

Secure Electronic Environment Project



S.E.E. PKI

Paper 12 – Certificate Types

Version 1.0

1	Introduction	2
2	Recommendations	2
3	Certificate uses	2
4	Certificate types	3
4.2	Qualifier meanings	3
4.3	Alignment with S.E.E. PKI	4
5	Implementation	5
5.1	Usage of the Policy OID	5
5.2	Usage of the O= field	5
5.3	Usage of the OU= field	5
5.4	Usage of the CN= field	6
5.5	Usage of the S= field	8
5.6	Control of the DN= structure	8

Franz Ombler – The Treasury
Mike Pearson – State Services Commission

1 Introduction

1.1.1 The S.E.E. PKI group has been asked to consider additional certificate types that did not appear to align with the S.E.E. PKI Certificate Policy. Meeting these additional requirements could mean minimising costs, establishing critical mass, and aligning with emerging de facto standards. The recommendations and findings are detailed below.

2 Recommendations

2.1.1 We recommend:

- Creating a unique policy OID for each certificate, in anticipation of being able to filter on policy extension in the future.
- Using the OU= field to provide additional information.
- Amending the S.E.E. PKI Certificate Policy to use the CN= field to differentiate certificate types, using the generic format “**CN = Commonname [SEEKEY name]**”
- Creating and maintaining a SEEKEY Name list to be used to indicate certificate type.
- For anonymous certificates, either “**O= - and CN=ANONYMOUS arbitraryString**”, or “**O=orgname and CN=ANONYMOUS arbitraryString**”.
- The Certificate Policy be amended: Where ‘hardened softkeys’ are available, they should be used in preference to normal softkeys.
- When choosing whether to include ENCRYPT capability for end-user certificates, sponsors should consider whether they want their users to be able to receive and store encrypted data, and the information management issues surrounding long term storage and retrieval of encrypted information.
- All S.E.E. Key certificates must have a policy extension for the Policy OID of the certificate type (e.g. 2.16.554.101.2.1.1.6), including a userNotice of the certificate type as it appears in the CN (e.g. [SEEKEY ASSOCIATE-ROLE]), and a cpsUri of <http://see.govt.nz/pki/cp.html#> suffixed with the certificate type (e.g. <http://see.govt.nz/pki/cp.html#associate-role>).

3 Certificate uses

3.1.1 There are two major uses of certificates: identity and access.

3.1.2 **Identity** certificates, have several sub-uses, which provide proof of identity for:

- Individual (person)
- Device (machine)
- Role (person(s) in a role)
- Membership (person has eligibility)
- Proxy (machine acting for a person)

- 3.1.3 The concept of Organisation can be covered by Role e.g. a role of “Common Seal of the Company” represents an organisation.
- 3.1.4 The concept of Delegation can be covered by Role. For instance, a PA has the delegated authority to act on behalf of the CEO in certain areas. The PA would have the role of “PA to the CEO”. The PA may sign on behalf of the CEO – typically there are other checks and balances to manage issues such as misrepresentation.
- 3.1.5 A membership certificate is used to demonstrate registration, membership, certification or similar capability.
- 3.1.6 **Access** certificates act similar to a physical key. They also have several sub-types
- Access to a resource
 - Anonymous access
- 3.1.7 Possession of an “access to a resource” certificate, acts like a physical key, the user can access a resource, such as an encrypted laptop.
- 3.1.8 An “anonymous access” certificate is similar to “access to a resource”, but has little or no identifying information – the equivalent of an unlabelled key – it provides access, but anyone finding it, must know where to present it, to be given access.

4 Certificate types

- 4.1.1 Certificate types are characterised by combining a specific but extensible set of qualifiers:
- Certificate class, (cQUALIFIER): PASSPORT or BUSINESS CARD or ASSOCIATE or ANONYMOUS
 - Certificate storage (sQUALIFIER): SMART-TOKEN, PROXY
 - Certificate purpose (pQUALIFIER): ACCESS or (ID, [SIGN,] ENCRYPT)
- 4.1.2 Certificates are typically used for ACCESS or ID. An ID certificate may also include SIGN and/or ENCRYPT functionality.
- 4.1.3 Note that in the context of this document, the term *Certificate types* is used to differentiate among certificate used for slightly different purposes and which have different rules around their use, issuing and reliance; they are thus formally different certificate policies and will have different Policy OIDs, but will be governed by the same Certificate Policy.

4.2 Qualifier meanings

- 4.2.1 PASSPORT: As per current Certificate Policy. Individual is identified using Gatekeeper 100 point system and certificate is not tied to a particular organisation – The DN O field is left blank.
- 4.2.2 BUSINESS-CARD: As per current Certificate Policy. The DN O field is populated with the organisation of the individual, the user is identified in the

CN Field by the name they are known to the organisation. Certificate request has been approved by a Sponsor delegated from CE of organisation. Email address can only be issued if domain name in control of organisation. Used to show that the individual represents the organisation – as if they were presenting a business card.

- 4.2.3 ASSOCIATE: As per current Certificate Policy. The O field must include the name of the organisation but may be different, e.g. *Associate of The Treasury*. Use of organisation name in O controlled as per BUSINESS-CARD. The OU will typically contain a disclaimer to differentiate it significantly from a BUSINESS-CARD style certificate. Typically used when an organisation wishes to control issuing of certificates to those outside the organisation interacting with it.
- 4.2.4 ANONYMOUS: A certificate that does not identify its use, e.g. with just a number in the CN field. If a private key is lost together with its certificate, the details of the certificate will give no clue to what it may unlock. May optionally include the organisation name.
- 4.2.5 SMART-TOKEN: The private key associated with the certificate is stored in a non-exportable form on a hardware token as per Certificate Policy.
- 4.2.6 PROXY: The private key is stored on a gateway server acting on behalf of the individual, e.g. email gateway signing or proxy authentication to a server.
- 4.2.7 ACCESS: Grants access to a resource. For example to a particular web based application, or to a laptop.
- 4.2.8 ID: Specifies that the certificate is intended to be used for identifying the user, for example for authentication to a web based application. The “digital signature” key usage flag should be set.
- 4.2.9 SIGN: Specifies that the certificate is intended to be used for digitally signing information for long term verification, for example a digitally signed email message or document. The “non-repudiation” key usage flag should be set.
- 4.2.10 ENCRYPT: Specifies that the certificate is intended for use in encrypting information for the certificate owner. The “key encipherment” key usage flag should be set.

4.3 Alignment with S.E.E. PKI

- 4.3.1 For the purposes of the S.E.E. PKI, Passport, Business Card or Associate certificates are the same as the first three Certificate types (see Implementation below).
- 4.3.2 Proxy and Access certificate types typically trade-off reduced trust in identity, for greater flexibility in meeting business needs, for reasons such as automatic on-the-fly certificate generation (proxy e-mail) or wide shared distribution (access to corporate laptops).
- 4.3.3 Therefore, only Associate certificates are suitable for Proxy and Access uses. To ensure stronger Access security, an Associate private key may be put on a hardware based token.

5 Implementation

5.1 Usage of the Policy OID

- 5.1.1 X.509v3 says applications should be able to filter certificates based on the contents of the policy extension. Section 4.2.1.5 of <http://www.ietf.org/rfc/rfc2459.txt> says:

Applications with specific policy requirements are expected to have a list of those policies which they will accept and to compare the policy OIDs in the certificate to that list. If this extension is critical, the path validation software MUST be able to interpret this extension (including the optional qualifier), or MUST reject the certificate.

- 5.1.2 Paper 4 stated this wouldn't currently work with Commercial-Off-The-Shelf software and our communications to major vendors showed that it would be a custom development for each platform. We feel the field should still be used, in anticipation of being able to filter on policy extension in the future.
- 5.1.3 Recommendation: Certificate policy amendment – Each certificate MUST have a unique policy OID for each certificate.
- 5.1.4 Recommendation: Certificate policy amendment - All S.E.E. Key certificates MUST have a policy extension for the Policy OID of the certificate type (e.g. 2.16.554.101.2.1.1.6), including a userNotice of the certificate type as it appears in the CN (e.g. [SEEKEY ASSOCIATE-ROLE], and a cpsUri of <http://see.govt.nz/pki/cp.html#> suffixed with the certificate type (e.g. <http://see.govt.nz/pki/cp.html#associate-role>).
- 5.1.5 In the interim, we have considered what other fields can be used for our purposes. The other available fields are O, OU, CN.

5.2 Usage of the O= field

- 5.2.1 The O= field was discounted, as it is likely to be used specifically for organisational name, by many CAs.
- 5.2.2 We note that the value in the O= field of many certificates is not user-friendly.
- 5.2.3 Recommendation: Certificate policy amendment - The O= field SHOULD reflect the proper relevant legal name of the organisation name e.g. O=Ministry of Water, not O=minwtr.govt.nz.

5.3 Usage of the OU= field

- 5.3.1 The OU field was discounted, as it can have multiple instances in a certificate, causing problems for applications trying to parse them. However it is useful for adding additional notes, such as a liability disclaimer.
- 5.3.2 Recommendation: Certificate policy amendment – The OU= field SHOULD be used to provide additional information, such as liability disclaimers.

5.4 Usage of the CN= field

- 5.4.1 The CN field was considered to have the greatest potential, as CAs typically place few controls over what can be placed in the field. A secondary advantage is that the CN field is typically displayed when a user has to choose between two or more certificates, thereby providing more information for them.
- 5.4.2 **Recommendation:** Certificate policy amendment - The CN= field MUST be used to differentiate certificate types, using the generic format “**CN = Commonname [SEEKEY name]**”.
- 5.4.3 In the Qualifiers column below, square brackets indicate an optional qualifier. In the CN, square brackets are required characters which permit precise filtering.

SEEKEY Name	Qualifiers / Policy OID	CN Example
Personal certificate. MUST be on a hardware token. Typically ID. Optionally SIGN. Optionally ENCRYPT.		
PASSPORT	PASSPORT, SMART-TOKEN, ID, [SIGN,] [ENCRYPT] 2.16.554.101.2.1.1.1	O= CN=Joe Bloggs [SEEKEY PASSPORT] E=joe.bloggs@ssc.govt.nz
Employer issued certificate. MUST be on a hardware token. Typically ID. Optionally SIGN. Optionally ENCRYPT.		
BUSINESS-CARD	BUSINESS CARD, SMART-TOKEN, ID, [SIGN,] [ENCRYPT] 2.16.554.101.2.1.1.2	O=State Services Commission CN=Joe Bloggs [SEEKEY BUSINESS-CARD] E=joe.bloggs@ssc.govt.nz
Organisation issued associate certificate. OPTIONAL hardware token. Typically ID. Optionally SIGN. Optionally ENCRYPT. SHOULD have an OU= liability statement.		
ASSOCIATE	ASSOCIATE, ID, [SIGN,] [ENCRYPT] 2.16.554.101.2.1.1.3	O= State Services Commission OU= For internal use only. We disclaim any liability from third parties accepting this certificate for their own purposes. CN=Mary Smith [SEEKEY ASSOCIATE] E=mary.smith@someplace.co.nz
Device certificate. OPTIONAL hardware token. Typically ID and ENCRYPT, optionally SIGN. NB: Web server certificates cannot use the CN qualifiers as common practice is for the DNS name to match the CN		
DEVICE	PASSPORT, ID, ENCRYPT or BUSINESS CARD, ID, ENCRYPT or ASSOCIATE, ID, ENCRYPT 2.16.554.101.2.1.1.4	O=State Services Commission CN=webserver.ssc.govt.nz E=webmaster@ssc.govt.nz
Employer issued role certificate. MUST be on a hardware token. Typically ID. Optionally SIGN. Optionally ENCRYPT. MUST be issued on a limited basis, to a group of users. SHOULD have a unique number for each token. SHOULD have a register showing user / token unique number. TOKEN may be shared among group of users.		
BUSINESS-ROLE	BUSINESS CARD, SMART-TOKEN, ID, [SIGN,] [ENCRYPT] 2.16.554.101.2.1.1.5	O=State Services Commission CN=Helpdesk [SEEKEY BUSINESS-ROLE] E=helpdesk@ssc.govt.nz
Organisation issued role certificate. MUST be on a hardware token. Typically ID. Optionally SIGN. Optionally ENCRYPT. MUST be issued on a limited basis, to a group of users. SHOULD have a unique number for each token. SHOULD have a register showing user / token unique number. SHOULD have an OU= liability statement.		

SEEKEY Name	Qualifiers / Policy OID	CN Example
ASSOCIATE-ROLE	ASSOCIATE, SMART-TOKEN, ID, [SIGN,] [ENCRYPT] 2.16.554.101.2.1.1.6	O=State Services Commission OU= For internal use only. We disclaim any liability from third parties accepting this certificate for their own purposes. CN=Helpdesk [SEEKEY ASSOCIATE-ROLE] E=helpdesk@someplace.co.nz
Membership certificate. Organisational name must match authority that approves membership. OPTIONAL hardware token. ID only. NO SIGN or ENCRYPT. MAY have duplicates. MUST be issued on a limited basis, to a group of users. MUST have a unique number for each token. MUST have a register showing user / token unique number. SHOULD have an OU= liability statement. Different types of membership can be achieved by adding a 3 rd part to the name.		
MEMBERSHIP-GOVIS-ASSOCIATE	PASSPORT, ID or BUSINESS CARD, ID or ASSOCIATE, ID 2.16.554.101.2.1.1.7	O= GOVIS OU= GOVIS warrants this certificate for the purposes of membership only CN=Joe Bloggs [SEEKEY MEMBERSHIP-GOVIS-ASSOCIATE]
MEMBERSHIP-GOVIS-FELLOW	PASSPORT, ID or BUSINESS CARD, ID or ASSOCIATE, ID 2.16.554.101.2.1.1.8	O= GOVIS OU= GOVIS warrants this certificate for the purposes of membership only CN=Joe Bloggs [SEEKEY MEMBERSHIP-GOVIS-FELLOW]
Organisation signing on behalf of an individual. OPTIONAL hardware token. Typically ID, SIGN, ENCRYPT. Typically used by mail gateways, to generate a certificate on the fly, for an individual, to sign an outgoing e-mail. This allows s/mime to individual e-mail clients to work without generating an error message. SHOULD have an OU= liability statement.		
PROXY	PASSPORT, PROXY, SIGN, ENCRYPT or BUSINESS CARD, PROXY, SIGN, ENCRYPT 2.16.554.101.2.1.1.9	O= State Services Commission OU= Proxy certificate used by mail server CN=Joe Bloggs [SEEKEY PROXY] E= joe.bloggs@ssc.govt.nz
Organisation access to a protected resource e.g. part of web server, through a proxy mechanism. Organisation confirms user identity through minimum of username/password. Organisation assigns unique username/password to each individual. NO ID, SIGN or ENCRYPT. SHOULD have an OU= liability statement.		
PROXY-ACCESS	BUSINESS CARD, PROXY, ACCESS 2.16.554.101.2.1.1.10	O= State Services Commission OU= Proxy certificate used by web server CN=Joe Bloggs [SEEKEY PROXY-ACCESS] E=joe.bloggs@ssc.govt.nz
General purpose certificate. MUST be on a hardware token. NO ID, SIGN or ENCRYPT. MAY have duplicates. SHOULD have an OU= liability statement.		
ACCESS-CARD	BUSINESS CARD, SMART-TOKEN, ACCESS or ASSOCIATE, SMART-TOKEN, ACCESS 2.16.554.101.2.1.1.11	O= State Services Commission OU= No validity for signing CN=Laptop [SEEKEY ACCESS-CARD]
General purpose certificate. MUST be on a hardware token. NO ID, SIGN or ENCRYPT. MAY have duplicates. SHOULD have an OU= liability statement.		
ANON-ACCESS-CARD	ANONYMOUS, SMART-TOKEN, ACCESS 2.16.554.101.2.1.1.12	O= - OU=No validity for signing CN=12345678 [SEEKEY ANON-ACCESS-CARD]

5.4.29 **Recommendation:** We recommend creating and maintaining a SEEKEY Name list to be used to indicate certificate type.

- 5.4.30 Other organisations can use other CN= labels, but CA must ensure they do not conflict with the SEEKEY Names.
- 5.4.31 CA processes must be such that the existence of the keyword SEEKEY in the CN can be relied upon to be confident that the certificate was issued under the S.E.E. Key Certificate Policy. Note this give the CA flexibility to produce other non-S.E.E. Key certificates using the same CA.
- 5.4.32 Access certificates may need to be anonymous (i.e. if you lose it, no-one else will know what it can be used for).
- 5.4.33 Recommendation: Certificate policy amendment - For anonymous certificates, we recommend either “**O=** - and **CN=ANONYMOUS arbitraryString**”, or “**O=orgname** and **CN=ANONYMOUS arbitraryString**”.
- 5.4.34 Recommendation: Certificate policy amendment - When choosing whether to include ENCRYPT capability for end-user certificates, sponsors should consider whether they want their users to be able to receive and store encrypted data, and the information management issues surrounding long term storage and retrieval of encrypted information.

5.5 Usage of the S= field

- 5.5.1 The original recommendation for the S= field was to set it to “-“. It was felt that applications would require a value in the field.

5.6 Control of the DN= structure

- 5.6.1 Based upon feedback from other agencies, it is apparent that organisations should have overall say of the DN structure used in their certificates. This is particularly important when they choose to swap CAs, as an imposed DN structure could mean the re-issuing of all certificates.
- 5.6.2 Recommendation: Guidelines for Agencies Choosing a CA – The organisation should determine the structure of the DN.
- 5.6.3 Recommendation: Certificate policy amendment - The organisation should determine the value of the S= field.
- 5.6.4 Recommendation: Certificate policy amendment - S.E.E. PKI applications should not require the presence or otherwise of the S= field in the DN.