X.509 Certificate Policy (CP)

Cogito PKI as a Service - Individual - Software Certificates

5 October 2023

Version 1.1

Notice to all parties seeking to rely

Reliance on a certificate issued under this Certificate Policy, identified by subarcs of the object identifier 1.2.36.151795998.4.1.1.2.1 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
2021-09-16	1.0	Brad Fardig	Released
2023-10-05	1.1	Brad Fardig	Review and correct typographical errors

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) Individual - Software identity certificates, including 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 in the 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 CP.

1.1 Overview

This CP only applies to certificates issued to Cogito PKIaaS and Subscriber individuals for the establishment of the identity of an individual who has an affiliation with the Cogito PKIaaS or the Subscribing Agency and has been approved to:

i. Interact directly with Subscribing Agency or Cogito PKIaaS assets or systems using Public Key Technology;

ii. Authenticate with a third party, as an affiliate of the Subscribing Agency or Cogito PKIaaS; or

iii. Provide a digital signature, as an individual affiliated with the Subscribing Agency or the Cogito PKIaaS.

There are two types of certificate issued under this CP namely:

i. Signing/authentication certificates; and

ii. Encryption/confidentiality certificates.

No authority, or privilege, applies to a resource by becoming an approved Individual - Software Certificate holder, other than confirming an affiliation with the Subscribing Agency or the Cogito PKIaaS.

This CP allows Subscriber's keys and certificates to reside on soft or hardware based tokens.

1.2 Document Name and Identification

The title for this CP is Cogito PKI as a Service - Individual - Software Certificates. The Object Identifier for this CP is: 1.2.36.151795998.4.1.1.2.1

{iso (1) iso-member (2) australia (36) cogito-group-pty-ltd (151795998) Cogito PKIaaS(4) pki (1) certificate policy (1) Individual (2) Software (1)}

Extensions of this OID represent the certificate variants governed by this CP. They are identified in Appendix B.

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.

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

A Subscriber refers to the individual (person) whose name appears in the subject in a certificate and includes any individual that has been approved as having a requirement to be authenticated as affiliated with the Subscribing Agency or the Cogito PKIaaS. Subscribers include:

i. Subscribing Agency or Cogito PKIaaS Personnel (permanent or casual);

ii. Subscribing Agency or Cogito PKIaaS Contractors, Consultants and Professional Service Providers; and

iii. Other persons approved by the Subscribing Agency or Cogito PKIaaS as having a requirement for a certificate.

A subscriber issued a certificate under this CP does not automatically receive assess, authority or privilege to Subscribing Agency or Cogito PKIaaS assets or systems. Subscribing Agency or Cogito PKIaaS assets or systems may act as a Relying Party granting access, authority, or privilege to an individual.

1.3.4 Relying Parties

A Relying Party may use an individual software certificate to:

i. Verify the identity of a subscriber;

ii. Verify the integrity of a communication with the Subscriber;

iii. Establish confidential communications with a Subscriber; and

iv. Ensure the non-repudiation of a communication with a Subscriber.

Before relying on the Subscriber certificate, a Relying Party must:

i. Verify the validity of a digital certificate;

ii. Verify that the digital certificate is being used within the limits specified in the CP; and

iii. Promptly notify the RA in the event that it suspects that there has been a compromise of the Subscriber's Private Keys.

A Relying Party is responsible for deciding whether, and how, to establish:

i. The processes of checking validity of the Subscriber's certificate;

ii. Any authority, or privilege, of the Subscriber to act on behalf of the Subscribing Agency or Cogito PKIaaS; and

iii. Any authority, access or privilege the Subscriber has to the Relying Party's assets or systems.

A Relying Party agrees to the conditions of this CP and the CPS. The use of a certificate, or associated revocation information, issued under this CP is the Relying Party's acceptance of the terms and conditions of this CP and CPS.

1.3.5 Other Participants

See CPS for other participants and their responsibilities.

1.4 Certificate Usage

Certificates issued under this CP, in conjunction with their associated private keys, may be used:

i. Authenticate themselves to a Relying Party electronically in online transactions;

ii. Digitally sign electronic documents, transactions, and communications; and

iii. Confidentially communicate with a Relying Party.

1.4.1 Appropriate Certificate Uses

Appropriate use for Certificates issued under this CP, in conjunction with their associated private key, is:

i. For the authentication of the identity of a Subscriber, during the conduct of any lawful business with that individual, as an individual affiliated with the Subscribing Agency or the Cogito PKIaaS and for which the level of assurance has been assessed as sufficient by the GRCG and the Relying Party organisation;

ii. To provide accountability and non-repudiation of the Subscriber transactions or communications;

iii. To verify the integrity of a communication from a subscriber to ta Relying Party; and

iv. For the sending and receiving of confidential communications, provided such communication is in accordance with normal Subscribing Agency or Cogito PKIaaS business and security policy and procedures.

1.4.2 Prohibited Certificate Uses

The prohibited uses for certificates issued under this CP are:

i. To use the certificate in a way that represents that the certificate possesses any attribute, authority, access, privilege, or delegations that may be afforded to the Subscriber;

ii. To use the certificate in a **way** that represents that communications and transactions can only occur over certain specified infrastructure for that transaction or communication; and

iii. For a Subscriber to conduct any transaction, or communication, which is any or all of the following:

   a. Unrelated to organisational business;

   b. Illegal;

   c. Unauthorised;

   d. Unethical; or

   e. Contrary to the Subscribing Agency or Cogito PKIaaS policies.

The acceptance of a certificate by a Relying Party for a prohibited purpose is at the Relying Party's risk. Engaging in a prohibited certificate use is a breach of the responsibilities and obligations agreed to by the Subscriber and Subscribing Agency; and the Cogito PKIaaS 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 CP 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

See CPS.

2.3 Time or Frequency of publication

See Section 4.9.7for CRL issuance frequency. For further information, see CPS.

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. Will have as an alternative name in the subjectAltName field the Subscriber's organisation email address, as well as the Microsoft Unique Principal Name (UPN); and

iii. Must have common name components of the name, for both the subjectName and subjectAltName that are unique to the individual within the organisation name space.

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

To achieve a unique DN the Common Name (CN) component is based on the Subscriber's organisation email address.

3.1.2 Need for Names to be Meaningful

Names used to identify the Subscriber are to be based on the Subscriber's organisation email address and:

i. Relate to identity of the Subscriber as provided by the Directory entry;

ii. Must not identify the Subscriber by role or position; and

iii. Evidence of Identity (EOI) information verifying the identity of the Subscriber must relate to the Subscriber's Directory entry.

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 Subscriber agency's name space. Names used in certificates are unique to the individual and valid for that individual irrespective of their affiliation or relative location to, or within the organisation.

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

The creation of a network account initiates the certificate issuance.

A soft token containing the key pair is generated for the individual on the workstation the first time the user logs in to their account. To prove possession of the private key, a digitally-signed certificate request is submitted to the RA. The submission is made using the credentials supporting access to the individuals account within the Subscribing Agency's information environment.

3.2.2 Authentication of organisation entity

To be identified as affiliated with the Subscribing Agency or the Cogito PKIaaS the Subscriber must be identified by their organisation.

3.2.3 Authentication of individual identity

Prior to certificate issuance the individual's identity is authenticated by the following processes:

i. The Subscriber undergoes the organisations process to obtain access to the organisations network. This process validates the Subscriber's identity;

ii. The Subscriber's identity is re-validated as part of the process to issue a facility access card (positive face-to-face identification using a government issued token with photograph);

iii. Depending on the Subscriber's role within the organisation, the Subscriber is:

   a. Registered within the Personnel Management system for that organisations employees; or

   b. Registered within the organisations system for managing contractors.

iv. To obtain a network account, the Subscriber's sponsor validates the Subscriber's security clearance (if applicable), positively identifies the applicant (Drivers Licence, Passport, etc), confirms the Directory entry and submits a network access request.

The Directory is used as the authoritative source when creating a user's account within the organisation.

3.2.4 Non-Verified Subscriber information

All Subscriber information included in the certificate request is verified by the Subscriber Agency.

3.2.5 Validation of authority

Applicants must have an account within the subscriber organisation information environment, thus the affiliation with the organisation is validated.

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

No additional identification is required for routine re-key. Authentication to the network automatically generates a routine re-key, where applicable.

3.3.2 Identification and authentication for re-key after revocation

See Section 3.2.2.

3.4 Identification and authentication for revocation requests

Certificates issued through auto-enrolment are normally not revoked; if there is a need to revoke because of actual or suspected compromise, the account will be disabled or disconnected. If a Subscriber knows or suspects that their Windows login has been compromised, they must contact network support immediately. Identification for such a support call follows normal organisation procedures.

See Section 4.9 in this CP and the CPS for more information on revocation.

4 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Any individual who has an approved affiliation with the Cogito PKIaaS or a Subscribing Agency, and who has been assigned a user account in a subscriber organisation information environment is eligible for a certificate.

4.1.2 Enrolment process and responsibilities

Once the process described in Section 3.2.3 has been completed and an applicant has been granted a network user account, the act of the applicant logging on for the first time initiates the certificate application process. This process is automated, using Windows' auto-enrol feature integrated with the Cogito PKIaaS.

The Subscribing Agency's processes and procedures are responsible for submitting the request for a network account and must validate the applicant's identity against their record in the Directory and ensure they have the clearances and approvals sufficient for the network account requested.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

See Section 3.2.3.

4.2.2 Approval or rejection of certificate applications

An RO may reject or approve a certificate application. Reasons for rejection may include invalid application, insufficient affiliation with the Cogito PKIaaS or subscriber organisation, or the provision of incorrect or insufficient identification details.

4.2.3 Time to process certificate applications

No Stipulation.

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

The auto-enrolment process returns the certificate directly to the Subscriber's certificate store within the specific network that the Subscriber is connected to. There is no other notification.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

The Subscriber is deemed to have accepted the certificate when they have exercised the private key.

4.4.2 Publication of the certificate by the CA

See 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

Subscriber private key and certificate usage is defined above in Section 1.4. Subscriber responsibilities are described below in Section 9.6.

If the extended key usage extension is present and implies any limitation on the use of the certificate and/or private key, the Subscriber must operate within those limitations.

4.5.2 Relying Party public key and certificate usage

Section 1.4and Section 1.3.4detail the Relying Party's 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

4.6.1 Circumstance for certificate renewal

This CP permits certificate renewal. The criteria for certificate renewal are defined in the CPS.

4.6.2 Who may request renewal

See Section 4.1.1.

4.6.3 Processing certificate renewal requests

The process for certificate renewal is consistent with the enrolment process defined in Section 4.1(Certificate Application). The identification and authentication procedures must comply with Section 3.3.

4.6.4 Notification of new certificate issuance to Subscriber

See Section 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

See Section 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

See Section 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate Re-key

4.7.1 Circumstance for certificate re-key

This CP permits certificate re-key. See CPS for relevant circumstances.

4.7.2 Who may request certification of a new public key

Certificate re-key may be requested by the:

i. GRCG; or

ii. Subscriber.

4.7.3 Processing certificate re-keying requests

Processing of certificate re-key requests is consistent with the processing of new certificate requests, as detailed in Section **Error! Reference source not found.**. The identification and a uthentication requirements must comply with Section 3.3.

4.7.4 Notification of new certificate issuance to Subscriber

See Section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See Section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

See Section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

No Stipulation.

4.8 Certificate modification

This CP does not support certificate modification. If a certificate needs to be modified, it will be re-keyed.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

If a Subscriber's account has been compromised, or the identification of the Subscriber changes, they are obliged to report this to the relevant information environment support channel. The account itself will then be disabled or re-keyed, requiring the Subscriber to create a new password. Its Auto-enrol Certificate will not normally be revoked or suspended.

An Auto-enrol Resource Certificate may be revoked where an authorised revocation requestor (see CPS 4.9.2) considers it desirable to do so.

4.9.2 Who can request revocation

See CPS.

4.9.3 Procedure for revocation request

Where used, revocation requests received by PKI Operators are to be verified on receipt in accordance with Section 3.4(Identification and authentication for revocation request) and processed in priority order.

After verification the Registration Officer (RO) or PKI Operator processes revocation requests by 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

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 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.

Certificates issued under this CP are unsuitable for a Relying Party's use if the requirements for revocation checking conflict with the clauses in Section 4.9 of this CP.

4.9.7 CRL issuance frequency (if applicable)

Refer to the Issuing CA's CP for the CRL issuance frequency.

4.9.8 Maximum latency for CRLs

Refer to the Issuing CA's CP.

4.9.9 Online revocation/status checking availability

Online Certificate Status Protocol service (OCSP) is available at:

http://ocsp.gatekeeper.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 Section 2.1 and the certificates CRL Distribution Point (CDP) 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

4.10.1 Operational Characteristics

See CPS.

4.10.2 Service Availability

See CPS.

4.10.3 Optional Features

No Stipulation.

4.11 End of subscription

See CPS.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Escrow practices differ for the two types of private keys issued under this CP (see Section 1.1)

Escrow, backup and archiving of private authentication keys issued is not permitted under this CP. However, escrow and backup of private confidentiality keys is permitted.

The Authorised Key Retriever (AKR) must submit either a signed email or memorandum to an RO or PKI operator. The operator undertakes recovery of a private confidentiality key from escrow after validating the identity of the AKR and rationale for the recovery. After validation, the RO uses the approved software to implement the process, which will log the transaction.

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 Compromise and disaster recovery

See CPS.

5.7 CA or RA termination

See CPS.

6 Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Subscriber keys are generated in the operating system's cryptographic application programming interface (API) during the requesting process based on rules defined by the account creation policy.

6.1.2 Private key delivery to the subscriber

The key generation is performed on the Subscriber's workstation and stored directly in the Subscriber's operating system certificate store, so no delivery is required.

Private confidentiality keys, if issued, are always encrypted in transit.

6.1.3 Public key delivery to certificate issuer

The Subscriber's public key is provided to the CA in a PKCS#10 certificate request file signed with the corresponding private key.

6.1.4 Public key delivery to relying parties

See CPS.

6.1.5 Key Sizes

The key size for RSA is a minimum of 2048 bits.

The key size for ECC is a minimum of 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)

Subscriber key and certificate usage is defined above in Section 1.4.

Subscriber certificates include key usage extension fields to specify the purposes for which the keys may be used, and also to technically limit the functionality of the certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of the Cogito PKIaaS.

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

Subscriber keys are stored in the user account certificate store, protected by the Subscriber's user account password.

HSMs used with the PKI core components are on the Evaluated Products List (EPL).

6.2.2 Private key (n of m) control

See CPS.

6.2.3 Private key escrow

Escrow of private authentication keys does not occur; however, private confidentiality keys are subject to escrow. Refer to CPS for escrow controls.

6.2.4 Private key backup

See CPS.

6.2.5 Private key archive

See CPS.

6.2.6 Private key transfer into or from a cryptographic module

See CPS.

Private confidentiality keys, if issued, are escrowed, and will be stored in encrypted form in the key management archive. Private confidentiality keys are always transferred using the PKI software confidentiality key(s).

6.2.7 Private key storage on cryptographic module

See CPS.

6.2.8 Method of activating private key

To activate key usage, the Subscriber must authenticate into their organisation information environment account, which gives the Subscriber access to the token associated with the Subscriber's key pair.

6.2.9 Method of deactivating private key

The Subscriber's private key will be deactivated when they log out of the network account to which the certificate has been issued.

6.2.10 Method of destroying private keys

See CPS.

6.2.11 Cryptographic module rating

See Section 6.2.1 of this CP.

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 Subscriber certificate has a maximum validity period of 2 years to limit the key lifetime. For further information, see CPS.

6.4 Activation Data

6.4.1 Activation data generation and installation

No stipulation.

6.4.2 Activation data protection

All passphrases used to activate the private key shall be kept in accordance with Subscribing Agency policy.

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 only certificates issued under this CP are:

i. Identity Signature/Authentication Certificate; and

ii. Identity Encryption/Confidentiality Certificate.

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 information, such as OCSP responses.

7.1.4 Name forms

The Common Name (CN) component is based, where possible, on the Subscriber's agency's email address and/or be unique in the subscriber organisation. It is encoded as an X.501 printable string where possible and using UTF-8 otherwise.

7.1.5 Name constraints

Name constraints are not present.

7.1.6 Certificate policy object identifier

Certificates issued under this CP shall assert this CPs OID { 1.2.36.151795998.4.1.1.2.1 }

Certificates issued under this policy shall assert the following LoA OIDs for the LoA under which it was 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

See also Appendix B.

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 CP 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 issued shall be X.509 Version 2 CRLs.

7.2.2 CRL and CRL entry extensions

See Issuing CA CP.

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.gatekeeper.securesme.com/

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”.

X.509 Certificate Policy (CP)

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.

X.509 Certificate Policy (CP)

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 Profiles

B.1 Individual – Software (Medium Assurance) Certificate - Authentication (RSA)

Field	Critical	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 36 months from date of issue.
Subject Distinguished Name		CN= <unique identifier> OU= <Subscriber OU> OU= PKI O= <Subscriber> C= AU	Note: Example only, actual naming will reflect the subscriber organisation. CN must be unique within the subscribing organisations namespace.

X.509 Certificate Policy (CP)

Field	Critical	Value	Notes
			An example would be the use of the left-hand side of the Subject's organisational email address, e.g. "Jan.Smith7" for a subject with the principal email address "Jan.smith7@someagency.com". Encoded as printable string where possible, and otherwise using UTF-8.
Subject Public Key Information		Minimum 2048-bit RSA key modulus, rsaEncryption	
Issuer Unique Identifier		Not Present	
Subject Unique Identifier		Not Present	
Issuers Signature		SHA256WithRSAEncryption	
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	
Extended key usage		{1.3.6.1.5.5.7.3.2} Microsoft Client Authentication {1.3.6.1.5.5.7.3.4} Secure email protection	

X.509 Certificate Policy (CP)

Field	Critical	Value	Notes
Private key usage period		Not Present	
Certificate policies	No	[1] Policy OID: { 1.2.36.151795998.4.1.1.3 } Policy Qualifier - CPS pointer: http://pki.gatekeeper.securesme.com/	The OID of this CP.
		[2] Policy OID: {1.2.36.151795998.4.1.2.1.2}	Level of Assurance – Medium (Individual). The Level of Assurance of this certificate.
		[3] Policy OID: {1.2.36.151795998.4.1.2.1.1}	Level of Assurance – Low (Individual). Included to allow the certificate to be used in lower assurance context.
Policy Mapping		Not Present	
Subject Alternative Name		RFC822 Name (email address) Other Name: Principal Name	
Issuer Alternative Name		Not Present	
Subject Directory Attributes		Not Present	
Basic Constraints		Not Present	
Name Constraints		Not Present	

X.509 Certificate Policy (CP)

Field	Critical	Value	Notes
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 [3] Access method: OCSP {1.3.6.1.5.5.7.48.1} Access location: http://ocsp.<Subscriber>.securesme.com/	
CRL Distribution Points	No	[1] Distribution Point Name (http): 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 reasons and cRLIssuer fields shall not 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 3: Individual – Software (Medium Assurance) Certificate - Authentication (RSA) Profile

B.2 Individual - Software (Medium Assurance) Certificate - Authentication (ECC)

Field	Critical	Value	Notes
Version		V3 (2)	Version 3 of X.509.
Serial		<octet string>	Must be unique within the PKIaaS namespace.
Issuer Signature Algorithm		ecdsa-with-SHA384	
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 36 months from date of issue.
Subject Distinguished Name		CN= <unique identifier> OU= <Subscriber OU> OU= PKI O= <Subscriber> C= AU	Note: Example only, actual naming will reflect the subscriber organisation. CN must be unique within the subscribing organisations namespace. An example would be the use of the left-hand side of the Subject’s organisational email address, e.g. “Jan.Smith7” for a subject with the principal email address “Jan.smith7@someagency.com”.

X.509 Certificate Policy (CP)

Field	Critical	Value	Notes
			Encoded as printable string where possible, and otherwise using UTF-8.
Subject Public Key Information		ecdsa-with-SHA384	
Issuer Unique Identifier		Not Present	
Subject Unique Identifier		Not Present	
Issuers Signature		ecdsa-with-SHA384	
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	
Extended key usage		{1.3.6.1.5.5.7.3.2} Microsoft Client Authentication {1.3.6.1.5.5.7.3.4} Secure email protection	
Private key usage period		Not Present	
Certificate policies	No	[1] Policy OID: { 1.2.36.151795998.4.1.1.3 }	The OID of this CP.

X.509 Certificate Policy (CP)

Field	Critical	Value	Notes
		Policy Qualifier - CPS pointer: http://pki.gatekeeper.securesme.com/	
		[2] Policy OID: {1.2.36.151795998.4.1.2.1.2}	Level of Assurance – Medium (Individual). The Level of Assurance of this certificate.
		[3] Policy OID: {1.2.36.151795998.4.1.2.1.1}	Level of Assurance – Low (Individual). Included to allow the certificate to be used in lower assurance context.
Policy Mapping		Not Present	
Subject Alternative Name		RFC822 Name (email address) Other Name: Principal Name	
Issuer Alternative Name		Not Present	
Subject Directory Attributes		Not Present	
Basic Constraints		Not Present	
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}	

Field	Critical	Value	Notes
		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.gatekeeper.securesme.com/	
CRL Distribution Points	No	[1] Distribution Point Name (http): 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 reasons and cRLIssuer fields shall not 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 4: Individual - Software (Medium Assurance) Certificate - Authentication (ECC) Profile

B.3 Individual – Software (Medium Assurance) Certificate - Confidentiality (RSA)

Field	Critical	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 36 months from date of issue.
Subject Distinguished Name		CN= <unique identifier> OU= <Subscriber OU> OU= PKI O= <Subscriber> C= AU	Note: Example only, actual naming will reflect the subscriber organisation. CN must be unique within the subscribing organisations namespace. An example would be the use of the left-hand side of the Subject’s organisational email address, e.g. “Jan.Smith7” for a subject with the principal email address “Jan.smith7@someagency.com”.

X.509 Certificate Policy (CP)

Field	Critical	Value	Notes
			Encoded as printable string where possible, and otherwise using UTF-8.
Subject Public Key Information		Minimum 2048-bit RSA key modulus, rsaEncryption	
Issuer Unique Identifier		Not Present	
Subject Unique Identifier		Not Present	
Issuers Signature		SHA256WithRSAEncryption	
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	keyEncipherment dataEncipherment	
Extended key usage		{1.3.6.1.5.5.7.3.4} Secure email protection	
Private key usage period		Not Present	
Certificate policies	No	[1] Policy OID: { 1.2.36.151795998.4.1.1.3 }	The OID of this CP.

X.509 Certificate Policy (CP)

Field	Critical	Value	Notes
		Policy Qualifier - CPS pointer: http://pki.gatekeeper.securesme.com/	
		[2] Policy OID: {1.2.36.151795998.4.1.2.1.2}	Level of Assurance – Medium (Individual). The Level of Assurance of this certificate.
		[3] Policy OID: {1.2.36.151795998.4.1.2.1.1}	Level of Assurance – Low (Individual). Included to allow the certificate to be used in lower assurance context.
Policy Mapping		Not Present	
Subject Alternative Name		RFC822 Name (email address) Other Name: Principal Name	
Issuer Alternative Name		Not Present	
Subject Directory Attributes		Not Present	
Basic Constraints		Not Present	
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}	

Field	Critical	Value	Notes
		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	[1] Distribution Point Name (http): http://crl.<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 reasons and cRLIssuer fields shall not 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: Individual – Software (Medium Assurance) Certificate - Confidentiality (RSA) Profile

B.4 Individual - Software (Medium Assurance) Certificate - Confidentiality (ECC)

Field	Critical	Value	Notes
Version		V3 (2)	Version 3 of X.509.
Serial		<octet string>	Must be unique within the PKIaaS namespace.
Issuer Signature Algorithm		ecdsa-with-SHA384	
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 36 months from date of issue.
Subject Distinguished Name		CN= <unique identifier> OU= <Subscriber OU> OU= PKI O= <Subscriber> C= AU	Note: Example only, actual naming will reflect the subscriber organisation. CN must be unique within the subscribing organisations namespace. An example would be the use of the left-hand side of the Subject’s organisational email address, e.g. “Jan.Smith7” for a subject with the principal email address “Jan.smith7@someagency.com”.

X.509 Certificate Policy (CP)

Field	Critical	Value	Notes
			Encoded as printable string where possible, and otherwise using UTF-8.
Subject Public Key Information		ecdsa-with-SHA384	
Issuer Unique Identifier		Not Present	
Subject Unique Identifier		Not Present	
Issuers Signature		ecdsa-with-SHA384	
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	keyEncipherment dataEncipherment	
Extended key usage		{1.3.6.1.5.5.7.3.4} Secure email protection	
Private key usage period		Not Present	
Certificate policies	No	[1] Policy OID: { 1.2.36.151795998.4.1.1.3 }	The OID of this CP.

X.509 Certificate Policy (CP)

Field	Critical	Value	Notes
		Policy Qualifier - CPS pointer: http://pki.gatekeeper.securesme.com/	
		[2] Policy OID: {1.2.36.151795998.4.1.2.1.2}	Level of Assurance – Medium (Individual). The Level of Assurance of this certificate.
		[3] Policy OID: {1.2.36.151795998.4.1.2.1.1}	Level of Assurance – Low (Individual). Included to allow the certificate to be used in lower assurance context.
Policy Mapping		Not Present	
Subject Alternative Name		RFC822 Name (email address) Other Name: Principal Name	
Issuer Alternative Name		Not Present	
Subject Directory Attributes		Not Present	
Basic Constraints		Not Present	
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}	

Field	Critical	Value	Notes
		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	[1] Distribution Point Name (http): 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 reasons and cRLIssuer fields shall not 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 6: Individual – Software (Medium Assurance) Certificate - Confidentiality (ECC) Profile