Cogito Group

DIGITAL IDENTITY AND SECURITY

X.509 Certificate Policy (CP)

Cogito PKI as a Service - Root and Subordinate Certificate Authorities

27 September 2021

Version 1.0

Notice to all parties seeking to rely

Reliance on a certificate issued under this Certificate Policy, identified by subarcs of the object identifier 1.2.36.151795998.4.1.1.1.1.0 for an RCA and 1.2.36.151795998.4.1.1.1.1.1 or 1.2.36.151795998.4.1.1.1.1.2 for Policy or Issuing SubCA that is signed by the RCA, is only permitted as set forth in this document. Use of a certificate issued under this CP constitutes acceptance of the terms and conditions set out in this document, as such, acceptance of a certificate by a Relying Party is at the Relying Party's risk. Refer to the CP and Cogito PKIaaS CPS for relevant disclaimers for warranties, liabilities and indemnities.

Owner:	Cogito Governance Risk and Compliance Group
Contact details:	Telephone: +61 2 6140 4494 Email: Security.services@cogitogroup.net
Document status:	RELEASED

Document Management

This document is controlled by:	Cogito Governance Risk and Compliance Group (GRCG)
Changes are authorised by:	Cogito Governance Risk and Compliance Group Gatekeeper Competent Authority (GCA)

Revision history

Revision date	Version No.	Author	Description of changes
2021-09-17	1.0	Brad Fardig	Released

Contents

1 Introduction

Certificate policies are, in the X.509 version 3 digital certificate standard, the named set of rules regarding the applicability of a certificate to a particular community and/or class of applications with common security requirements. A CP may be used by a Relying Party to help in deciding whether a certificate, and the binding therein, are sufficiently trustworthy and otherwise appropriate for a particular application.

This Certificate Policy (CP) identifies the rules to manage the Cogito Group PKI as a Service (PKIaaS) Root Certificate Authority(ies) (CA) certificates, Subordinate-Certificate Authority (Sub-CA) certificates and associated core component certificates. It includes the obligations of the Public Key Infrastructure (PKI) entities, and how the parties, indicated below, use them. It does not describe how to implement these rules as that information is found in the Cogito PKIaaS Certification Practice Statement (CPS), or documents referenced by the CPS. In general, the rules identify the minimum standards in terms of performance, security and/or quality.

The headings in this CP follow the framework set out in the Internet Engineering Task Force Request for Comment (RFC) 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

A document hierarchy applies: the provisions of any applicable contract such as a Subscriber Agreement, Deed of Agreement or other relevant contract override the provisions of this CP. The provisions of this CP prevail over the provisions of CPS to the extent of any direct inconsistency. The provisions of CPS govern any matter on which this CP is silent. (Note: where subtitled sections of the framework provide no additional information to detail provided in the CPS they have not been further extrapolated in this document).

This section identifies and introduces the set of provisions and indicates the types of entities and applications applicable for this Cogito Group PKI as a Service (PKIaaS) Root Certificate Authority and Sub-CA Certificate Policy (CP).

1.1 Overview

The purpose of this CP is to identify the rules to manage the Cogito Group PKIaaS Root Certificate Authority(ies) (RCA) certificates, Subordinate Policy and Issuing Certificate Authority(ies) (Sub-CA) certificates and associated core component certificates, based on ISM compliant RSA or ECC encryption algorithms.

This CP includes the obligations of the PKI entities, and how the parties, indicated below, use them. It does not describe how to implement these rules as that information is in the Cogito PKIaaS CPS, or documents referenced by the CPS. In general, the CP identifies the minimum standards in terms of performance, security and/or quality of the Cogito PKIaaS.

The Root CA is used to self-sign the Root CA certificate, digitally sign Policy-CA certificates to validate their properties, sign and issue the certificates used by operational servers and operation personnel, and generate and update the RCA Certificate Revocation List (CRL, incorporating the Authority Revocation List (ARL). The RCA is the highest point of trust within the Cogito PKIaaS PKI hierarchy and all other CA and RA entities in the hierarchy rely on this trust point.

A Policy CA certificate is signed by the RCA and signs the certificates used by operational servers and operations personnel as well as signing the certificates issued to Issuing CAs.

An Issuing CA certificate is signed by the Policy CA, or Root CA, and signs the certificates used by operational servers and operations personnel as well as signing the certificates issued to end-entities.

This CP only allows the RCA and any Sub-CA (Policy or Issuing) private keys to reside on an approvedHardware Security Module (HSM). Any operations certificates required for PKI core components are required to be stored in accordance with the associated Cogito Group Key Management Plan (KMP).

Except for Registration Officers (RO) this CP allows Operators' keys and certificates to only reside on a hardware-based token with an embedded cryptographic engine. Before issuing Operators' keys and certificates, the applicant is required to perform a face-to-face identity verification that complies with the Evidence of Identity requirements for Gatekeeper Level of Assurance (LOA), very high confidence, and be cleared to the required level in accordance with the Cogito PKIaaS System Security Plan (SSP).

1.2 Document Name and Identification

The title for this CP is X.509 Certificate Policy (CP) for Cogito PKI as a Service Root and Subordinate Certificate Authorities. The Object Identifier for the Root CA CP is: 1.2.36.151795998.4.1.1.1.1

{iso (1) iso-member (2) australia (36) cogito-group-pty-ltd (151795998) Cogito PKIaaS(4) pki (1) certificate policy (1) certificate authority (1) Root CA CP(1) Root CA(0)}

In addition, this CP is issued for any Policy SubCA that is signed by the Root CA, in this circumstance the OID is 1.2.36.151795998.4.1.1.1.1.1

{iso (1) iso-member (2) australia (36) cogito-group-pty-ltd (151795998) Cogito PKIaaS(4) pki (1) certificate policy (1) certificate authority (1) Root CA CP(1) Policy CA(0)}

In addition, this CP is issued for any Issuing SubCA that is signed by the Root CA, in this circumstance the OID is 1.2.36.151795998.4.1.1.1.1.2

{iso (1) iso-member (2) australia (36) cogito-group-pty-ltd (151795998) Cogito PKIaaS(4) pki (1) certificate policy (1) certificate authority (1) Root CA CP(1) Issuing CA(2)}

1.3 PKI Participants

1.3.1 Certification Authorities

The Certificate Authority(ies) (CA or CAs) that issue certificates under this CP are the Cogito PKIaaS CAs.

This CP relates to:

i. the self-signed RCA authentication certificates that the RCA issues to itself;

ii. the authentication and confidentiality certificates signed by the RCA and issued to SubCAs;

iii. the authentication and confidentiality certificates issued by the Sub-CAs for the core operational infrastructure, e.g. the Registration Authority (RA) server; and

iv. all operator certificates used for the purpose of maintenance and issuance responsibilities, such as CA operators (CAO) and Registration Officers (ROs).

1.3.2 Registration Authorities

The Registration Authority (RA), or RAs, that perform the registration functions under this CP are authorised by the Cogito Governance Risk and Compliance Group (GRCG). For those certificates issued in accordance with the Gatekeeper accreditation, a Gatekeeper accredited RA must be used. An RA is formally bound to perform the registration functions in accordance with this CP and other relevant Approved Documents.

1.3.3 Subscribers

No end-entity Subscribers are issued certificates under this CP.

Certificates issued by the RCA or Sub-CA to the operators of core components will not be used as a validation mechanism for that individual. All such certificates will only be valid for use within the PKI core components.

An entity issued a certificate under this CP must have access, authority or privilege to Cogito PKIaaS assets or systems. Cogito PKIaaS assets and systems may act as a Relying Party, with respect to chain of trust aspects, having granted access, authority, or privilege to an individual.

1.3.4 Relying Parties

Other than the chain of trust aspects there are no Relying Parties for the certificates issued under this CP. This chain of trust is created by the RCA signing the Sub-CA certificate that signs the certificate issued to the end-entity and the issuance of Certificate Revocation Lists (CRLs).

Relying Parties are bound by the relevant CP that an end-entity certificate is issued under.

1.3.5 Other Participants

See CPS for other participants and their responsibilities.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued under this CP, in conjunction with their associated private keys, allow the RCA to:

i. Self-sign the RCA certificate;

ii. Digitally sign a SubCA certificate;

iii. Sign the operational certificates required by the PKI, including OCSP responder;

iv. Sign the CRL; and

v. Sign its own internal log files.

Certificates issued under this CP, in conjunction with their associated private keys, allow a SubCA to:

i. Digitally sign a certificate for any CA subservient to the SubCA;

ii. Sign the operational certificates required by the PKI; and

iii. Sign its own internal log files.

All other core component certificates will only be valid for use within the PKI and used for the authentication and confidentiality (as appropriate) of core component activities.

1.4.2 Prohibited Certificate Uses

The prohibited uses for certificates issued under this CP are:

i. For the RCA, to sign certificates issued to end-entity Subscribers;

ii. To sign the certificate of a non-Lead Agency approved CA;

iii. To validate the identity of a AS operator (CMS ROs excepted); and

iv. To establish a Sub-CA to conduct any transaction, or communication, which is any or all of the following:

a) Unrelated to Subscribing Agency or Cogito PKIaaS business;

b) Illegal or criminal;

c) Unauthorised;

d) Unethical, or

e) Contrary to Subscribing Agency, Cogito PKIaaS or Gatekeeper policy.

Engaging in a prohibited certificate use is a breach of the responsibilities and obligations agreed to by the PKI operators and Cogito Group disclaims any and all liability in such circumstances.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

See CPS.

1.5.2 Contact Person

See CPS.

1.5.3 Authority determining CPS suitability for the policy

See CPS.

1.5.4 CPS approval procedures

See CPS.

1.6 Definitions, acronyms and interpretation

Acronyms and terms used in this CPP are defined in the CPS.

The Interpretation clause in Appendix C.3 of the CPS also applies to this CP.

2 Publication and Repository Responsibilities

2.1 Repositories

See CPS.

2.2 Publication of certification information

Cogito publishes the issuing CA certificate and issuing CA's latest CRL in its repository. This information is available to Relying Parties.

Cogito provides for Subscribers and Relying Parties the URL of a website which Cogito uses to publish:

i. This CP;

ii. The CP for any end entity certificates; and

iii. The CPS.

2.3 Time or Frequency of publication

Public documents are published/updated promptly on approved change.

Cogito PKIaaS CAs publish new certificates and CRLs as operationally required (see 4.9.7 and relevant CP).

2.4 Access controls on repositories

See CPS.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Every certificate issued under this CP:

i. Must have a clear distinguishable and unique Distinguished Name (DN) in the certificate subjectName field;

ii. The common name components of the name are unique to the PKI name space;

iii. The DN will be approved by the GRCG;

iv. The RCA DN must be composed of <Subscriber>CA<Serial>; and

v. The Sub-CAs DN must be composed of <Subscriber>CA<Serial>.

The DN is in the form of a X.501 printable string and is not blank.

3.1.2 Need for Names to be Meaningful

Names used to identify the PKI core components are based on their PKI role and serial number. Additionally, names are used to identify individual operators to allow for system auditing.

3.1.3 Anonymity or pseudonymity of Subscribers

Anonymous Certificates are not supported.

3.1.4 Rules for interpreting various name forms

No stipulation as there is only one form.

3.1.5 Uniqueness of Names

Names are unique within the Cogito PKIaaS name space.

3.1.6 Recognition, authentication, and Role of Trademarks

See CPS.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

Private Key generation of critical PKI core components is performed using Evaluation Assurance Level 4 (EAL4) and Federal Information Processing Standard Publication 140-3 (FIPS-140-3) approved Hardware Security Modules (HSMs). These private keys are generated internally which ensures that the private key is never exposed or accidentally released. To initiate the key generation process, the CA operator must use the HSM in the presence of the required staff as dictated by the Key Management Plan (KMP).

All PKI Operators (RCAOs, CAOs, ROs etc.) use hard token technology to generate and securely store private keys, with passphrase access controls. The key generation process requires the operator to enter their token's passphrase thereby proving the operator has possession of the

token with the generated private key. Where soft tokens are used, certificate requests are submitted to the CA via PKCS#10 requests where proof of possession of the private key is ensured as the Key Pair is generated at the time the certificate request is created.

3.2.2 Authentication of organisation entity

To establish the RCA or SubCA, the GRCG must grant approval prior to the key generation ceremony. The establishment of other Cogito PKIaaS Sub-CAs requires GRCG approval prior to the key generation.

For details of the authentication process see CPS.

3.2.3 Authentication of individual identity

See CPS.

3.2.4 Non-Verified Subscriber information

See CPS.

3.2.5 Validation of authority

The Operations Manager is responsible for ensuring that all PKI core components are validated in accordance with the KMP.

3.2.6 Criteria for interoperation

See CPS.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The minimum identification and authentication requirements for routine re-key will be as per 3.2.2., Authentication of Organisation Entity.

3.3.2 Identification and authentication for re-key after revocation

Re-key is not allowed for CAs after revocation

For Operators, re-key after revocation shall occur in the same manner as initial identity verification.

3.4 Identification and authentication for revocation requests

Revocation of certificates is in accordance with this section and section 4.9 of this CP and the CPS.

The PKIaaS Operations Manager, or their nominated agent in their absence must authenticate all requests for revocation of PKIaaS core components, including the reason for revocation.

Prior to revocation the Operator verifies the authority of the requestor.

The GRCG must approve all requests for revocation of PKIaaS CAs. Revocation of PKIaaS core components can be approved by the PKIaaS Operations Manager or the PKIaaS Security Officer, this includes Operator certificates.

The revocation process provides an auditable record of this process, which includes:

- The identity of the requestor;
- The reason for requesting the revocation;
- The identity of the operator performing the revocation; and
- The issuing CA name and the serial numbers of the certificates authorised for revocation or the reason the revocation request was rejected.

4 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Individuals affiliated with a Cogito PKIaaS subscriber can submit a certificate application. Creation of CAs must be authorised by the GRCG. There are no subsequent submissions of applications for the creation of PKIaaS core components related to that CA.

4.1.2 Enrolment process and responsibilities

The enrolment processes and responsibilities are outlined in the PKIaaS Operations Manual and the PKIaaS KMP.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The PKIaaS Operations Manager must ensure that each CA creation application is in accordance with the PKIaaS KMP and undergoes:

- Confirmation of approval for RCA or SubCA creation; and
- Validation of all information to be included in the certificate.

The PKIaaS Operations Manager is not required to investigate or ascertain the authenticity of any document received by them as evidence of any matter required as part of the CA creation process unless they are aware, or should reasonably be aware, that the document is not authentic, or they are otherwise required to do so by law.

4.2.2 Approval or rejection of certificate applications

The GRCG approves or rejects CA certificate applications.

4.2.3 Time to process certificate applications

Processing for certificate applications will occur in a timely manner.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

See CPS.

4.3.2 Notification to Subscriber by the CA of issuance of certificate

Operators shall be notified when a certificate has been issued and of any requirements necessary to update the operator's token.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

The PKIaaS core components are deemed to have accepted a certificate when they exercise the private key.

4.4.2 Publication of the certificate by the CA

The only certificates published will be the CA certificates. These will be published to the Certificate Publishing repository and external repositories as per the CPS.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Keypair and certificate usage

4.5.1 Subscriber private key and certificate usage

There are no end entity Subscribers to this CP. Certificate usage is defined above in Section 1.4 (Certificate Usage) and as such core components, other than CAs, may only be used within the PKIaaS.

Custodians shall protect private keys from access by other parties in accordance with the KMP and CPS.

If the basic constraints, naming constraints, or extended key usage extension is present and implies any limitation on the use of the certificate and/or private key, the CA will operate within those limitations.

4.5.2 Relying Party public key and certificate usage

1.4 (Certificate Usage) and 1.3.4 (Relying Parties) detail the Relying Party public key and certificate usage and responsibilities.

The interpretation and compliance with extended key usage attributes, and any associated limitations on the use of the certificate and/or private key, is in accordance with RFC 6818.

4.6 Certificate renewal

The RCA and Sub-CA certificates cannot be renewed; however, associated core components can be renewed.

4.6.1 Circumstance for certificate renewal

The CPS defines the criteria for certificate renewals.

Certificate renewal shall not permit an operator to avoid re-key or the associated identification and authentication process.

Renewal of revoked certificates is not permitted after revocation regardless of the reason for revocation.

4.6.2 Who may request renewal

Same as per applications - see **Error! Reference source not found.** (**Error! Reference source not found.**)

4.6.3 Processing certificate renewal requests

The process for certificate renewal is consistent with the enrolment process defined in Section **Error! Reference source not found.** (Certificate Application), however identification and authentication complies with Section **Error! Reference source not found.** (Identification and Authentication for Re-Key Requests).

4.6.4 Notification of new certificate issuance to Subscriber

Operators shall be notified when a “renewal” certificate has been issued, and of any requirements necessary to update the operator’s token.

4.6.5 Conduct constituting acceptance of a renewal certificate

See Section 4.4.1 (Conduct constituting certificate acceptance).

4.6.6 Publication of the renewal certificate by the CA

PKI core component renewed certificates will not be published.

4.6.7 Notification of certificate issuance by the CA to other entities

Not Applicable.

4.7 Certificate Re-key

4.7.1 Circumstance for certificate re-key

See CPS for relevant circumstances. Loss or compromise of a current private key requires revocation.

4.7.2 Who may request certification of a new public key

Certificate re-key requests are made by an operator or the GRCG.

4.7.3 Processing certificate re-keying requests

The process for certificate re-keying is consistent with the enrolment process defined in Section **Error! Reference source not found.** (Certificate Application), however identification and authentication complies with Section **Error! Reference source not found.** (Identification and Authentication for Re-Key Requests).

4.7.4 Notification of new certificate issuance to Subscriber

The operator receives notification when a re-keyed certificate is issued, or if a certificate request for re-key is rejected.

The GRCG receives notification of progress, issues, and completion of GRCG initiated certificate re-keys.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See 4.4.1 (Conduct constituting certificate acceptance).

4.7.6 Publication of the re-keyed certificate by the CA

PKI core component re-keyed certificates will not be published.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

The circumstances permitted for certificate modification are:

- Details relevant to the Operator have changed or have been found to be incorrect;
- Interoperation with approved Third-Party PKIs or PKIaaS assets and systems require certificate attributes or contents inserted, modified, or deleted; or
- Other circumstances deemed appropriate by the GRCG.

4.8.2 Who may request certificate modification

Certificate modification may be requested by:

- The GRCG;
- Operations Manager; or
- PKIaaS Operator.

4.8.3 Processing certificate modification requests

The process for certificate modification must comply with enrolment process defined in Section 4.1 (Certificate Application). The identification and authentication procedures must comply with Section 3.3 (Identification and Authentication for Re-Key Requests).

If the modification request changes the certificate substantially, it must be approved by the GRCG.

4.8.4 Notification of new certificate issuance to Subscriber

The PKIaaS operator or key custodian receives notification when issued a modified certificate, or if rejection of a modification request occurs.

The GRCG receives notification of requests, issues, and completion of all certificate modifications.

4.8.5 Conduct constituting acceptance of modified certificate

See 4.4.1 (Conduct constituting certificate acceptance).

4.8.6 Publication of the modified certificate by the CA

See 4.4.2 (Publication of the certificate by the CA).

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

See CPS.

4.9.2 Who can request revocation

See CPS.

4.9.3 Procedure for revocation request

Revocation requests for PKIaaS core components are performed by an authorised Certificate Authority Operator (CAO) but must be validated by the PKIaaS Operations Manager prior to initiation. The Disaster Recovery and Business Continuity Plan (DRBCP) details the revocation process for the RCA and Sub-CA in the event of an emergency.

After verification, the CAO processes the revocation request using the PKI software, which captures an auditable record of the process.

After a certificate is revoked, the CA includes the applicable certificate (certificate serial number) in the CRL that is signed by the CA and published in the repositories.

4.9.4 Revocation request grace period

For an RCA, a grace period of three business days is permitted.

For all SubCAs, a grace period of one business day is permitted.

The GRCG, or an approved delegate, in exceptional circumstances (such as security or law enforcement investigation), may approve a delay in submission of a revocation request. An audit record of this approval is required and must be submitted with the revocation request upon expiry of the approved delay.

4.9.5 Time within which the CA must process the revocation request

A CA shall process shell process revocation requests for certificates issued under this CP promptly after receipt.

4.9.6 Revocation checking requirement for relying parties

Before using a certificate, the Relying Party must validate it against the CRL. It is the Relying Party’s responsibility to determine their requirement for revocation checking.

4.9.7 CRL issuance frequency (if applicable)

CRLs for the RCAs are published when a Sub-CA is revoked, or a new Sub-CA is established, or every 180 days; whichever is the shorter period.

CRLs for Sub-CAs under this CP are published on each certificate revocation or at intervals no longer than 24 hours, if there are no other updates in that period.

The CRL lifespan for Sub-CA types will be:

- 30 days for Policy CAs; and
- 10 days for Issuing CAs.

4.9.8 Maximum latency for CRLs

The maximum latency between the generation and publication of CRLs is 3 days.

4.9.9 Online revocation/status checking availability

Online Certificate Status Protocol service (OCSP) is available at:
http://ocsp.<subscriber>.securesme.com/

Refer to the relevant Certificate Profile in Appendix B - if the certificate is issued with an OCSP access location reference (Authority Information Access extension), OCSP is available to the Relying Party as a certificate status checking method.

The latest CRL is available from the published repositories; refer to 2.1 (Repositories) and the certificates CRL Distribution Point for further information.

4.9.10 On-line revocation checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

See CPS.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

This CP does not support certificate suspension.

4.9.14 Who can request suspension

This CP does not support certificate suspension.

4.9.15 Procedure for suspension request

This CP does not support certificate suspension.

4.9.16 Limits on suspension period

This CP does not support certificate suspension.

4.10 Certificate status services

See CPS.

4.11 End of subscription

See CPS.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Escrow, backup and archiving of private keys issued under this CP is permitted to enable the retrieval of keys in a disaster recovery situation.

PKIaaS Operator hard tokens shall not be backed up or cloned.

Escrow, backup, and archiving is to be undertaken in accordance with the KMP.

Retrieval will be undertaken in accordance with the PKI DRBCP recovery policy and practices.

4.12.2 Session key encapsulation and recovery policy and practices

Symmetric Keys are not required to be escrowed.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

See CPS.

5.2 Procedural Controls

See CPS.

5.3 Personnel controls

See CPS.

5.4 Audit logging procedures

See CPS.

5.5 Records archival

See CPS.

5.6 Key changeover

See CPS.

5.7 Compromise and disaster recovery

See CPS.

5.8 CA or RA termination

See CPS.

6 Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pair generation is via a combination of product and processes approved by the GRCG. Key pair generation is in accordance with the KMP and as such:

- critical core components (e.g. CA and RA) generate keys within an HSM;
- operators generate keys within a hard token or using EAL4 accredited software; and
- non-critical core components generate keys using EAL4 accredited software (and protect them within PKCS#12 files).

6.1.2 Private key delivery to the subscriber

Private key delivery is in accordance with the KMP.

Private keys generated within hardware elements (tokens, HSMs) are not delivered. Soft tokens for core components are to be delivered direct to the PKI core component protected by a PKCS#12 file.

6.1.3 Public key delivery to certificate issuer

RCA public keys are self-generated and do not require delivery.

Sub-CA public key delivery to the RCA is a witnessed event, with the key being delivered via airgap in a PKCS#10 file, signed with the corresponding private key.

Other PKI core components' public keys are either delivered protected within the PKI software, or delivered to the issuer in a PKCS#10 file, signed with the corresponding private key.

6.1.4 Public key delivery to relying parties

See CPS.

6.1.5 Key Sizes

Keys used for this CP are in accordance with the KMP and will use SHA2 for signing and RSA public key algorithm.

The key sizes for RSA CAs:

- RCA is a minimum of 4096 bits;
- Sub-CAs and components, other than operators, are a minimum 2048 bits; and
- Operators are a minimum 2048 bits.

The key sizes for ECC CAs:

- RCA is a minimum of 384 bits;
- Sub-CAs and components, other than operators, are a minimum 384 bits; and

- Operators are a minimum 384 bits

6.1.6 Public key parameters generation and quality checking

See CPS.

6.1.7 Key usage (as per X.509 key usage field)

In addition to the key usage defined in Section 1.4, certificates include key usage extension fields to specify the purposes for which the Certificate may be used, and to technically limit the functionality of the certificate when used with the PKI software.

Note that the CAs have key usages “Digital Signature” and “Non-Repudiation” for the purpose of signing their own log entries.

Key usages are specified in the Certificate Profile set forth in Appendix B.

6.2 Private key production and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

All cryptographic modules used with PKI core components comply with ISM requirements, specifically in complying the Common Criteria scheme Evaluation Assurance Level 4 (EAL4) and US Federal Information Processing Standard Publication 140-3 (FIPS-140-3) requirements.

6.2.2 Private key (n of m) control

See CPS.

6.2.3 Private key escrow

Escrow of private keys is permitted for Sub-CAs and occurs in accordance with the KMP and the PKI DRBCP. Refer to CPS for escrow controls.

6.2.4 Private key backup

See CPS.

6.2.5 Private key archive

Private Key archival occurs in accordance with the PKIaaS KMP and PKIaaS DRBCP.

6.2.6 Private key transfer into or from a cryptographic module

See CPS.

6.2.7 Private key storage on cryptographic module

See CPS.

6.2.8 Method of activating private key

Activating private keys occurs by the CAO or RAO authenticating to the cryptographic module. For HSMs, it is activated with the applicable physical key in the remote PIN Entry Device (PED) or directly into the HSM. The session stays live until deactivated (see 6.2.9 - Method of deactivating private key).

6.2.9 Method of deactivating private key

Deactivation can be achieved via:

- shut down or restart of the system;
- removal of the token; or
- shut down of the service that operates the token.

6.2.10 Method of destroying private keys

See CPS.

6.2.11 Cryptographic module rating

See 6.2.1 (Cryptographic module standards and controls).

6.3 Other aspects of key pair management

6.3.1 Public key archival

See CPS.

6.3.2 Certificate operational periods and key pair usage periods

The RSA RCA certificate validity has a maximum period of 10 years at generation.

The ECC RCA certificate validity has a maximum period of 20 years at generation. A Sub-CA certificate may have a validity period of up to 5 years.

Certificate lives and key pair usage for all other core components, other than Operators, complements the relevant CA they are associated with.

Operator certificates have a maximum validity period of two years.

6.4 Activation Data

6.4.1 Activation data generation and installation

To protect private keys, a passphrase is entered by the key custodian at the time of key generation. This passphrase is used to activate the key pair for usage.

Other passphrases and PINs used within the PKI system are created by operators at the time of installation.

Lifecycle management of passphrases, passwords and PINs used in the system is in accordance with the PKIaaS KMP and ISM.

6.4.2 Activation data protection

All passphrases used to activate core components are kept in accordance with the PKIaaS KMP

6.4.3 Other aspects of activation data

No stipulation

6.5 Computer security controls

See CPS.

6.6 Life cycle technical controls

See CPS.

6.7 Network security controls

See CPS.

6.8 Time stamping

See CPS.

7 Certificate, CRL, and OCSP Profiles

Appendix B contains the formats for the certificates, and CRL profiles and formats relative to this CP. The certificates issued under this CP are:

- The Root Certificate Authorities;
- Sub-CA certificates signed by the Root Certificate Authorities;
- Certificates issued to the PKI core components supporting a CA, such as the Registration Authority; and
- Certificates issued to the operators of the above components to ensure their abilities to undertake administration activities.

7.1 Certificate Profile

7.1.1 Version number(s)

All certificates are X.509 Version 3 certificates.

7.1.2 Certificate extensions

See Appendix B.

7.1.3 Algorithm object identifiers

Certificates under this CP will use one of the following OIDs for signatures.

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }

Table 1: Signature OIDs

Certificates under this CP will use one of the following OIDs for identifying the algorithm for which the subject key was generated.

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type (2) 1}
id-ecDH	{iso(1) identified-organization(3) certicom(132) schemes(1) ecdh(12) }
dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
Id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

Table 2: Algorithm OIDs

CAs shall certify only public keys associated with the crypto-algorithms identified above and shall only use the signature crypto-algorithms described above to sign certificates, CRLs, and any other PKI product, including other forms of revocation such as OCSP responses.

7.1.4 Name forms

The Common Name (CN) component is based on the name assigned by the GRCG to the CA being created presented as a printable string.

All other DN components are fixed and defined in Appendix B.

7.1.5 Name constraints

Name constraints are not present.

7.1.6 Certificate policy object identifier

CA Certificates issued under this policy shall assert the OID {1.2.36.151795998.4.1.1.1.1.0} for RCA certificates or {1.2.36.151795998.4.1.1.1.1.1} for Policy CA certificates or {1.2.36.151795998.4.1.1.1.1.2} for Issuing CA certificates.

All RCA and Sub-CA certificates shall also assert the 'any Policy' OID of {2.5.29.32.0}.

The Sub-CA certificate shall also assert the following OIDs representing Levels of Assurance (LoA) of certificates issued:

Individual:	Low	1.2.36.151795998.4.1.2.1.1
	Medium	1.2.36.151795998.4.1.2.1.2
	High	1.2.36.151795998.4.1.2.1.3
Resources:	Low	1.2.36.151795998.4.1.2.2.1
	Medium	1.2.36.151795998.4.1.2.2.2
	High	1.2.36.151795998.4.1.2.2.3

7.1.7 Usage of policy constraints extension

Policy constraints are not present.

7.1.8 Policy qualifiers syntax and semantics

The only policy qualifiers that are permitted are the CPS Pointer qualifier and the User notice qualifier.

The CPS Pointer, if used, shall contain a HTTP URI link to the Certification Practice Statement (CPS) published by the CA, or to a webpage from which the CPS can then be downloaded.

The User notice, if used, shall only contain the explicitText field.

7.1.9 Processing semantics for the critical certificate policies extension

This policy does not require the certificate policies extension to be critical. Relying Parties whose client software does not process this extension do so at their own risk.

7.2 CRL Profile

7.2.1 Version Number(s)

CRLs for certificates issued under this CPS shall assert a version number as described in the X.509 standard [ISO/IEC 9594-8:2014]. CRLs shall assert Version 2.

7.2.2 CRL and CRL entry extensions

Detailed CRL profiles covering the use of each extension are available in Appendix B.

7.3 OCSP profile

7.3.1 Version number(s)

OCSP is implemented using version 1 as specified under RFC 6960.

7.3.2 OCSP extensions

Refer to CPS and Validation Authority (VA) CP for full OCSP profile.

8 Compliance Audit and Other Assessments

8.1 Frequency or circumstances of assessment

See CPS.

8.2 Identity/qualifications of assessor

See CPS.

8.3 Assessor's relationship to assessed entity

See CPS.

8.4 Topics covered by assessment

See CPS.

8.5 Actions taken as a result of deficiency

See CPS.

8.6 Communication of results

See CPS.

9 Other business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

The Cogito PKIaaS fees charged for certificates and related services can be obtained from https://www.securesme.com/pricing/.

9.1.2 Certificate access fees

Certificates are published into the certificate directory, there is no additional fee for accessing certificates.

9.1.3 Revocation or status information access fees

Revocation status is published in the CRL. There is no additional fee for accessing the CRL.

9.1.4 Fees for other services

Fees for other Cogito PKIaaS services can be obtained from https://www.securesme.com/pricing/.

9.1.5 Refund policy

Where a fee is charged for a certificate, once that certificate is issued a refund will not be provided except where Cogito is responsible for the error. Cogito may at its discretion issue a replacement certificate free of charge or refund the certificate.

9.2 Financial responsibility

9.2.1 Insurance coverage

Cogito shall maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self insured retention.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

Cogito does not provide any insurance and/or extended warranty coverage for end entity certificates issued pursuant to the Gatekeeper framework.

9.3 Confidentially of business information

See CPS.

9.4 Privacy of personal information

See CPS.

9.5 Intellectual property rights

See CPS.

9.6 Representations and Warranties

See CPS.

9.7 Disclaimers of warranties

See CPS.

9.8 Limitations of liability

See CPS.

9.9 Indemnities

See CPS.

9.10 Term and termination

9.10.1 Term

This CP and any amendments shall become effective upon publication in the repository and will remain in effect until notice of their termination is communicated by the Cogito PKIaaS on its repository or website.

The CP is available at http://pki.gatekeepersecuresme.com/policy

9.10.2 Termination

See CPS.

9.10.3 Effect of termination and survival

See CPS.

9.11 Individual Notices and communications with participants

See CPS.

9.12 Amendments

See CPS.

9.13 Dispute resolution provisions

See CPS.

9.14 Governing law

See CPS.

9.15 Compliance with applicable law

See CPS.

9.16 Miscellaneous provisions

See CPS.

9.17 Other provisions

See CPS.

Appendix A Definitions, Acronyms and Interpretation

A.1 Definitions

Accreditation Agencies	Those agencies that provide independent assurance that the facilities, practices, and procedures used to issue certificates comply with the relevant accreditation frameworks (policy, security and legal). Principally these will consist of the DTA.
Application (Request)	A formal request to be considered for a position or to be allowed to do or have something, submitted to an authority, institution, or organization.
Application (Software)	A computer application or relevant component of one (including any object, module, function, procedure, script, macro, or piece of code).
Approved Documents	The Approved Documents are those approved by the GRCG and include those approved by the Gatekeeper Competent Authority. E.g., CPS, CPs, ICTSP, SSP, KMP, DRBCP, IRP and PKI Operations Manual.
Authorised Key Retriever	An AKR is a RO who is authorised to retrieve confidentiality keys from the Key Archive Server (KAS).
Authorised RA	Has the meaning given to it in paragraph 1.3.2 of this CPS.
Business Day	Any day other than a Saturday, Sunday or public holiday for the whole of the Australian Capital Territory. Traditionally such days are from 0900 to 1700.
Certificate	An electronic document signed by the Certification Authority which: i. Identifies a Subscriber by way of a Subject Distinguished Name (Identity certificates) and a Resource by way of a Subject Distinguished Name and/or Subject Alternative Name (Resource certificates); ii. Binds the Subject to a Key Pair by specifying the Public Key of that Key Pair; and iii. Contains the information required by the Certificate Profile.
Certificate Assurance Level	See Level of Assurance.
Certificate Information	Information needed to generate a digital certificate required by the Certificate Profile.
Certificate Policy	Means the definition adopted by RFC3647, which defines a Certificate Policy as “A named set of rules that indicates the

	applicability of a Certificate to a particular community and/or class of applications with common security requirements".
Certificate Profile	A certificate profile provides details about the format and contents of a digital certificate, including, for a natural person, their Distinguished Name.
Certificate Repository	The Certificate Repository provides a scalable mechanism to store and distribute certificates, cross-certificates and CRLs to end users of the PKI.
Certificate Revocation List	The published file which lists the Digital Certificates that have been revoked by the Issuing CA before their scheduled expiration.
Certificate Authority	A Certificate Authority (or Certification Authority) (CA) is an entity which issues digital certificates for use by other parties.
Certificate Store	Storage location for certificates on a computer or device.
Certification Practice Statement	A statement of the practices that a Certification Authority employs in managing the digital Certificates it issues (this includes the practices that a Registration Authority employs in conducting registration activities on behalf of that Certification Authority). These statements will describe the PKI certification framework, mechanisms supporting the application, insurance, acceptance, usage, suspension/revocation, and expiration of Digital Certificates signed by the CA, and the CA's legal obligations, limitations, and miscellaneous provisions.
Common Name	Is the characteristic value within a Distinguished Name. Typically, it is a descriptive name of the user or service e.g., "Bruce Smith" or "Application Web Handler". Where technically required, the Common Name can be the resources domain name.
Cross certification	The establishment of a trust relationship between two PKIs, where one CA signs another PKI's CA certificate. This creates a chain of trust allowing the subscribers of the cross-certifying CA to trust those of the cross-certified CA. If done two-ways (PKIs signing each other's CAs' certificates), mutual trust can be established.
Cross Certification Ceremony	The event where a cross-certification agreement is executed, i.e. one CA creates a cross-certification request to another CA. The cross-signing CA creates and returns the cross-certificate, signed with its own private key. The "ceremony" is a formal event and is witnessed by representatives of both CAs. Details of the event are recorded and signed by the witnesses to provide an audit record.
Custodian	A person who has custody of something, a keeper or guardian; in the context of PKI, usually a Key Custodian.

Device	Device means any computer hardware or other electronic device.
Digital Signature	An electronic signature created using a Private Signing Key.
Directory Service	A directory service is a software application - or a set of applications – that stores and organises information about a computer network's users and network resources, and that allows network administrators to manage users' access to the resources. Additionally, directory services act as an abstraction layer between users and shared resources. The X.500 and LDAP directory services are examples of general-purpose distributed hierarchical object-oriented directory technologies. Both offer complex searching and browsing capabilities are used for white pages, network information services, PKI, and a wide range of other applications.
Distinguished Name (DN)	A unique identifier assigned to, as relevant: i. the Subject identified by; and ii. the issuer of a Certificate, having the structure required by the Certificate Profile.
Evaluated Product List (EPL)	The Evaluated Product List is produced to assist in the selection of products that will provide an appropriate level of information security. The list, maintained by ASD, is published at https://www.cyber.gov.au/acsc/view-all-content/epl-products The EPL lists products that: i. Have completed Common Criteria (CC) or ITSEC certification, ii. Are in evaluation within the AISEP, or iii. Have completed some other recognised ASD evaluation methodology.
Evaluation Assurance Level	The Evaluation Assurance Level (EAL1 through EAL7) of a computer product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation, an international standard in effect since 1999. The increasing assurance levels reflect added assurance requirements that must be met to achieve Common Criteria certification. The intent of the higher levels is to provide higher confidence that the system's principal security features are reliably implemented. See also Protection Profile.
Evidence of identity	Evidence (e.g. in the form of documents) issued to substantiate the identity of the presenting party, usually produced at the time of Registration (i.e. when authentication credentials are issued).

Exercised	To discharge or perform a function. An act of employing or putting into play.
Gatekeeper	The Commonwealth Government strategy to develop Public Key Infrastructure to facilitate Government online service delivery and electronic procurement.
Hard Token	A hard token, sometimes called an “authentication token”, is a hardware security device that is used to authorise a Subscriber. A common example of a hard token is a smartcard.
High Assurance Certificate (Gatekeeper)	A digital certificate issued by a Gatekeeper Accredited or Recognised Service Provider to Organisations and individuals for the purpose of transacting online with government agencies and whose risk and threat to data are assessed as high. This category is characterised by a requirement for a Formal Identity Verification Model EOI check by a Gatekeeper accredited Registration Authority.
Identity Certificate	An identity certificate is a certificate which uses a digital signature to bind together a public key with a human identity – information such as the name of a person, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
Key	A Key is a string of characters used with a cryptographic algorithm to encrypt and decrypt.
Key Custodian	A key custodian refers to the authorised person appointed to manage a key on behalf of the subscriber.
Key Pair	A pair of asymmetric cryptographic Keys (e.g. one decrypts messages which have been encrypted using the other) consisting of a Public Key and a Private Key.
Level of Assurance	Levels of trust associated with a credential as measured by the associated technology, processes, and policy and practice statements controlling the operational environment. In the context of this CPS, the term refers to four levels of assurance of certificates (low, medium, high, very high) defined for the PKIaaS. A “No Assurance” level OID is used for test certificates.
Network Resource	Network Resources (devices) are units that mediate data in a computer network. Computer networking devices are also called network equipment and commonly include routers, gateways, switches, hubs, repeaters, and firewalls.
National Cryptographic Authority (NCA)	The NCA of Australia is the Australian Signals Directory (ASD).ASD also maintain a list of evaluated and approved security products for use by Australian Government agencies (Evaluated Products List – EPL).

No Lone Zone	A physically secure area which has been defined as an area which when occupied must have 2 or more trusted personnel as occupants.
Non-Person Entity	An entity with a digital identity (for example an IP address or MAC address) that acts in cyberspace but is not a legal entity. This can include web sites, hardware devices, software applications, and information artefacts.
Modification (of Certificate)	Certificate modification means the issuance of a new certificate due to changes in the information in the certificate other than the Subscriber public key (RFC3647).
Object Identifier	An OID is a string of decimal numbers that uniquely identifies an object. These objects are typically an object class or an attribute. It serves to name almost every object type in X.509 Certificates, such as components of Distinguished Names and Certificate Policies.
Online Certificate Status Protocol (OCSP)	Method of establishing the status of a certificate that has not expired. A PKI enabled client requests the status of a certificate from an OCSP responder. The responder provides a response (“good”, “revoked” or “unknown”) to the client. OCSP is a more bandwidth efficient method than the download of a full Certificate Revocation List (CRL).
Operational CA	A CA that issues and manages end-entity certificates.
Operator	Any individual who is assigned keys and certificates to perform functions within the PKI. They are not regarded as either Subscribers or Relying Parties for the purposes of the PKIaaS.
Personal Identity Verification (PIV)	Standard created by National Institute for Standards and Technology (NIST) in response to Homeland Security Presidential Directive 12 (HSPD 12) of Aug 2004. Full name “Personal Identity Verification of Federal Employees and Contractors”. Also known as FIPS 201. Specifies interfaces, biometrics, and algorithms for PIV compliant cards.
PKI Operations Manager	Manages PKI Operations of the PKIaaS.
PKI Operator	PKI Operators perform day to day operations, maintenance and support of the PKI systems managed as part of the PKIaaS.
PKI Software	Software programs that manage digital certificate lifecycle operations and token management.
PKI Systems Administrator	A PKI Systems Administrator performs system administration tasks on the PKIaaS systems.

Private Certificate Signing Key	The Private Key used by the CA to digitally sign certificates.
Private Confidentiality Key	The key used by the addressee to decrypt messages, which have been encrypted using the corresponding Public Confidentiality Key
Private Key	The private key in an asymmetric key pair that must be kept secret to ensure confidentiality, integrity authenticity and non-repudiation.
Private Signing Key	A private key used to digitally sign messages on behalf of the relevant certificate Subject.
Protection Profile	A document that stipulates the security functionality that must be included in Common Criteria evaluation to meet a range of defined threats. Protection Profiles also define the activities to be taken to assess the security function of an evaluated product.
Public Key	The Key in an asymmetric key pair which may be made public.
Public Key Infrastructure (PKI)	The combination of hardware, software, people, policies, and procedures needed to create, manage, store and distribute keys and certificates based on public key cryptography.
Public Key Technology (PKT)	Public Key Technology is the hardware and software used for encryption, signing and verification as well as the software for managing Digital Certificates.
Registration Authority (RA)	A Registration Authority (RA) is an entity that is responsible for one or more of the following functions on behalf of a CA: i. Processing certificate application; ii. Processing requests to revoke certificates; and iii. Processing requests to renew, re-key or modify certificates. Processing includes the identification and authentication of certificate applicants and approval or rejection of requests. See section 1.3.2 (Registration Authorities) of this CPS and the relevant Certificate Policy (CP) for more information about the applicable RA.
Registration Officer (RO)	A person authorised by a Registration Authority (RA) to perform RA functions in accordance with this CPS, the relevant Certificate Policy and other applicable documentation.
Re-Key	A Subscriber or other participant generating a new keypair and applying for the issuance of a new certificate that certifies the new

	public key. Normally used at the time of expiry of the certificate (RFC3647).
Relying Party	A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.
Renewal (of certificate)	Renewal means the issuance of a new certificate to the subscriber without changing the Subscriber's public key or any other information in the certificate (RFC3647). The validity period and serial number will be different in the renewed certificate.
Repository	A database of information (e.g. Certificate status, evaluated documents) which is made accessible to users including the Relying Parties.
Resource	Includes any Network Resource, Application, code, electronic service or process, Device, or data object that is capable of utilising a Certificate.
Resource Administrator	The Resource Administrator has the day-to-day responsibility for a resource and will in most cases be the person who requests, or installs, a certificate for the resource they are managing (also referred to as a Systems Administrator or Trusted Installer).
Resource Certificate	A Resource Certificate is a certificate issued in respect of a resource.
Revoke	Tio terminate a certificate prior to the end of its operational period.
Root CA	A CA that is the top of a certificate chain, i.e. its own certificate is self signed.
Subordinate CA (SubCA)	A CA which has been established under the certificate path of a Root CA. A SubCA usually issues certificates to end entities and manages those certificates. See also Operational CA.
Subscriber	A Subscriber is, as the context allows: i. For Identity Certificates, i.e. those issued to Person Entities (PE); the person whose Distinguished Name appears as the "Subject Distinguished Name" on the relevant Certificate; and ii. For Resource Certificates, i.e. those issued to Non-Person Entities (NPE); the person or legal entity that applied for that Certificate, and/or administers the system that utilises the Certificate. Individual CPs provide context for the definition of Subscriber relevant to that CP.
Subscriber Agreement	An agreement between the relevant Service Provider and a Subscriber, which sets out the respective rights, obligations, and

	liabilities of those parties, and which legally, binds those parties to the relevant Certificate Policy and Certification Practice Statement.
Superior CA	A CA which establishes/signs the certificate of a Subordinate CA.
Token	A hardware security device containing a user's Private Key(s), and Public Key Certificate.
Transport Layer Security (TLS)	A cryptographic protocol that provides security for communications over networks such as the Internet. TLS encrypts the segments of network connections at the Transport Layer end-to-end.
Universally Unique Identifier (UUID)	A universally unique identifier is a 128-bit label used for information in computer systems. The term globally unique identifier is also used, often in software created by Microsoft (GUID). When generated according to the standard methods, UUIDs are, for practical purposes, unique. See RFC 4122.
Validation Authority	A Validation Authority (VA) is an entity that can perform one or more of the following functions: i. processing certificate status requests; ii. validating credentials and authentication requests; iii. validating signatures; and iv. other services related to PKI and online authentication. The PKIaaS Validation Authority provides certificate status information through the provision of OCSP responders.

Additional terms not defined in this Glossary, but which may be relevant can be found in the Identity and Access Management Glossary (refer to https://www.dta.gov.au). Where terms are defined in both the Identity and Access Management Glossary and this Glossary then for the purpose of Gatekeeper accreditation the definition in the Identity and Access Management Glossary will be determinative. The GRCG is the authoritative source of definitions relating to the Cogito PKIaaS, any requirement for clarification can be referred to the GRCG.

A.2 Acronyms

ACT	Australian Capital Territory
AKR	Authorised Key Retriever
ASD	Australian Signals Directorate
CA	Certification Authority
CP	Certificate Policy

CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DRBCP	Disaster Recovery and Business Continuity Plan
DTA	Digital Transformation Agency
EAL	Evaluated Assurance Level
EOI	Evidence of Identity
EPL	Evaluated Products List
GRCG	Governance Risk and Compliance Group
HSM	Hardware Security Module
ICTSP	Information and Communication Technology Security Plan
IEC	International Electrotechnical Commission
IETF	Internet Engineering Taskforce
IP	Intellectual Property
IPR	Intellectual Property Rights
ISM	Australian Government Information Security Manual
ISO	International Standards Organisation
ITSEC	Information Technology Security Evaluation Criteria
KAS	Key Archive Server
KMP	Key Management Plan
LTSK	Long Term Key Storage
NCA	National Cryptographic Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKT	Public Key Technology

PSPF	Protective Security Policy Framework
RA	Registration Authority
RCA	Root Certification Authority
RFC	Request For Comment
RO	Registration Officer
SO	Security Officer
SRMP	Security Risk Management Plan
SSP	System Security Plan
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time

A.3 Interpretation

In Approved Documents, unless the contrary intention appears:

i. A reference to the singular includes plural and vice versa;

ii. Words importing a gender include any other gender;

iii. A reference to a person includes a natural person, partnership, body corporate, association, governmental or local authority or agency, or Device or Application or other entity;

iv. A reference to a document or instrument includes the document or instrument as altered, amended, supplemented or replaced from time to time;

v. A reference to a section is a reference to the relevant section of that document;

vi. An amendment or replacement of a document does not imply any consequent amendment or alteration to any other document;

vii. Where a word or phrase is given a particular meaning, other parts of speech and grammatical forms of that word or phrase have corresponding meanings;

viii. The meaning of general words is not limited by specific examples introduced by ‘including’, ‘for example’ or similar expressions;

ix. The headings are for convenience only and are not to be used in the interpretation of an Approved Document; and

x. Any appendix or attachment to an Approved Document (no matter how named) forms part of that document.

Appendix B Certificate and CRL Profiles and Formats

B.1 RSA Root CA Signature/Authentication Certificate

Field	Critical	RSA Root Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509.
Serial		<octet string>	Must be unique within the PKIaaS namespace.
Issuer Signature Algorithm		SHA256WithRSAEncryption	
Issuer Distinguished Name		CN= <Subscriber>CA<Serial> OU= CAs OU= PKI O= <Subscriber> C= AU	Encoded as printable string. <Subscriber> is an identifier for the subscribing organisation. <Serial> denotes the number after <Subscriber> that represents the issuing CA. starting at “001”.
Validity Period		Not before <UTCtime> Not after <UTCtime>	Maximum 10 years from date of issue.
Subject Distinguished Name		CN= <Subscriber>CA<Serial> OU= CAs	Encoded as printable string.

Field	Critical	RSA Root Certificate Value	Notes
		OU= PKI O= <Subscriber> C= AU	As this is a Root CA, the Issuer and Subject Distinguished Name should be the same.
Subject Public Key Information		Minimum 4096 bit RSA key modulus, rsaEncryption	
Issuer Unique Identifier		Not Present	
Subject Unique Identifier		Not Present	
X.509 V3 extensions:			
Authority Key Identifier	No	<octet string>	256 bit SHA256 hash of binary DER encoding of the issuing CA's public key.
Subject Key Identifier	No	<octet string>	256 bit SHA256 hash of binary DER encoding of subject's public key.
Key usage	Yes	digitalSignature, nonRepudiation, Certificate signing, CRLsigning, Off-line CRL signing	Digital signature and non-repudiation key usages are only used for the signing of the CA's own log entries.
Extended key usage		Not Present	

Field	Critical	RSA Root Certificate Value	Notes
Private key usage period		Not Present	
Certificate policies	No	[1] Policy OID: {1.2.36.151795998.4.1.1.1.1} Policy Qualifier - CPS pointer: http://pki.gatekeeper.securesme.com/	The OID of this CP (RCA).
		[2] Policy OID: {2.5.29.32.0}	anyPolicy OID.
Policy Mapping		Not Present	
Subject Alternative Name		Not Present	
Issuer Alternative Name		Not Present	
Subject Directory Attributes		Not Present	
Basic Constraints	Yes	CA=True, path length constraint=none	
Name Constraints		Not Present	
Policy Constraints		Not Present	

Field	Critical	RSA Root Certificate Value	Notes
Authority Information Access		Not Present	
CRL Distribution Points		Not Present	

Table 3: RSA Root CA Signature/Authentication Certificate

B.2 RSA RCA CRL

See RFC 6818 for detailed syntax. The following table lists which fields are expected

Field	Critical	RSA Root CA CRL Value	Notes
Version		V2 (1)	X.509 Version 2 CRL profile.
Issuer Signature Algorithm		SHA256WithRSAEncryption	
Issuer Distinguished Name		CN= <Subscriber>CA<Serial> OU= CAs OU= PKI O= <Subscriber>	

		C= AU	
thisUpdate		<UTCTime>	
nextUpdate		<UTCTime>	Date by which the next CRL will be issued (at the latest. If a CA certificate is revoked, or a new CA generated, a CRL will be issued at that time) thisUpdate +180 days.
Revoked certificates list		0 or more 2-tuple of certificate serial number and revocation date (in UTCTime)	
CRL extensions			
CRL Number	No	<Integer>	
Authority Key Identifier	No	<Octet String>	The value of this field is the 256 bit SHA256 hash of the binary DER encoding of the CA public key information.
CRL entry extensions			
Invalidity Date	No	Optional	Date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid.
Reason Code	No	Optional	

Table 4: RSA RCA CRL Profile

B.3 RSA Subordinate CA Signature/Authentication Certificate

Field	Critical	RSA Sub Certificate Authority Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509.
Serial		<octet string>	Must be unique within the PKIaaS namespace.
Issuer Signature Algorithm		SHA256WithRSAEncryption	
Issuer Distinguished Name		CN= <Subscriber>CA<Serial> OU= CAs OU= PKI O= <Subscriber> C= AU	Encoded as printable string. <Serial> denotes the number after <Subscriber> that represents the issuing CA starting at “101”.
Validity Period		Not before <UTCtime> Not after <UTCtime>	Maximum 5 years from date of issue.
Subject Distinguished Name		CN= <Subscriber>CA<Serial> OU= CAs OU= PKI	Encoded as printable string. <Serial> denotes the number after <Subscriber> that represents this CA. starting from “301”.

Field	Critical	RSA Sub Certificate Authority Certificate Value	Notes
		O= <Subscriber> C= AU	
Subject Public Key Information		Minimum 2048 bit RSA key modulus, rsaEncryption	
Issuer Unique Identifier		Not Present	
Subject Unique Identifier		Not Present	
X.509 V3 extensions:			
Authority Key Identifier	No	<octet string>	256 bit SHA256 hash of binary DER encoding of the issuing CA's public key
Subject Key Identifier	No	<octet string>	256 bit SHA256 hash of binary DER encoding of subject's public key
Key usage	Yes	digitalSignature, nonRepudiation, Certificate Signing, Off-line CRL Signing, CRL Signing	Digital signature and Non repudiation key usages only used for signing the CA's own log entries.
Extended key usage		Not Present	

Field	Critical	RSA Sub Certificate Authority Certificate Value	Notes
Private key usage period		Not Present	
Certificate policies	No	[1] Policy OID: {1.2.36.151795998.4.1.1.1.1} (this CP/Sub-CAs) Policy Qualifier - CPS pointer: http://pki.gatekeeper.securesme.com/	The OID of this CP (Sub-CA).
		[2] Policy OID: {2.5.29.32.0}	OID for “anyPolicy”.
		[3] Policy OID: {1.2.36.151795998.4.1.2.1.1} (Individual – Low Assurance)	
		[4] Policy OID: {1.2.36.151795998.4.1.2.1.2} (Individual – Medium Assurance)	
		[5] Policy OID: {1.2.36.151795998.4.1.2.1.3} (Individual - High Assurance)	
		[6] Policy OID: {1.2.36.151795998.4.1.2.2.1} (Resource – Low Assurance)	
		[7] Policy OID: {1.2.36.151795998.4.1.2.2.2} (Resource – Medium Assurance)	
		[8] Policy OID: {1.2.36.151795998.4.1.2.2.3} (Resource – High Assurance)	

Field	Critical	RSA Sub Certificate Authority Certificate Value	Notes
Policy Mapping		Not Present	
Subject Alternative Name		Not Present	
Issuer Alternative Name		Not Present	
Subject Directory Attributes		Not Present	
Basic Constraints	Yes	CA=True, Path length constraint=0	
Name Constraints		Not Present	
Policy Constraints		Not Present	
Authority Information Access	No	[1] Access method: CAIssuer {1.3.6.1.5.5.7.48.2} Access location: http://pki.<Subscriber>.securesme.com/Certificates/<Subscriber>CA<Serial>.cer [2] Access method: CAIssuer {1.3.6.1.5.5.7.48.2} Access location: http://pki.<Subscriber>.securesme.com/Certificates/<Subscriber>CA<Serial>.p7b	

Field	Critical	RSA Sub Certificate Authority Certificate Value	Notes
		[3] Access method: OCSP {1.3.6.1.5.5.7.48.1} Access location: http://ocsp.<Subscriber>.securesme.com/	
CRL Distribution Points	No	Distribution Point: [1] URL= http://pki.gatekeeper.securesme.com/CRL/<Subscriber>CA<Serial>.crl [2] Distribution Point Name (LDAP): ldap://dir.<Subscriber>.securesme.com/cn=<Subscriber>CA<Serial>,ou=CAs,ou=PKI,o=<Subscriber>,c=au?certificateRevocationList	The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reason field may be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Table 5: RSA Subordinate CA Signature/Authentication Certificate Profile

B.4 RSA SubCA CRL

See RFC 6818 for detailed syntax. The following table lists which fields are expected. This profile can be used for both Policy and Issuing CAs under this CP.

Field	Critical	RSA Sub-CA CA CRL Value	Notes
Version		V2 (1)	X.509 Version 2 CRL profile.

Issuer Signature Algorithm		SHA256WithRSAEncryption	
Issuer Distinguished Name		CN= <Subscriber>CA<Serial> OU= CAs OU= PKI O= <Subscriber> C= AU	<Serial> denotes the number after <Subscriber> that represents the associated CA.
thisUpdate		<UTCTime>	
nextUpdate		<UTCTime>	Date by which the next CRL will be issued (at the latest – if a certificate is revoked, a CRL will be issued at that time). Policy CA: thisUpdate + 30 days. Issuing CA: thisUpdate + 10 days.
Revoked certificates list		0 or more 2-tuple of certificate serial number and revocation date (in UTCTime)	
CRL extensions			
CRL Number	No	<Integer>	

Authority Key Identifier	No	<Octet String>	The value of this field is the 256-bit SHA256 hash of the binary DER encoding of the CA public key information.
CRL entry extensions			
Invalidity Date	No	Optional	Date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid.
Reason Code	No	Optional	

B.5 ECC RCA Signature/Authentication Certificate

Field	Critical	ECC Root Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509.
Serial		<octet string>	Must be unique within the PKIaaS namespace.
Issuer Signature Algorithm		sha384ECDSA	

Field	Critical	ECC Root Certificate Value	Notes
Issuer Distinguished Name		CN= <Subscriber>CA<Serial> OU= CAs OU= PKI O= <Subscriber> C= AU	Encoded as printable string. <Serial> denotes the number after <Subscriber> that represents the issuing CA. and is expected to start at “001”.
Validity Period		Not before <UTCtime> Not after <UTCtime>	Maximum 10 years from date of issue.
Subject Distinguished Name		CN= <Subscriber>CA<Serial> OU= CAs OU= PKI O= <Subscriber> C= AU	Encoded as printable string.
Subject Public Key Information		sha384ECDSA	ECC secp384r1 FIPS186-3 p-384
Issuer Unique Identifier		Not Present	

Field	Critical	ECC Root Certificate Value	Notes
Subject Unique Identifier		Not Present	
X.509 V3 extensions:			
Authority Key Identifier	No	<octet string>	384 bit SHA384 hash of binary DER encoding of signing CA's public key.
Subject Key Identifier	No	<octet string>	384 bit SHA384 hash of binary DER encoding of subject's public key.
Key usage	Yes	digitalSignature, nonRepudiation, Certificate signing, CRLsigning, Off-line CRL signing	Digital signature and non-repudiation key usages are only used for the signing of the CA's own log entries.
Extended key usage		Not Present	
Private key usage period		Not Present	
Certificate policies	No	[1] Policy OID: {1.2.36.151795998.4.1.1.1.1} Policy Qualifier - CPS pointer: http://pki.gatekeeper.securesme.com/	The OID of this CP (RCA).
		[2] Policy OID: {2.5.29.32.0}	anyPolicy OID.

Field	Critical	ECC Root Certificate Value	Notes
Policy Mapping		Not Present	
Subject Alternative Name		Not Present	
Issuer Alternative Name		Not Present	
Subject Directory Attributes		Not Present	
Basic Constraints	Yes	CA=True, path length constraint=none	
Name Constraints		Not Present	
Policy Constraints		Not Present	
Authority Information Access		Not Present	
CRL Distribution Points		Not Present	

Table 6: ECC RCA Signature/Authentication Certificate Profile

B.6 ECC RCA CRL

Field	Critical	ECC Root CA CRL Value	Notes
Version		V2 (1)	X.509 Version 2 CRL profile.
Issuer Signature Algorithm		sha384ECDSA	
Issuer Distinguished Name		CN= <Subscriber>CA<Serial> OU= CAs OU= PKI O= <Subscriber> C= AU	
thisUpdate		<UTCTime>	
nextUpdate		<UTCTime>	Date by which the next CRL will be issued (at the latest – if a certificate is revoked, a CRL will be issued at that time) thisUpdate + 31 days.
Revoked certificates list		0 or more 2-tuple of certificate serial number and revocation date (in UTCTime)	
CRL extensions			
CRL Number	No	<Integer>	
Authority Key Identifier	No	<Octet String>	The value of this field is the 384 bit SHA384 hash of the binary DER encoding of the CA public key information

CRL entry extensions			
Invalidity Date	No	Optional	Date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid.
Reason Code	No	Optional	

Table 7: ECC RCA CRL Profile

B.7 ECC SubCA Signature/Authentication Certificate

Field	Critical	ECC SubCA Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509.
Serial		<octet string>	Must be unique within the Cogito PKIaaS namespace.
Issuer Signature Algorithm		sha384ECDSA	
Issuer Distinguished Name		CN= <Subscriber>CA<Serial> OU= CAs OU= PKI O= <Subscriber>	Encoded as printable string.

Field	Critical	ECC SubCA Certificate Value	Notes
		C= AU	
Validity Period		Not before <UTCtime> Not after <UTCtime>	Maximum 5 years from date of issue.
Subject Distinguished Name		CN= <Subscriber>CA<Serial> OU= CAs OU= PKI O= <Subscriber> C= AU	Encoded as printable string. <Serial> denotes the number after <Subscriber> that represents the issuing CA.
Subject Public Key Information		Minimum 384bit ECC secp384r1	
Issuer Unique Identifier		Not Present	
Subject Unique Identifier		Not Present	
X.509 V3 extensions:			
Authority Key Identifier	No	<octet string>	384 bit SHA384 hash of binary DER encoding of the issuing CA's public key.

Field	Critical	ECC SubCA Certificate Value	Notes
Subject Key Identifier	No	<octet string>	384 bit SHA384 hash of binary DER encoding of subject's public key.
Key usage	Yes	digitalSignature, nonRepudiation, Certificate Signing, Off-line CRL Signing, CRL Signing	Digital signature and Non repudiation key usages only used for signing the CA's own log entries.
Extended key usage		Not Present	
Private key usage period		Not Present	
Certificate policies	No	[1] Policy OID: {1.2.36.151795998.4.1.1.1.1} (this CP/SubCAs) Policy Qualifier - CPS pointer: http://pki.gatekeeper.securesme.com/	The OID of this CP (SubCA).
		[2] Policy OID: {2.5.29.32.0}	OID for "anyPolicy".
		[3] Policy OID: {1.2.36.151795998.4.1.2.1.1} (Individual – Low Assurance)	
		[4] Policy OID: {1.2.36.151795998.4.1.2.1.2} (Individual – Medium Assurance)	
		[5] Policy OID: {1.2.36.151795998.4.1.2.1.3} (Individual - High Assurance)	

Field	Critical	ECC SubCA Certificate Value	Notes
		[6] Policy OID: {1.2.36.151795998.4.1.2.2.1} (Resource – Low Assurance)	
		[7] Policy OID: {1.2.36.151795998.4.1.2.2.2} (Resource – Medium Assurance)	
		[8] Policy OID: {1.2.36.151795998.4.1.2.2.3} (Resource – High Assurance)	
Policy Mapping		Not Present	
Subject Alternative Name		Not Present	
Issuer Alternative Name		Not Present	
Subject Directory Attributes		Not Present	
Basic Constraints	Yes	CA=True, Path length constraint=1	
Name Constraints		Not Present	
Policy Constraints		Not Present	

Field	Critical	ECC SubCA Certificate Value	Notes
Authority Information Access	No	[1] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://pki.<Subscriber>.securesme.com/Certificates/<Subscriber>CA<Serial>.cer [2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://pki.<Subscriber>.securesme.com/Certificates/<Subscriber>CA<serial>.p7b [3] Access method: OCSP {1.3.6.1.5.5.7.48.1} Access location: http://ocsp.<Subscriber>.securesme.com/	
CRL Distribution Points	No	Distribution Point: [1] URL= http://pki.<Subscriber>.securesme.com/crl/<Subscriber>CA<Serial>.crl [2] Distribution Point Name (LDAP): ldap://dir.<Subscriber>.securesme.com/cn=<Subscriber>CA<serial>,ou=CAs,ou=PKI,o=<Subscriber>,c=AU?certificateRevocationList	The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reason field may be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Table 8: ECC SubCA Signature/Authentication Certificate

B.8 ECC SubCA CRL

See RFC6818 for detailed syntax. The following table lists which fields are expected. This profile can be used for both policy or issuing CAs

Field	Critical	ECC Sub-CA CA CRL Value	Notes
Version		V2 (1)	X.509 Version 2 CRL profile.
Issuer Signature Algorithm		sha384ECDSA	
Issuer Distinguished Name		CN= <Subscriber>CA<Serial> OU= CAs OU= PKI O= <Subscriber> C= AU	
thisUpdate		<UTCTime>	
nextUpdate		<UTCTime>	Date by which the next CRL will be issued (at the latest – if a certificate is revoked, a CRL will be issued at that time). Policy CA: thisUpdate + 30 days. Issuing CA: thisUpdate + 10 days.

Revoked certificates list		0 or more 2-tuple of certificate serial number and revocation date (in UTCTime)	
CRL extensions			
CRL Number	No	<Integer>	
Authority Key Identifier	No	<Octet String>	The value of this field is the 384 bit SHA384 hash of the binary DER encoding of the CA public key information.
CRL entry extensions			
Invalidity Date	No	Optional	Date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid.
Reason Code	No	Optional	

Table 9: ECC SubCA CRL Profile