and Direct Connect OEM device certificate issuance.
- Direct Connect OEM MICA's are currently managed offline by OEMs. OEM MICAs allow for the simplest OEM support. A single OEM MICA enables valid certificates across all DNSPs. Note: DNSPs have the option to limit access via mechanisms on their Utility Server (e.g. through ACLs). A near term plan is moving these to online MICAs on the PKI platform to improve security.
- DNSP MICA's are online and can only be used by interacting with the DigiCert PKI hosting platform. DNSP MICA's allow segregation between DNSPs for a majority of CER power under management.

Certificate Profiles

Certificates are expected to be issued as per the following:

Certificate Type	**Implementation Details**
SERCA	Completed as per section "6.11.8.2 Root certificate" of IEEE 2030.5 2018 (as referenced in CSIP-AUS v1.2). Within Interim PKI implementation the following are permitted: 1. Issued by: Self signed 2. Issuer and Subject Name are: <u>Test:</u> % openssl x509 -issuer -noout -in test_SERCA.pem issuer= /C=AU/O=SwitchDin Pty Ltd/OU=For TEST Purposes ONLY/CN=SwitchDin Test SERCA G1/serialNumber=001 <u>Production (US):</u> % openssl x509 -issuer -noout -in prod_SERCA.pem issuer= /C=AU/O=SwitchDin Pty Ltd/CN=SwitchDin SERCA G1/serialNumber=001 <u>Production (AUS):</u> % openssl x509 -issuer -noout -in au_prod_SERCA.pem

Certificate Type	Implementation Details
	issuer= /C=AU/O=Smart Energy/CN=IEEE 2030.5 Root/serialNumber=002 Extensions: 3. certificatePolicy: Critical; anyPolicy 4. keyUsage: Critical; keyCertSign, crlSign 5. basicConstraints: Critical; cA=true, pathLen absent (unlimited) 6. subjectKeyIdentifer: set.
MCA (Direct Connect)	To be completed as per section "6.11.8.3.1 MCA certificate" of IEEE 2030.5 2018. Within Interim PKI implementation the following are permitted: 1. Issued by: SERCA 2. Subject Name: C=AU, O=SwitchDin Pty Ltd, CN=SwitchDin MCA G1 or CN=IEEE 2030.5 MCA, serialNumber=<num> a. In the Test Environment only, an OU is set to "For TEST Purposes ONLY". Extensions: 3. Certificate policies are set to - critical: a. Policy: 1.3.6.1.4.1.40732.1.1 b. Policy: 1.3.6.1.4.1.40732.1.2 c. Policy: 1.3.6.1.4.1.40732.1.3 d. Policy: 1.3.6.1.4.1.40732.2.1 (Test Environment only) 4. keyUsage: critical; keyCertSign 5. basicConstraints: critical; cA=true, pathLen=1 6. subjectKeyIdentifier: set 7. authorityKeyIdentifier: set
DNSP MICAs	To be completed as per section "6.11.8.3.2 MICA certificate" of IEEE 2030.5 2018. Within Interim PKI implementation the following are permitted: 1. Issued by: SERCA. 2. Subject Name: C=<country>, O=<Manufacturing Org>, CN=IEEE 2030.5 MICA, serialNumber=<num> a. CN may be: <DNSP> IEEE 2030.5 MICA. (non preferred) b. In the Test Environment only, an OU is set to "For TEST Purposes ONLY".

Certificate Type	Implementation Details
	Extensions: 3. Certificate policies are set to - critical: a. Policy: 1.3.6.1.4.1.40732.1.1 b. Policy: 1.3.6.1.4.1.40732.1.2 c. Policy: 1.3.6.1.4.1.40732.1.3 d. Policy: 1.3.6.1.4.1.40732.2.1 (Test Environment only) 4. keyUsage: critical; keyCertSign 5. basicConstraints: critical; cA=true, pathLen=0 6. subjectKeyIdentifier: set 7. authorityKeyIdentifier: set E.g. in Test: % openssl x509 -noout -in Test_DNSP_MICA.pem -subject subject= /C=AU/O=DNSP/OU=For TEST Purposes ONLY/CN=IEEE 2030.5 MICA/serialNumber=001 E.g. in Production: % openssl x509 -noout -in Prod_DNSP_MICA.pem -subject subject= /C=AU/O=DNSP/CN=DNSP IEEE 2030.5 MICA/serialNumber=001
Utility Server Certificates	To be completed as per section "6.11.8.3.3 Device certificate" of IEEE 2030.5 2018. Within Interim PKI implementation the following are permitted: 1. Issued by: DNSP MICA. 2. The Subject field must be set. Attributes must include C, O and CN fields. The CN field should record the DNS name. Other Subject fields are optional. Extensions: 3. Certificate policies are set to - critical: a. Policy: 1.3.6.1.4.1.40732.1.1 b. Policy: 1.3.6.1.4.1.40732.2.1 (Test Environment only) 4. The Subject Alternative Name is marked critical and includes both a: a. hardwareModuleName; and b. DNS Name. Note: The Subject Alternative Name field must set the DNS field to the DNS name of the Utility Server. The

Certificate Type	Implementation Details
	hardwareModuleName field is made up of hwType and hwSerialNum. hwSerialNum is stored as a OCTET STRING as per RFC 4108. c. hwType records the PEN d. hwSerialNum is set to xxx<PEN>yyymmdd where xxx is a counter for the day for the DNSP. If required, the DNSP may set this field. Note: the combination of hwType and hwSerialNum must be unique. 5. keyUsage: critical; keyAgreement, digitalSignature 6. authorityKeyIdentifier: set Note: the following may also be set: 7. OCSP set. No Utility Server Certificates signed after 01/07/2025 have this value set. 8. X509v3 Extended Key Usage is set to: TLS Web Server Authentication, TLS Web Client Authentication. No Utility Server Certificates signed after 01/07/2025 have this value set. 9. subjectKeyIdentifier set. No Utility Server Certificates signed after 01/07/2025 will have this value set.
Aggregator Certificates	To be completed as per section "6.11.8.3.3 Device certificate" of IEEE 2030.5 2018. Within Interim PKI implementation the following are permitted: 1. Issued by: DNSP MICA. 2. Subject Name: [EMPTY]. Extensions: 3. Certificate policies are set to - critical: a. Policy: 1.3.6.1.4.1.40732.1.1 b. Policy: 1.3.6.1.4.1.40732.2.1 (Test Environment only) 4. The Subject Alternative Name is marked critical and includes a hardwareModuleName entry. This field is made up of hwType and hwSerialNum. hwSerialNum is stored as a OCTET STRING as per RFC 4108. a. hwType records the PEN b. hwSerialNum is set to xxx<PEN>yyymmdd where xxx is a counter for the day for the DNSP. If required, the OEM may set this field. Note: the combination of hwType and hwSerialNum must be unique. 5. keyUsage: critical; keyAgreement, digitalSignature 6. authorityKeyIdentifier: set

Certificate Type	Implementation Details
	Note: the following may also be set: 7. OCSP is set. No Aggregator Certificates signed after 01/07/2025 have this value set. 8. Extended Key Usage is set to: TLS Web Server Authentication, TLS Web Client Authentication. No Aggregator Certificates signed after 01/07/2025 have this value set. 9. subjectKeyIdentifier set. No Aggregator Certificates signed after 01/07/2025 will have this value set.
Aggregator Notification Server Certificates	To be completed as per Aggregator Certificates (see above) with the following addition: • Subject Alternative Name: critical. With the DNS field set to the URL of their notification server.
OEM MICA (Direct Connect)	To be completed as per section "6.11.8.3.2 MICA certificate" of IEEE 2030.5 2018. Within Interim PKI implementation the following are permitted: 1. Issued by: Direct Connect MCA. 2. Subject Name: C=<country>, O=<Manufacturing Org>, CN=IEEE 2030.5 MICA, serialNumber=<num> a. In the Test Environment only, an OU is set to "For TEST Purposes ONLY". b. CN must be set to "IEEE 2030.5 MICA" (after 1 July 2025). c. Subject Name attribute matches the above order for all certificates after 1 July 2025. Extensions: 3. Certificate policies are set to - critical: a. Policy: 1.3.6.1.4.1.40732.1.1 b. Policy: 1.3.6.1.4.1.40732.1.2 c. Policy: 1.3.6.1.4.1.40732.1.3 d. Policy: 1.3.6.1.4.1.40732.2.1 (Test Environment only) 4. Key Usage must be set to - critical, Certificate Sign (only) after 1 July 2025. 5. basicConstraints: critical; cA=true, pathLen=0 6. subjectKeyIdentifier: set 7. authorityKeyIdentifier: set
Device Certificates (Direct Connect)	To be completed as per section "6.11.8.3.3 Device certificate" of IEEE 2030.5 2018.

Certificate Type	Implementation Details
	Within Interim PKI implementation the following are permitted: 1. Issued by: OEM MICA. 2. Subject Name: [EMPTY]. Extensions: 3. Certificate policies are set to - critical. One device type identifier as a Policy Identifier from the below: a. Policy: 1.3.6.1.4.1.40732.1.1 b. Policy: 1.3.6.1.4.1.40732.1.2 c. Policy: 1.3.6.1.4.1.40732.1.3 4. The following policy assignment identifier must be set as a Policy Identifier for test device certificates: a. Policy: 1.3.6.1.4.1.40732.2.1 (Test Environment only) 5. As per the standard, the Subject Alternative Name is marked critical and includes one GeneralName of type OtherName of hardwareModuleName. This field is made up of hwType and hwSerialNum. a. hwType records the PEN b. hwSerialNum can be determined by the OEM but the combination of hwType and hwSerialNum must be unique. 6. keyUsage: critical; keyAgreement, digitalSignature 7. authorityKeyIdentifier: set

Note: refer to the Repository section for details on common SERCA and MCA (Direct Connect).

2.2. Registration Authority (RA)

The RA is responsible for verifying the organisation and the identity of the Authoriser of the business entity (the Authoriser). Identity verification is performed to the Gatekeeper PKI Framework published by the Digital Transformation Office of the Australian Government. Identify Verification of the Authoriser is performed in line with the Gatekeeper frameworks Level of Assurance 2.

An Authoriser is a member of a class of persons with a clear capacity to commit an organisation and to appoint a Certificate Manager. Persons who are members of this class may include but are not limited to a Chief Executive Officer, Company Director, Trustee, Sole Trader, Partner or Company Owner. For more information refer to "Evidence of Association" under the Gatekeeper Framework page.

The Authoriser also nominates one or more certificate managers authorised to manage digital certificates on behalf of the organisation. Certificate Managers are verified against the approved list prior to certificate issuance. No identity checks are required.

2.3. Repository

All relevant information relating to the Interim PKI service can be found on the SwitchDin support portal repository including:

- Valid and invalid certificates - Reports page.
- Certified list of OEMs (per DNSP) - Production PKI Certified List.
- Process documentation (including this document) - Document Repository.
- Common SERCA, MCA and DC MICAs - are not stored on the repository but provided to certificate requestors in a bundle as needed by the requestor.

2.4. Governance

Detailed Design (this document)

The Interim PKI will be run in line with the practices documented in this detailed design document and those processes it refers to.

Policy Steering Committee

A Policy Steering Committee guides the development of this policy framework that supports the secure and coordinated implementation of the Interim PKI. There is a strong emphasis on alignment to requirements of a national solution. The Committee includes appropriate representation from the different stakeholders of the Interim PKI as well as those interested in ensuring interoperability, security, and consistency across the broader energy ecosystem. This includes SwitchDin, DigiCert, participating DNSPs, OEMs, and other relevant stakeholders.

Significant security issues detected (e.g. a compromise of an OEM MICA) will be reported immediately to relevant stakeholders. All other issues will be reported on during regular steering committee meetings for visibility.

OEM Requirements

Upon registering, OEMs sign a set of Certificate Practice Requirements stating their obligations when operating in the Interim PKI.

3. PKI Processes

3.1. Contacting support

SwitchDin support can be reached via:

- Our online Support Hub (accessible 24x7) - https://support.switchdin.com/hc/en-us/requests/new
- By email at support@switchdin.com
- By phone at +61 (0) 2 4786 0426

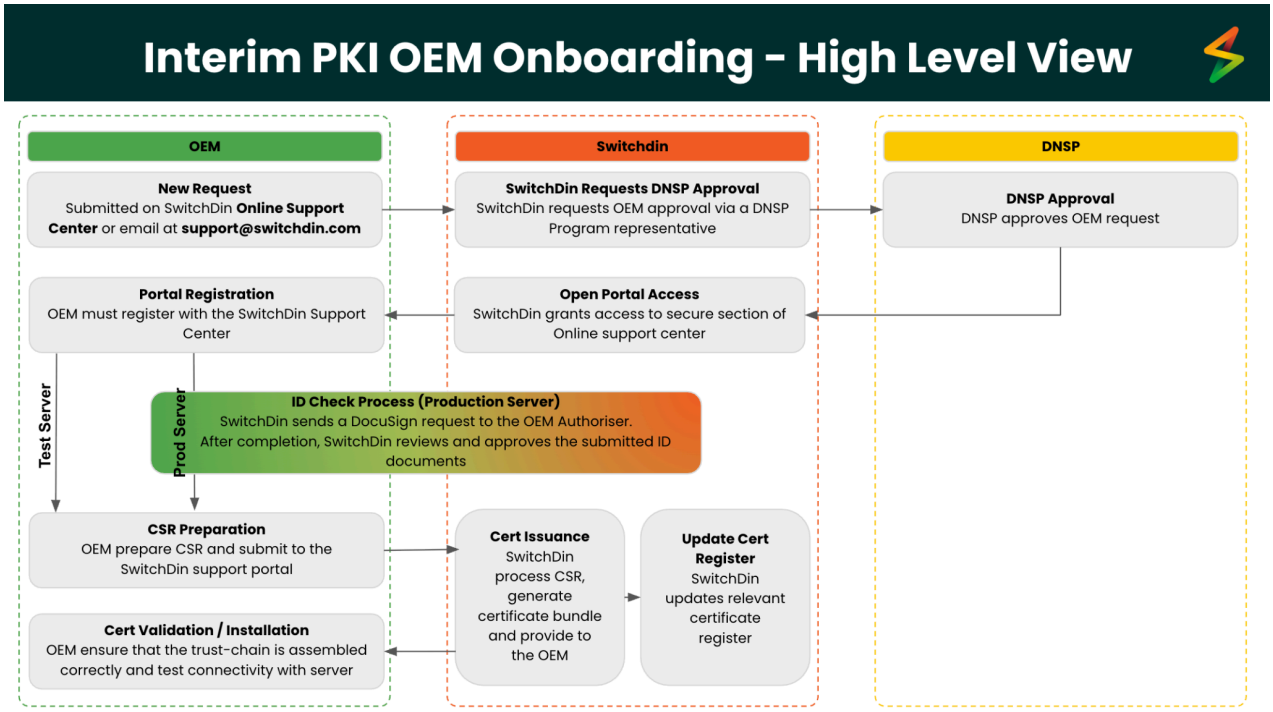
SwitchDin Support Standard Operating Hours are from 9am AEDT to 5pm AWST on business days.

3.2. DNSP Registration and Issuance

1. DNSP registration to the service commences upon receipt of a signed contract and purchase order.
2. SwitchDin create DNSP profiles in the relevant Certificate Request forms and Interim PKI Document Repository including:
    a. Valid and invalid certificates - Reports page.
    b. Certified list of OEMs (per DNSP) - Production PKI Certified List.
    c. Certificate Request forms.
3. SwitchDin authorises DNSP users to access the Interim PKI Document Repository.
4. DNSP authorised users to register to the support portal and the Interim PKI Document Repository.
5. DNSP MICA setup - SwitchDin will populate MICA Naming Documents for DNSP review and approval. Note: MICA setup requires a physical key signing ceremony and thus forms must be submitted 10 days before the key signing ceremony (completed by DigiCert weekly on Wednesday's).
6. Utility Server Certificates (Test/Production) - DNSP to initiate Utility Server Client Certificate request. Note: Production requests are expected to be completed after appropriate validation in a Test environment.
7. SwitchDin records all certificates created in the relevant DNSP Certificate Tracker.
8. DNSP is responsible for testing the certificate and connectivity in a timely manner to close out the support ticket.

3.3. OEM Registration and Issuance

The following process flow describes the high-level steps involved in registering a new OEM through to certificate issuance:



OEM Registration

1. New Request - OEM to submit a new request to be onboarded to the Interim PKI for the specific DNSP required - https://support.switchdin.com/hc/en-us/requests/new
2. DNSP approval -
    a. A support ticket has been opened and sent to DNSP for approval.
    b. Authorisation is tracked on the Production PKI Certified List of OEM per DNSP
3. Open Portal Access - SwitchDin authorises OEM users to access the Interim PKI Document Repository.
4. OEM Portal Registration - OEM authorised users to register to the support portal and the Interim PKI Document Repository.

Note: during initial onboarding periods (or for other unforeseen reasons) this process may differ. SwitchDin will ensure DNSP approval is provided prior to servicing OEM requests.

ID Check Process

Two ID Check Processes are currently supported as requested by customer DNSPs:

- Option 1 - requires OEM organisation verification and personal ID checking

- Option 2 - requires only OEM organisation verification checking.

Option 1 is the default for DNSP's unless specifically agreed with the DNSP. This may be on a per OEM basis or as across all OEMs onboarding to that DNSP.

Note: this step must be completed prior to Production Certificate Issuance.

1. SwitchDin sends the Organisation Verification Request Form to the nominated Authoriser via Docusign.
2. The Authoriser completes the relevant forms and attaches the required evidence. The key sections of this form include:
    a. Organisation Information
    b. Authoriser Information - this is a member of a class of persons with a clear capacity to commit an organisation and to appoint a Certificate Manager.
    c. Authoriser evidence of association with the entity - refer here for more details on Understanding "Evidence of Association" Under the Gatekeeper PKI Standard.
    d. (not required for the Option 2 ID check process - i.e. OEM organisation verification only) Authoriser Individual ID Verification Documents. Individual Identity Proofing requirements are designed to provide Level of Assurance (LoA) 2 per the Gatekeeper Public Key Infrastructure Framework published by the Australian Government, Department of Finance. This requires 1 Primary and 1 Secondary type of evidence.
    e. Certificate Manager Contact Details - details of one or more certificate managers authorised to manage digital certificates on behalf of the organisation.
    f. Authorised Representative Signature - confirming all information provided is accurate.
    g. Authorised Representative Signature on Certificate Practice Requirements
3. SwitchDin verifies the Authorisers documentation including:
    a. The Authoriser Form is completed.
    b. Verifies the Authorisers evidence of association with the entity.
    c. (not required for the Option 2 ID check process) Verifies the Authorisers Individual ID Verification documents.

Note 1: ID checks do not need to be re-performed for OEMs who have completed the process for another DNSP in the last year provided that:

- The Authoriser and Certificate Manager remain the same, and
- The level of ID checking is appropriate i.e. an OEM with option 2 ID checking will require additional personal ID checks to be onboarded to a DNSP requiring option 1 ID checking.

Note 2: By signing these forms, the Authoriser confirms acceptance of the obligations set out in the OEM Certificate Practice Requirements outlined in the form.

Note 3: Where insufficient documentation is provided as part of the identity check process, SwitchDin will request additional details to be provided. Significant delays will be communicated to the DNSP.

Certificate Request and Issuance (Test and Production)

1. Certificate Signing Request (CSR) Preparation - The OEM initiates the certificate request via the relevant forms:
    a. Aggregator OEM Process
    h. Direct Connect OEM Process
2. Certificate Issuance - SwitchDin returns the signed certificate to the OEM on the support ticket once completed.
3. Certificate Register Updated - SwitchDin updates the relevant Certificate Tracker for DNSP visibility.
4. Certificate Validation / Installation - OEM is responsible for testing the certificate and connectivity in a timely manner to close out the support ticket.

Note 4: Any issues identified with the CSR will be requested to be updated prior to certificate issuance.

Note 5: Issue identified post certificate issuance will be rectified by providing a new certificate. The certificate will be marked as revoked in the PKI portal. SwitchDin will request the OEM to delete the private key and/or certificate as required. The OEM is responsible for securely completing this deletion.

4. Future work

This section outlines design improvements that have been identified for future work but are not included in the current design. These will act as a checklist or backlog for future design iterations. The list is not intended to be exhaustive.

- Online hosted OEM MICAs for Direct Connect OEMs. To standardise security practices for all OEMs without requiring distributed security audits.
- Alternative processes for identity checking. E.g. where required due to an update to the Gatekeeper framework.

Completed:

- A SERCA hosted in Australia. To ensure sovereignty of private key material.