



Australian Government

National Office for the Information Economy

Australian Business Number Digital Signature Certificate (ABN-DSC)

Broad Specification

Version 3.6

September 2003

This work is copyright. The Commonwealth grants a royalty-free, irrevocable, world-wide, perpetual, non-exclusive licence, including the right to sub-licence, to reproduce this work for the purpose of gaining accreditation under the Gatekeeper strategy. Apart from this purpose and any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without the prior written permission from the National Office for the Information Economy. Requests and enquires concerning reproduction rights should be addressed to:

*Manager
Government Authentication
Information Framework
National Office for the Information Economy
GPO Box 390
Canberra ACT 2601*

Contents

1	INTRODUCTION.....	5
1.1	THE AUSTRALIAN BUSINESS NUMBER (ABN).....	5
1.2	USE OF DIGITAL CERTIFICATES.....	5
1.3	USE OF DIGITAL CERTIFICATES BY THE ATO	6
1.4	THE ABN-DSC CONCEPT	6
1.5	THIS DOCUMENT	7
1.6	NON-REPUDIATION	8
2	WHAT IS THE ABN-DSC?	9
2.1	POLICY OBJECTIVE	9
2.2	POLICY SPECIFICATION.....	9
3	THE ABN-DSC AND GATEKEEPER.....	11
4	USE OF THE ABN-DSC.....	12
4.1	HOW AND WHEN MAY IT BE USED?.....	12
4.2	WHAT TRANSACTIONS MAY IT BE USED FOR?	12
4.3	WHICH ORGANISATIONS SHOULD USE IT?.....	13
4.4	FINANCIAL LIMITATIONS.....	13
4.5	CONFIDENTIALITY LIMITATIONS.....	14
5	ISSUING THE ABN-DSC.....	15
5.1	TO WHOM MAY THE ABN-DSC BE ISSUED?	15
5.2	MANAGEMENT OF CERTIFICATES BY BUSINESS ENTITIES.....	16
5.3	USE OF THE ABN-DSC WITH THE ATO	16
5.4	HOW MIGHT THE ABN-DSC BE ISSUED?.....	16
6	THE ABN-DSC CERTIFICATE POLICY AND PROFILE.....	18
6.1	GATEKEEPER MODEL CERTIFICATE POLICY AND CERTIFICATE PROFILE	18
6.2	ABN-DSC CERTIFICATE POLICY	18
6.3	ABN-DSC CERTIFICATE PROFILE.....	18
6.4	CONSTRUCTION OF THE DISTINGUISHED NAME IN AN ABN-DSC.....	20
6.4.1	Examples.....	23
6.5	INCLUSION OF THE ABN.....	23
7	REGISTRATION REQUIREMENTS	24
7.1	INTRODUCTION.....	24
7.2	AIM.....	24
7.3	THE AUTHORISED OFFICER	25
7.4	REGISTRATION PROCESSES.....	26
7.5	LEGAL OR REGULATORY DOCUMENTS.....	27
7.6	INDICATIVE PROCEDURE	27
7.7	ADDITIONAL CERTIFICATES.....	29
8	FEES	30
9	PRIVACY.....	31
10	CERTIFICATE REVOCATION.....	32
10.1	CIRCUMSTANCES FOR REVOCATION.....	32
10.2	WHO CAN REQUEST REVOCATION	32
10.3	REVOCATION PROCESS.....	33
10.4	CERTIFICATE SUSPENSION	33

10.5 CERTIFICATE RENEWAL33

11 RECORD ARCHIVAL.....35

12 OPERATION OF DIRECTORIES36

13 INTEROPERABILITY.....37

14 LIABILITY.....38

ATTACHMENT A - GLOSSARY.....39

1 INTRODUCTION

The Government has sought to use its position as a leading edge user of information technology and telecommunications systems to support the take-up of online technologies across the Australian economy.

The Government has addressed specific impediments to broader Internet use by measures such as:

- the *Electronic Transaction Act 1999 (Cth)* which recognises the validity of online transactions; and
- the implementation of the *Gatekeeper* strategy to ensure a whole-of-government framework to facilitate authentication, non-repudiation, confidentiality and integrity for online transactions.

1.1 The Australian Business Number (ABN)

The introduction of tax reform has provided an opportunity for further enabling e-commerce, chiefly through the use of a national unique business identifier, the Australian Business Number (ABN). The ABN, is a single identifier for all business dealings with the Australian Taxation Office (ATO) and for future dealings with other Agencies.

The introduction of the ABN addresses a number of deficiencies in previously used unique business identifiers; particularly the Australian Company Number (ACN). The ACN was issued only to bodies registered under the Corporations Law. The ABN is to be used by a much wider range of business entities, including sole traders.

The ABN is being issued to Business Entities, organisations and Agencies. The ABN is identified in *A New Tax System - Australian Business Number 1999 (Cth)* legislation as a mechanism that will allow Business Entities to identify themselves when dealing with Government. Government has required Agencies to standardise the use of the ABN to identify Australian businesses.

1.2 Use of digital certificates

The Commonwealth has a policy to support the widespread use of digital certificates within business and sees digital certificates supporting the use of the ABN as a universal business identifier. The Government sought to develop the Australian Business Number Digital Signature Certificate (ABN-DSC) as a digital certificate, built around the ABN, to identify Australian businesses online.

1.3 Use of digital certificates by the ATO

The Government was also keen to leverage off the use of digital certificates for the electronic lodgement of Business Activity Statements with the ATO to achieve a wider use of this technology across the Australian economy.

The ATO is a leader in the introduction of new IT&T technologies within Government. Its initial proposals for taxation reform included measures for electronic lodgement using the Internet. The use of digital certificates allows this to be done in a secure and trusted manner.

The ATO was aware of the Government's requirement for the delivery of services online by 2001, however implementation deadlines meant that the ATO had to implement a digital certificate before the development of the ABN-DSC was completed. ATO has implemented a closed digital certificate hierarchy that can be used only for specific transactions with the ATO. However, it is expected that the ABN-DSC will be accepted by the ATO as an alternative to the current ATO digital certificate from the second quarter of 2002.

The ATO system is one of the largest digital certificate implementations in the world. It is also a first for an implementation of this scale that involves so many external users. This is the first significant implementation of *Gatekeeper* digital certificates. The experience to date proves the viability of the ABN-DSC concept.

1.4 The ABN-DSC concept

The ABN-DSC is a class of digital certificates based around the ABN. It is intended that the ABN-DSC be used primarily for supporting business to Government online transactions. This will allow businesses to require only one online identity in all their dealings with Government agencies and reduce both costs, and inconvenience, to businesses and agencies.

The Commonwealth decisions in 1999 have required Agencies to use the ABN, the *Gatekeeper* strategy and the ABN-DSC.

- In July 1999, the Commonwealth government agreed that:
 - any future online authentication digital certificates issued by Agencies to Business Entities and individuals be *Gatekeeper* compliant; and
 - that Agencies will use only the ABN as the identifier of Business Entities.
- In December 1999, the Commonwealth government agreed that the Australian Business Number - Digital Signature Certificate (ABN-DSC) be issued for whole of Commonwealth government use to ensure that a single digital certificate can be used by a Business Entity in electronic transactions with Agencies.

In November 2000 the Ministerial meeting of the Online Council (Commonwealth, State and Territory Governments and the Australian Local Government Association) agreed in principle to the adoption of the *Gatekeeper* strategy and ABN-DSC, where appropriate, to support electronic transactions within their respective jurisdictions.

NOIE has been working since early 1999 to develop the ABN-DSC concept. This work led to the need for a detailed specification for a broad use digital certificate, based around the ABN, which can be used by all Agencies in their online dealings with Business Entities.

This work has largely been undertaken by government due to "perceived market failure". That is, a broad use digital certificate wasn't available for use by Agencies. The Government did not want to burden business with the need to obtain or use a variety of digital certificates from any number of Agencies wanting to undertake online transactions with clients.

However, the market has been changing and feedback received by NOIE from stakeholders has indicated the need to provide a level of flexibility in specifying the ABN-DSC broad use type of digital certificate.

On 19 March 2001, Cabinet agreed that the Project Angus digital certificate be regarded as an ABN-DSC. This is the first such solution to facilitate the technical change and encourage the use of e-commerce in the Australian economy in an effort to support the governments' direction outlined in *Investing for Growth*.

In this instance, cross recognition will be completed with each Project Angus member (PKI implementation), prior to the Angus certificate being regarded by Agencies as an ABN-DSC.

Throughout this Broad Specification for the ABN-DSC, there is reference to Gatekeeper fully accredited CAs and RAs. This reference now encompasses certificates regarded as ABN-DSCs, issued from a cross-recognised PKI provider. (ie the whole chain of trust has been assessed).

The providers must still ensure compliance with this Broad Specification prior to any acceptance of an ABN-DSC by Agencies.

1.5 This document

This document provides a broad specification for an ABN-DSC type of digital certificate. It sets out the policy objectives, business rules and method of operation for such a class of digital certificate. Those business rules and methods of operation are provided as a model that could be adopted by organisations that want to use the ABN-DSC. Different implementations of the ABN-DSC may use variations of this model, however, it will be used as the

benchmark for those seeking *Gatekeeper* Accreditation for their implementation of an ABN-DSC Certificate Policy.

For information:

This document should be read in conjunction with the *Gatekeeper* model Certificate Policy (CP) which is available at:
(<http://www.noie.gov.au/projects/confidence/Securing/001214%20Model%20CP%20v7%20clean.PDF>)
and the ABN-DSC Implementation of the ABN Private Extension document which is available at:
(http://www.noie.gov.au/publications/NOIE/ABNDSC/ABN-DSC_PrivateExtensionDetails.pdf)

Terms used in this document are defined in the glossary at Attachment A.

1.6 Non-Repudiation

There is a view by some PKI service providers that non-repudiation can only be offered by employing a trusted third party technical solution. However, other providers have a view that non-repudiation can be offered through the use of existing applications supported by clear and concise policies and procedures. In a legal sense all allegations put forward by a party to litigation may be disputed by the other party.

As there has yet to be a judicial decision dealing with non-repudiation in a PKI environment, or an interpretation of the electronic signature requirements in the *Electronic Transactions Act*, the choice of service provider and what they have to offer by way of non-repudiation, is a business decision for organisations.

2 WHAT IS THE ABN-DSC?

The Australian Business Number - Digital Signature Certificate (ABN-DSC) is a policy and a specification for a standard digital certificate incorporating the ABN.

2.1 Policy objective

The implementation of the ABN-DSC is policy outcome based. The concept grew out of the Prime Minister's 1997 statement *Investing for Growth* in which the Government sought to use its position as a leading edge user of IT to help get Australia online. The required policy outcomes are:

- the fostering of trust in e-commerce for transactions between business to government (B2G) and between business to business (B2B);
- the development of a broad use digital certificate to supplement the ABN unique business identifier; and
- the growth of the information economy.

2.2 Policy specification

The ABN-DSC is a specification for a broad use digital certificate based on the ABN. Specifically, the ABN-DSC specification defines a class of digital certificate that:

- will be used by Agencies to identify Business Entities when conducting online transactions;
- a Business Entity can use to deal with Agencies;
- a Business Entity can use to undertake online transactions with other businesses ;
- will have a common Certificate Profile and CP based on the *Gatekeeper* strategy;
- will be based on the X.509 standard;
- will be able to be issued by any *Gatekeeper* fully accredited Certification Authority (CA) (or cross recognised PKI provider);
- will be accepted by all Agencies ;

- may be called whatever a CA chooses to name their particular issue of the "ABN-DSC" eg *XYZ Business Certificate*;
- may have multiple Key Holders in an organisation, accepted by multiple Relying Parties, with numerous issuers of digital certificates.
- requires two Key Pairs known as the:
 - authentication keys – the keys used for creating and verifying digital signatures; and
 - confidentiality keys - the keys used for encrypting and decrypting messages for confidentiality purposes.

3 THE ABN-DSC AND GATEKEEPER

Ensuring trust and confidence in the use of the ABN-DSC is the paramount objective of the ABN-DSC policy proposal. The ABN-DSC is designed to operate under the *Gatekeeper* strategy.

Gatekeeper is the Commonwealth's PKI strategy. It was set up to provide a mechanism for the implementation of Public Key Technology by Agencies. It aims to facilitate interoperability and allow agencies to choose from a panel of service providers whose products and methods of delivery have been evaluated and accredited to meet prescribed government standards for integrity and trust.

The *Gatekeeper* Accreditation process for CAs and Registration Authorities (RA) ensures that digital certificate implementations maintain appropriate Commonwealth policies, including privacy and security and ensures interoperability between accredited organisations. The aim of the accreditation process is to provide certainty and trust for all parties involved in the use of *Gatekeeper* digital certificates.

The ABN-DSC will be a *Gatekeeper* compliant digital certificate. It will be an organisational digital certificate, which in terms of the current *Gatekeeper* strategy is a Type 2 (non-individual) certificate and will be designated as Grade 2 within that group. However, the ABN-DSC, as specified, will only be utilised to protect information up to the In-Confidence level. Financial limitations will be determined by transacting parties and the CP under which the particular ABN-DSC is issued.

CAs and RAs who wish to issue ABN-DSCs must be *Gatekeeper* fully accredited (or cross-recognised). If Commonwealth agencies want to undertake the role of CAs or RAs they must be accredited under the *Gatekeeper* scheme. Accredited CAs and RAs are listed on the NOIE website at www.noie.gov.au

ABN-DSC Certificate Policies (CP) developed by CAs must be *Gatekeeper* accredited prior to an ABN-DSC being issued. The *Gatekeeper* Accreditation process has developed a considerable degree of market place acceptance, nationally and internationally. The rigour that is inherent in the *Gatekeeper* strategy will be applied to this type of digital certificate.

While the ABN-DSC will be the primary digital certificate for use by Agencies when dealing online with Business Entities, there will be other *Gatekeeper* digital certificates issued by accredited service providers that will not conform to the ABN-DSC specification. These digital certificates will be used to meet specific business needs or will be issued to individuals.

4 USE OF THE ABN-DSC

4.1 How and when may it be used?

Use of PKI is a business and risk management decision for Agencies. Should Agencies choose to use PKI for supporting online transactions, they are required to use *Gatekeeper* accredited products and services. Similarly, if agencies themselves decide to directly provide PKI related services, they are required to obtain *Gatekeeper* Accreditation.

Specifically, the ABN-DSC:

- will be used by Agencies to authenticate Business Entities with whom they are undertaking a range of online regulatory and commercial transactions;
- will be used by Agencies for Government to Government (G2G) transactions;
- **Will not** be used for transacting online business with individuals as individuals
 - the ABN-DSC is intended for use to transact with Business Entities which have an ABN (including sole traders)

Agencies may be Subscribers to an ABN-DSC, and also act as a Relying Party.

Agencies may choose to accept any digital certificate at their own discretion. They are not required to accept only *Gatekeeper* accredited digital certificates or the ABN-DSC. This is consistent with Government policy on the use of the ABN-DSC and the *Gatekeeper* strategy as the digital certificates in the above case are not being issued/commissioned by Agencies.

4.2 What transactions may it be used for?

The ABN-DSC may be used in a variety of B2G regulatory and commercial requirements such as:

- regulatory returns (eg tax, ABS, Customs);
- online applications (eg for program funding);
- public registers (eg update of the ABR);
- e-procurement applications;

- tender applications;
- order/purchase (eg publications);
- online payments; and
- secure data transactions (see 4.5 below).

4.3 Which organisations should use it?

The ABN-DSC is primarily intended for B2G use. Nothing in the design of the CP and Certificate Profile prevents its use by businesses when transacting online with other businesses (B2B). However, the Commonwealth does not accept any liability for B2B use of the ABN-DSC.

All Agencies covered by the *Financial Management Accountability Act 1997* as well as agencies covered by the *Commonwealth Authorities and Companies Act 1997* are to use the ABN-DSC when identifying business entities online. This is consistent with the requirements for use of the Commonwealth's *Gatekeeper* framework.

Government Business Enterprises and companies will need to exercise their commercial judgement as to whether and to what extent they utilise PKI and the ABN-DSC for conducting online transactions.

State and Territory governments have agreed to adopt the *Gatekeeper* and ABN-DSC strategies, where appropriate, for implementation of PKI in their respective jurisdictions.

4.4 Financial limitations

Any financial limit on transactions supported by the ABN-DSC will be a matter for the Relying Party in that particular transaction (such as an Agency accepting a communication from a business) to determine and communicate to other parties as necessary. It should be noted that any such limit applies to the transaction value that the Relying Party and the Subscriber are prepared to accept for that particular business transaction, not to the ABN-DSC itself. This will allow a Subscriber to use the same digital certificate to transact business with different Agencies even though those Agencies may operate different internal transaction limits.

4.5 Confidentiality limitations

The general security offered by *Gatekeeper* standards and processes along with its associated CPs will make the ABN-DSC suitable for supporting the wide range of transactions with business discussed above, including regulatory return transactions such as data collections and licensing.

The ABN-DSC, as specified, is suitable for supporting the transmission of information up to and including the "in-confidence" level (as defined in the Commonwealth Protective Security Manual).

5 ISSUING THE ABN-DSC

5.1 To whom may the ABN-DSC be issued?

An ABN-DSC may be issued to any entity which holds an ABN. The list of entities which can hold an ABN is extensive and includes Commonwealth, State and Territory agencies. However, to comply with the *Gatekeeper* strategy the ABN-DSC must be issued to an individual representing the Business Entity.

The following outlines a model that could be adopted by organisations who wish to use the ABN-DSC. It is based broadly on the corporate credit card model and promotes e-commerce by allowing the Business Entity to manage multiple digital certificates. Different implementations of the ABN-DSC may use variations of this model. However, this model will be used as the benchmark for those seeking *Gatekeeper* Accreditation for ABN-DSC CPs.

Under this model, the Business Entity is expected to manage its digital certificates and will need to appoint an Authorised Officer who is to hold the initial ABN-DSC on behalf of the business. The Authorised Officer must be authorised by a person with a clear capacity to commit the business entity for the purposes of these activities (Section 7 provides further details on the definition and role of the Authorised Officer).

A Business Entity may require several people to conduct electronic transactions on behalf of the company. (eg ordering, accounts payable, customer relations etc) or there may be various points of contact within the business to deal with different Agencies. Therefore, multiple ABN-DSCs may be required. Where this is the case:

- additional ABN-DSCs will be issued to business representatives nominated by the Authorised Officer;
- there may be multiple Authorised Officers in any one Business Entity;
- there will be no limitation on the number of ABN-DSCs that may be issued to a business;
- all ABN-DSCs issued to a Business Entity will have the same ABN embedded in them;
- all ABN-DSCs will be considered to be of equal status in terms of binding a Business Entity to a transaction.

5.2 Management of certificates by Business Entities

A Business Entity must take full responsibility for the management of its ABN-DSCs. How digital certificates are allocated, what delegations are held by Key Holders of ABN-DSCs and how new digital certificates need to be issued or existing ones revoked as organisational structures change, are internal matters for the Business Entity to manage.

This process becomes particularly important where a Business Entity acquires multiple ABN-DSCs. The Business Entity must take on full responsibility and liability for the management and use of those digital certificates and should put appropriate certificate management processes in place.

5.3 Use of the ABN-DSC with the ATO

From the second quarter of 2002 it is expected that the ABN-DSC will be accepted by the ATO as an alternative to the current ATO digital certificate. To allow this to occur the Public Officer of a Business Entity may also need to be issued with an ABN-DSC. In the taxation context, Public Officers are entities established under the *Income Tax Assessment Act (Cth)*, and must be appointed by all incorporated business taxpayers. They act as the business taxpayer's representative with the Australian Tax Office. Public Officers are entities primarily recognised by tax law and are not usually business principals, such as company directors, with power to represent and bind the Business Entity.

The provision of an ABN-DSC to the Public Officer would be undertaken at the discretion of the Authorised Officer, as the issue of an additional digital certificate for the Business Entity, where necessary. It should be noted that the ABN-DSC will only identify the holder as a representative of the Business Entity, not specifically as the Public Officer, and will not indicate any authority for the Key Holder in the role as the Public Officer. The role and responsibilities of the Public Officer in regard to use of an ABN-DSC must be managed internally by the Business Entity.

5.4 How might the ABN-DSC be issued?

Only RAs and CAs accredited under the *Gatekeeper* strategy (or granted cross-recognition) can register applicants and issue ABN-DSCs respectively.

If Commonwealth agencies consider they have a particular need to undertake CA or RA functions themselves to meet business requirements they must become *Gatekeeper* accredited.

The issue of digital certificates to Business Entities to transact online with the Agencies will take place in a number of ways, including:

- Agencies may commission a Gatekeeper Accredited CA(s) to issue ABN-DSCs to their clients/customers to meet a particular business need;
- Agencies, if they are *Gatekeeper* fully accredited, may issue digital certificates directly to clients;
- Agencies may approach clients/business customers requesting that they acquire an ABN-DSC from an accredited service provider;
- the implementation of whole-of-government e-commerce initiatives may be accompanied by an issue of ABN-DSCs to specific businesses;
- a Business Entity may approach an agency and/or a Gatekeeper Accredited CA for a digital certificate to be used with Agencies;
- a Business Entity may request a CA to issue ABN-DSCs; and
- With the take up of the ABN-DSC strategy by State and Territories, Agencies of the States and Territories may also commission accredited CAs to issue ABN-DSCs.

6 THE ABN-DSC CERTIFICATE POLICY AND PROFILE

6.1 Gatekeeper model Certificate Policy and Certificate Profile

This specification does not include a specific CP or Certificate Profile for the ABN-DSC. It is based on the Gatekeeper model CP and Certificate Profile provided under *Gatekeeper* for all *Gatekeeper* digital certificates.

6.2 ABN-DSC Certificate Policy

The ABN-DSC will be based around a common CP and Certificate Profile. CAs are expected to maintain consistency with the *Gatekeeper* model when issuing their own versions of the ABN-DSC. It is expected that the actual digital certificates issued by any *Gatekeeper* fully accredited CA will essentially be the same except for fields such as the identification of the issuing CA and the name(s) and ABN of the person and Business Entity to which the digital certificate is issued.

It is expected that CAs may choose to add their own marketing components to the ABN-DSCs they issue. CAs must submit their ABN-DSC Certificate Policy for *Gatekeeper* Accreditation prior to digital certificates being issued.

This approach has been taken to provide Subscribers and Relying Parties with a high level of certainty about the benefits and obligations inherent in the use of the ABN-DSC while still allowing a degree of flexibility for service providers. The differences in products being offered by CAs can be identified from the CP.

6.3 ABN-DSC Certificate Profile

It should be noted that the ABN-DSC is a standard digital certificate. It will comply with the broad international X.509 standard and the draft Australian standard AS 4539 for digital certificates. CAs are expected to maintain consistency with the *Gatekeeper* Certificate Profile when issuing their own versions of the ABN-DSC. To this end, CAs must submit their ABN-DSC Certificate Profile for *Gatekeeper* Accreditation prior to digital certificates being issued.

For information:

The Gatekeeper X509 Certificate and Certificate Revocation List Profile is available at:

(http://www.noie.gov.au/projects/confidence/Securing/Gatekeeper/Gatekeeper_Certificate_and_CRL_Profile_v2.0.pdf)

The Gatekeeper PICS Proforma is available at:

(<http://www.noie.gov.au/projects/confidence/Securing/Gatekeeper/Gatekeeper%20PICS%20Proforma%20v2.pdf>)

The ABN-DSC Implementation of the ABN Private Extension V1.3 is available at:

(http://www.noie.gov.au/publications/NOIE/ABNDSC/ABN-DSC_PrivateExtensionDetails.pdf)

6.4 Construction of the Distinguished Name in an ABN-DSC

The private key associated with an ABN-DSC must be issued to a individual on behalf of the Business Entity. The corresponding public key is bound to the 'Distinguished Name' of that individual by use of a digital certificate.

A convention for Distinguished Names must take many factors into account. The convention must comply with the relevant standards, namely X.509, X.500, X.520, RFC2459, MP59 and AS4539. These standards define how a Distinguished Name can be constructed in compliance with the standards, but they do not discuss what objects the elements of the Distinguished Name would represent in terms of entries in an X.500 compliant directory nor do they imply any information hierarchy¹. Such considerations are very important if the certificate is to be published to a directory using the same Distinguished Name as the Subject name of the certificate.

The standard X.521 provides standard object classes that should be supported by compliant directories and recommends name forms and Directory Information Tree (DIT) structure rules that the directory should support. The name forms and DIT rules are the two directory schema items that define what attribute types can be used to name an object in the directory and how different entries may be hierarchically arranged based on the type of object they are. This document includes a modified version of Figure B.1 from Part 7 of X.521 in Figure 1.

This modified diagram combines the DIT structure rules and name forms of X.521 but only with respect to a limited set of objectClasses that are regarded as applicable and useful in the scope of ABN-DSC certificates. Figure 1 prescribes DIT structure rules which must be used when publishing ABN-DSC certificates to a directory. This figure also shows the naming attribute that must be used in ABN-DSC certificates when naming these objects, that is, the name forms. The concept of name forms is discussed in more detail in the next paragraph.

Figure 1 can be wholly used to construct Distinguished Names for ABN-DSC certificates that conform with this profile. To use the diagram, work from the top of the diagram at the country object, and choose a path that ends at the organizationalPerson object at the bottom of the diagram. For each object along the path, including the start and end points, the DN is formed by concatenating the naming attributes.

¹ Except for MP59

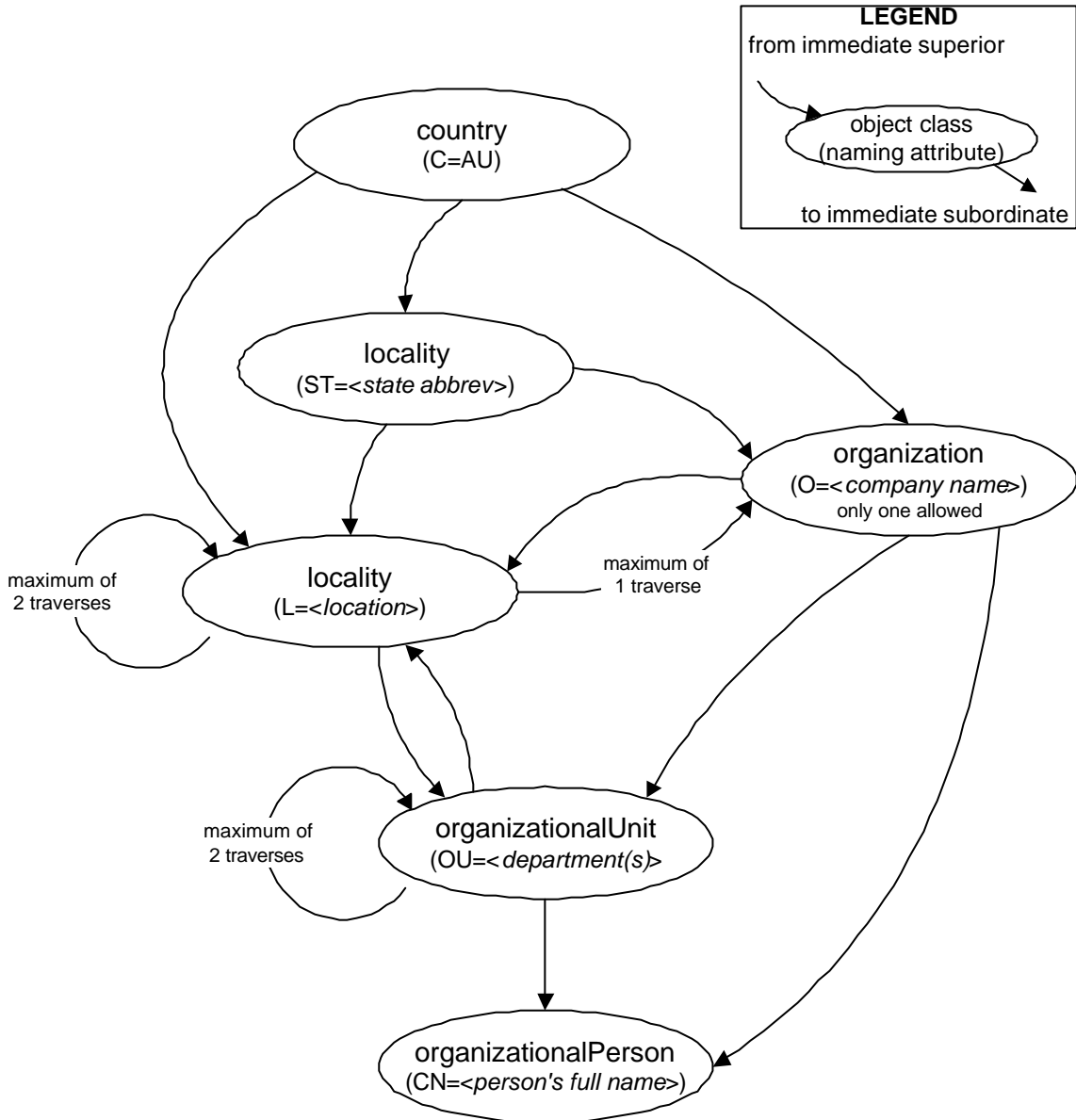


Figure 1 - ABN-DSC DIT structure rules and name forms

An example of a minimalist DN that can be constructed using the diagram (in X.500 order convention from X.501) is:

- C=AU, O=Organisation Pty Limited, CN=John Andrew Citizen

Such a DN has chosen the rightmost path from top to bottom.

Figure 1 shows that the object class for the certificate holder's entry is organizationalPerson. However, in implementation, this object class has to be subclassed or an auxiliary object class (like strongAuthenticationUser) has to be used so that it has an attribute type against which the certificate can be written and held as a value. The mandated attribute for which ABN-DSC certificates are to be written is userCertificate as defined in X.520. This document only mandates use of at least the person and organizationalPerson object classes for entries

representing ABN-DSC certificate holders; the actual object may be a combination of several more object classes (either through additional subclasses or auxiliary classes).

The X.521 name rules translate which attribute types of the object class must or may be used to name the object. Table 1 defines the name forms that, should be incorporated in the Distinguished Name field of an ABN-DSC and is based on the name forms defined in the 1993 version of the standard. The order of name forms in the table does not dictate permitted orders of DN elements; Figure 1 is used to prescribe such an order.

It should be noted that an additional attribute may be required to ensure DN uniqueness in specific instances. To achieve this the use of the serialNumber attribute type as per RFC 3039 Section 3.1.2, possibly as part of the organizationalPerson RDN, should be strongly considered. If used the serialNumber should be unique enough to achieve its purpose but not globally unique in a way that would constitute a global identifier.

Applies to this object class	Attributes to be used in Naming	Description	Example
country	countryName	Two letter form of country.	AU
locality	stateOrProvinceName	Three letter form of state name (as per MP59) where business is registered or where the certificate holder conducts business.	QLD
locality	localityName	Locality name where business is registered or where the certificate holder conducts business. Maximum of three for ABN-DSC certificates.	South Melbourne
organization	organizationName	Registered Company name. Maximum of one for ABN-DSC certificates.	Organisation Pty Ltd
organizationalUnit	organizationalUnitName	Qualifier of Organization Name, such as department name, though other formulations are allowable. Maximum of three for ABN-DSC certificates.	Accounts
person organizationalPerson	commonName	Private key holder's full name	John Orville Smith

Table 1 – Permitted name forms for ABN-DSC certificates

6.4.1 Examples

The following Distinguished Names were constructed using Figure 1 and hence conform to this recommendation:

- C=AU, O=Organisation Pty Limited, OU=Accounts, CN=John Andrew Citizen
- C=AU, ST=NSW, O=Organisation Pty Limited, OU=Accounts, CN=John Andrew Citizen
- C=AU, O=Organisation Pty Limited, L=Sydney, OU=Accounts, CN=John Andrew Citizen
- C=AU, O=Organisation Pty Limited, OU=Financial Department, L=Sydney, OU=Accounts, CN=John Andrew Citizen
- C=AU, L=Sydney, O=Organisation Pty Limited, CN=John Andrew Citizen
- C=AU, ST=NSW, L=Sydney, O=Organisation Pty Limited, OU=Accounts, CN=John Andrew Citizen

6.5 Inclusion of the ABN

The inclusion of the ABN of the subject in the ABN-DSC provides an essential characteristic of the digital certificate. This allows the digital certificate to be used to truly identify a Business Entity.

However, the inclusion of the ABN in the ABN-DSC Certificate Profile is not supported by current standards for digital certificates and a number of options for its location were considered. The most suitable location was deemed to be in a private certificate extension.

It should be noted that this extension is to be marked non-critical to maximise the interoperability with applications that are not aware of the ABN or the ABN-DSC.

7 REGISTRATION REQUIREMENTS

This document is not intended to be prescriptive with respect to operational processes for Registration Authorities. It is accepted that roles, responsibilities and arrangements may differ depending on the organisations involved and the particular business models, that they choose to adopt. The process outlined below is indicative of the process required for an ABN-DSC (*Gatekeeper* non-individual) certificate, however it will be used as the basis for *Gatekeeper* ABN-DSC CP evaluation.

7.1 Introduction

For the issue of Keys and Certificates to a Business Entity there must be a process where confirmation that the Business Entity exists can be achieved, and that the person authorised to receive a digital certificate on behalf of the Business Entity, is who they say they are. The process below describes an Evidence of Identity (EOI) process by which this can be achieved.

7.2 Aim

The aim of the process is:

- To bind a Business Entity to a business name and to an Australian Business Number (ABN);
- To bind the physical person to the name of the Authorised Officer;
- To bind the Authorised Officer (see 7.3) to the Business Entity;
- To bind the person who gives the Authorised Officer the power to act, that is, the person with a 'clear capacity to commit the business', to the Business Entity; and
- To bind additional names to the Business Entity via the Authorised Officer (ie for issue of additional ABN-DSCs).

7.3 The Authorised Officer

The Authorised Officer is an entity created specifically for this ABN-DSC specification. It was generally supported by feedback from the range of stakeholders consulted during the development of this specification. It is not a role which could be said to be a traditional part of PKI.

An Authorised Officer is a person duly authorised by the Business Entity or by law (this would normally be an officer or employee of the business) to:

- submit an application to hold an ABN-DSC;
- complete, sign and lodge the necessary documentation that provide evidence of the identity of the Business Entity and the Authorised Officer;
- request additional ABN-DSCs as required for use by other representatives of the Business Entity;
- on behalf of the Business Entity, vouch for the identity of all representatives for whom applications to hold ABN-DSCs are made; and
- undertake on behalf of the Business Entity that it will accept responsibility for the use of all ABN-DSCs.

An Authorised Officer is given the authority to act on behalf of the Business Entity by an Authoriser, who is a member of a class of persons with a 'clear capacity to commit the Business Entity' for the purposes of these activities. Persons who are members of this class include (but are not limited to):

- chief executive officer;
- company director;
- trustee;
- partner;
- company owner.

The Authorised Officer must be able to show evidence of such authorisation by reference to one or more documents which permit or instruct the officer to perform all the activities listed above and which are signed by an "Authoriser".

In addition, that Authoriser's association with the Business Entity must be evidenced by reference to:

- an authoritative public register; or
- appropriate legal, or regulatory documents issued by a government agency (see Section 7.5).

It should be noted that the Authorised Officer as described above and the person providing the Authorised Officer with that authority (the Authoriser) may in fact be the same person.

While a Business Entity would normally only have one Authorised Officer for managing ABN-DSCs, a very large or very decentralised organisation, for example, may need to appoint additional Authorised Officers for practical operational purposes. Given the critical role played by the Authorised Officer in the management of ABN-DSCs for an organisation, the allocation of such positions is expected to be strictly managed by the Business Entity.

7.4 Registration Process

RAs may propose other Registration processes for consideration by Gatekeeper evaluators for the issue of an ABN-DSC as long as they meet the minimum requirements below, and that the ABR is part of the validation of a Business Entity with an ABN. Operating processes are evaluated on a case by case basis for each service provider seeking Gatekeeper accreditation. However, the basic requirement for an Authorised Officer and 100 points of EOI for that officer will remain a consistent aspect of the ABN-DSC.

7.4.1 Evidence of Identity that would be acceptable for ABN-DSC purposes by a Business Entity for the issuance of an ABN-DSC is:

- an original or certified copy of the notice issued by the Registrar of the Australian Business Register (ABR) bearing the Business Entity's name and the ABN (if either the owner, chief executive or other officer or employee with clear capacity to commit the Business Entity, is named as the Public Officer on the document issued by the Registrar of the ABR, then this document only will suffice). (online verification with the ABR to link the organisation's ABN to its business name is recommended); OR
- if the notice issued by the Registrar of the ABR cannot be provided then:
a legal or regulatory document binding either the Authorised Officer or the Authoriser with a clear capacity to commit the Business Entity, to the Business Entity (in this case online verification with the ABR to link the organisation's ABN to its business name must be achieved); AND
- EOI documentation to the value of 100 points for the Authorised Officer of the Business Entity using the Financial Transaction Reports Act 1998 (Cth) Form 201 Identification Record for a Signatory to an Account. Specifically, EOI required for the Authorised Officer is:
(1) One Primary Document @ 70 points (Birth Certificate OR Passport OR Citizenship Certificate); AND
(2) One, or a combination of, secondary documents equalling 40 points and below, to achieve a minimum overall total of 100 Points under the following conditions;

- (a) If a current photo is not provided with a Primary Document then it must be provided as part of a secondary document;
- (b) Where a name shown in a Primary Document differs from the name shown in a secondary document, proof of the reason for that name change must be provided. This proof does not count towards the 100 point check; and
- (c) Documents within the FTR Act Form 201 identified for use by deposit-taking institutions (ADIs) can only be used by those authorities.

7.4.2. The applicant's full name, as shown on the EOI documentation, shall be used as the subject's common name in the ABN-DSC.

7.5 Legal or regulatory documents

The new Annex P to the Gatekeeper strategy contains a list of documentation recognised by Gatekeeper. These documents are appropriate for use with the ABN-DSC EOI process.

7.6 Indicative Procedure

The following is an indicative procedure that satisfies the requirements outlined above.

The Business Entity applies to the CA (or directly to an RA depending on the business model adopted by the CA) for a digital certificate. The Business Entity should indicate in its application (mail, e-mail, or online) as much information about itself as possible to allow preliminary organisational EOI checks to begin.

For example:

- provide the Business Entity name;
- provide the Business Entity ABN;
- provide both the Business Entity's postal and street addresses; and
- provide both the Business Entity's phone and facsimile numbers.

The CA/RA would provide, or in an online environment allow the completion of, an application, individually identified with a unique serial number or other such individually recognisable indicator.

The Business Entity would provide a letter from a person with clear capacity to commit the Business Entity, stating the name of the Authorised Officer; that is the person authorised to receive the Business Entity's initial ABN-DSC. The Authorised Officer will bring this letter, with the completed application and

relevant documentation to the RA for a formal face-to-face EOI check, to enable the 100 point EOI requirement to be satisfied.

The RA in accordance with its accredited process for the digital certificate requested would:

- check the documentation and/or ABR binding the Business Entity to an ABN;
- check the documentation binding either the owner, chief executive or other officer or employee with clear capacity to commit the Business Entity, to that Business Entity;
- check the documentation binding the Authorised Officer to the Business Entity; and
- check the documentation binding the physical person of the Authorised Officer to the name provided by either the owner, chief executive or other officer or employee of either the owner, chief executive or other officer or employee with clear capacity to commit the Business Entity.

Note: The RA may also choose to utilise online facilities or third party services to provide additional checks on legal or regulatory records/documents.

When the RA is satisfied that the above EOI checks have been met, a formal application for a digital certificate, containing only that information necessary for the creation of a digital certificate, is forwarded to the CA. The RA will retain registration documentation.

Delivery of the ABN-DSC is then achieved securely in accordance with the accredited process for that particular CA.

7.7 Additional certificates

Where a Business Entity requires additional ABN-DSCs, the Authorised Officer will send an authorised request to the CA or RA (for example, digitally sign an e-mail using his/her ABN-DSC) requesting digital certificates for additional representatives from the Business Entity. This process would bind the additional names to the Business Entity. The issue of additional digital certificates to additional persons is to be securely achieved in accordance with the accredited CA processes.

Requests for additional ABN-DSCs for a Business Entity should be made through the same CA or RA that supplied the initial ABN-DSC as a specific process may be required to check that the request came from an Authorised Officer. Arrangements may need to be put in place between the CA and RA to this effect as it is likely that only the RA will have relevant records indicating that a Key Holder is an Authorised Officer of a particular Business Entity.

The business has to accept full responsibility for these digital certificates and will be expected to put in place appropriate procedures to ensure that a full documentary trail is maintained for the issue and management of these digital certificates.

It would be expected that, as part of the nomination process, the Business Entity would undertake checks of employment records and other appropriate records to assure the Authorised Officer that the person being nominated to hold additional ABN-DSCs for the entity has been properly identified.

CAs may choose to initiate specific arrangements with the Business Entity in regard to responsibility and liability for these digital certificates.

8 FEES

Payment arrangements for the issue of ABN-DSCs will vary depending upon the business application being addressed and the nature of the relationship between the commissioning entity and its business clients.

In some cases the commissioning entity may pay the issue costs, while in others the costs may be borne by business Subscribers, a third party or some combination of the above.

This ABN-DSC specification does not specify a particular fee arrangement. This will need to be negotiated between a commissioning entity and the selected service provider and would normally form part of a tendering process undertaken to select a service provider to undertake the roll out of digital certificates. As ABN-DSCs are able to be issued by all *Gatekeeper* fully accredited service providers, Agencies will be able to select from a number of service providers and market forces will determine the prices charged for services.

9 PRIVACY

Privacy issues in regard to the ABN-DSC will be managed in a number of ways, including:

- The ABN-DSC will only be issued by *Gatekeeper* fully accredited CAs. The *Gatekeeper* Accreditation criteria require strict adherence to the Commonwealth's Information Privacy Principles incorporated in the Privacy Act 1988. Under these arrangements there is to be no release by RAs of personal information about applicants or holders of digital certificates to third parties.
- There will be no central or coordinated recording of digital certificates issued or of their usage; the ABN-DSC can be issued by any of a number of CAs.
- The digital certificate itself, developed under this specification, will contain very limited information, and any personal information will relate only to the individual *as a representative of a business*. The only personal information held in a digital certificate will be the name of person who is the Key Holder, which is part of the distinguished name field.

While the use of the ABN-DSC derives from the publicly available business identifier mandated by legislation for Commonwealth use (ie the ABN), it does not provide any connection to the Australian Tax Office unless specifically used for business to ATO transactions.

10 CERTIFICATE REVOCATION

Certificate Revocation Lists (CRL) are the means by which Relying Parties confirm the status of a digital certificate in order to decide whether they will trust/accept a particular digital certificate or not. Under *Gatekeeper* Accreditation requirements, CAs must maintain a complete and readily available CRL, updated at regular intervals, to enable Relying Parties to check the revocation status or validity of digital certificates. It is recommended that digital certificate status be checked on each occasion that a Relying Party receives a transmission or transaction.

10.1 Circumstances for revocation

It is expected that Keys and Certificates will be revoked where any one of the following circumstances arises:

- a Private Key is compromised;
- media holding a Private Key is compromised or lost;
- the Business Entity ceases to hold an Australian Business Number;
- the Key Holder ceases to represent the business;
- there has been improper or faulty issue of the Keys and Certificates;
- the Certificate information becomes inaccurate;
- the relevant CA ceases to operate;
- the CA receives a revocation request from the Authorised Officer of the Business Entity or the Key Holder.

10.2 Who can request revocation

Digital certificate revocation may be initiated by:

- the Key Holder;
- the Authorised Officer of the Business Entity;
- a person with clear capacity to commit the Business Entity (eg the Authoriser);
- authorised third parties such as parties with Power of Attorney from the Business Entity or the Key Holder or an Australian court with appropriate jurisdiction;

- the relevant CA if they believe "circumstances for revocation" exist.

Agencies, as Relying Parties, cannot initiate revocation action as while one agency may no longer wish to recognise a particular digital certificate, it may be quite valid with other agencies.

Agencies, when acting as Key Holders may initiate the revocations of their own digital certificates.

10.3 Revocation process

To process a revocation request a CA would be expected to do the following:

- publish notice of revoked digital certificates in the Certificate Revocation List (CRL);
- issue a notice, confirming the revocation of the Keys and Certificates and the date and time that the digital certificate was revoked, to the business and/or the Key Holder. The notice need not include the reason for revocation;
- list the certificate in the CRL until its validity period expires and then archive the revoked digital certificate; and
- provide access to certificate status information via an approved X.509 compliant protocol (eg. DAP, LDAP or OCSP). CAs are not confined to using a single protocol for the distribution of digital certificate information. It is the CAs responsibility to ensure information in 'directories' is synchronised.

The above arrangements will be reflected in Subscriber agreements between the CA and Key Holders and in other documentation accredited in accordance with the *Gatekeeper* strategy and the CA's implementation of the ABN-DSC.

10.4 Certificate suspension

Suspension of an ABN-DSC will only be supported where the issuing CA supports this functionality.

10.5 Certificate renewal

Business Entities holding ABN-DSCs will be expected to manage the Certificate renewal cycle to a large extent.

It is expected that an ABN-DSC will have a life of two years. Only the Authorised Officer of a Business Entity will be able to request a renewal of digital certificates, for themselves or for others nominated to hold ABN-DSCs for the Business Entity, up to a maximum of six years (ie two renewal cycles). They can do this by using

their current digital certificate to sign such requests. This will avoid the need to go through any further EOI processes.

If, however, the Authorised Officer's Certificate has expired, they (the Authorised Officer) will have to undertake the full RA/EOI process as outlined in Section 7 above before being issued with a new ABN-DSC.

After six years (two renewal cycles), the Authorised Officer will be required to undergo the full RA/EOI process including a 100 point EOI check.

11 RECORD ARCHIVAL

ABN-DSC holders' private keys will not normally be held by Agencies or accredited CAs.

ABN-DSCs shall be archived for a minimum period of seven years from the date when they expire, unless another period is specifically required by a commissioning agency.

Audit trail information shall be kept for a minimum period of seven (7) years from the date of generation, unless a longer period is specifically agreed by a commissioning agency.

Archive media shall be protected either by physical security, or a combination of physical security and cryptographic protection. It shall also be protected from environmental factors such as temperature, humidity, and magnetism. Notwithstanding all of the above, archival of ABN-DSC information may be subject to jurisdictional legislation and other legal constraints. These may override the conditions described above.

12 OPERATION OF DIRECTORIES

CAs which issue ABN-DSCs will be required to operate a directory structure that supports the issued digital certificates. As a minimum, CAs are expected to operate standard X.500 directory services in accordance with ITU X.509 V3.

13 INTEROPERABILITY

Interoperability issues will be addressed under the *Gatekeeper* strategy by *Gatekeeper* Accreditation processes, by adoption of the international X.509.V3 standard for the ABN-DSC and by implementation of the *Gatekeeper* Accreditation Certificate (GAC).

The primary purpose of the *Gatekeeper* strategy is to provide the trust hierarchy for X.509 digital certificates within the Australian government's domain.

In order to ensure interoperability within the *Gatekeeper* strategy and with other trust hierarchies, a Commonwealth trust point needs to be established. This will take the form of a self-signed X.509 digital certificate. CAs that have been accredited under the *Gatekeeper* strategy will be issued a GAC. Under this hierarchy, a Relying Party will be able to trust the Public Keys of any digital certificate issued within the *Gatekeeper* strategy by referring to a single trust point. The implementation will be fully compliant with X.509 (2000) and backwardly compatible with X.509 (1997).

14 LIABILITY

This section sets out proposed legal liability positions appropriate for Agencies using the ABN-DSC. These positions seek to encourage service providers while restricting Commonwealth liability risks and avoiding undue liability risks for Agencies' business clients when using the ABN-DSC.

Generally, liability will be determined under the relevant law in Australia that is recognised and would be applied by the High Court of Australia.

The Commonwealth position is that it will not accept any liability for losses resulting from:

- the use of an ABN-DSC where an Agency was not a party to the ABN-DSC supported transaction; and
- any reliance on, or errors in, the Australian Business Register. Please view the disclaimer to the online ABR at www.business.gov.au

Furthermore, the Commonwealth makes no representation and offers no warranties or conditions, express or implied, in relation to:

- the activities or performance of any of the Government Public Key Infrastructure; or
- if relevant, the services or products of a particular PKI Entity.

Gatekeeper accredited service providers, including any Agency which acts as an accredited provider, will be expected to fulfil their responsibilities as set out in *Gatekeeper* accredited CPs or Subscriber Agreements. They should therefore expect to be liable to their Subscribers or other Relying Parties for losses clearly due to their breach of those responsibilities, within any agreed liability limits.

Gatekeeper accredited CPs will also set out responsibilities for Subscribers and Relying Parties, notably to handle their private keys securely and to exercise due diligence in checking the validity of digital certificates. Losses for breaches of those responsibilities will generally be expected to lie with the party at fault.

The Commonwealth's position with respect to liability is fully detailed in the *Gatekeeper* model CP which can be found at:

<http://www.noie.gov.au/projects/confidence/Securing/001214%20Model%20CP%20v7%20clean.PDF>

ATTACHMENT A - GLOSSARY

In any document to which this Glossary applies, words and phrases have the following meanings unless a contrary intention is evident.

Additional Applicant	An individual who has been nominated by a Business Entity to become an Additional Key Holder.
Additional Certificates	Certificates which have been issued via the Authorised Officer, but are held by additional Key Holders.
Additional Key-holder	A Key Holder other than an Authorised Officer.
Agency	<ul style="list-style-type: none"> (a) a Department of State, or a Department of the Parliament, of the Commonwealth, a State or a Territory; (b) a body corporate or an unincorporated body established or constituted for a public purpose by Commonwealth, State or Territory legislation, or an instrument made under that legislation (including a local authority); (c) a body established by the Governor-General, a State Governor, or by a Minister of State of the Commonwealth, a State or a Territory; or (d) any incorporated company, other than the Contractor, over which the Commonwealth, a State or a Territory exercises control.
Applicant	A person who has applied to become a Key –Holder, prior to the time at which Keys and Certificates are issued to and accepted by them.
Australian Business Number (ABN)	The Australian Business Number (ABN) is a new single identifier for dealings with the Australian Taxation Office (ATO) and for future dealings with other government departments and Agencies.
Australian Business Register (ABR)	The Australian Business Register (ABR) contains all the publicly available information provided by businesses when they register for an Australian Business Number (ABN). The Australian Business Register was established under s.24 of the <i>A New Tax System (Australian Business Number) Act 1999</i> .
Authorised Officer	An Authorised applicant who has been issued with, and accepted, Keys and Certificates and is authorised by a Business Entity to nominate additional Key Holders to the CA.

Authoriser	<p>A class of persons with a clear capacity to commit the Business Entity.</p> <p>Persons who are members of this class include (but are not limited to):</p> <ul style="list-style-type: none"> • Chief Executive Officer • Company Director • Trustee • Partner • Company Owner <p>These persons are identified by the operation of section 7.5 Legal and Regulatory Documents.</p>
Business Entity	An entity entitled to have an ABN within the meaning of s.8 of the <i>A New Tax System (Australian Business Number) Act 1999</i> .
Business to Business (B2B)	Denotes online communication between Business Entities.
Business to Consumer (B2C)	Denotes online communication between Business Entities and consumers/individuals.
Business to Government (B2G)	Denotes online communication between Business Entities and government.
CEO, NOIE	The Chief Executive Officer of the National Office for the Information Economy
Certificate	<p>An electronic document signed by the CA which:</p> <ol style="list-style-type: none"> (1) identifies a Key Holder and the Business Entity he or she represents; (2) binds the Key Holder to a Key Pair by specifying the Public Key of that Key Pair; and (3) should contain the other information required by the Certificate Profile
Certificate Directory	The published directory listing digital certificates currently in force.
Certificate Information	Information needed to complete a Certificate as required by the Certificate Profile.
Certificate Profile	The specification of the fields to be included in a Certificate and the contents of each.
Certificate Revocation List (CRL)	The published directory which lists revoked and/or suspended Certificates. The CRL may form part of the Certificate Directory or may be published separately.
Certification Authority (CA)	A <i>Gatekeeper</i> accredited entity that verifies the identity of a user, allocates a Distinguished Name to that user, and verifies the correctness of information concerning that user by signing the data which constitutes the digital signature for that user.
Certification Authority Revocation List	A list of certification authorities that have had their <i>Gatekeeper</i> Accreditation status revoked.

Commonwealth	The Commonwealth of Australia and its agencies, employees, servants and agents.
Community of Interest	The group of entities which are eligible to apply as Business Entity's for issue of Keys and Certificates.
Competent Authority	The entity which approves the CA's infrastructure and practices (including the accredited documents and any changes to them) as meeting the criteria for <i>Gatekeeper</i> Accreditation. The Competent Authority for this PKI is the CEO, NOIE.
compromise	A situation in which the secrecy of a Private Key cannot be relied on, e.g. if there has been unauthorised access to the cryptographic module in which the Private Key is stored or used, or unauthorised access to or loss or theft of media on which the Private Key is stored.
correspond	A Public Key and a Private Key correspond if they belong to the same Key Pair. A Private Key corresponds to a Certificate if it corresponds to the Subject Public Key specified in the Certificate.
Defence Signals Directorate (DSD)	The Australian national authority for information security.
digital signature	An electronic signature created using a Private Signature Key.
digital certificate	An electronic document signed by the CA which: <ul style="list-style-type: none"> (1) identifies a Key Holder and the Business Entity he or she represents; (2) binds the Key Holder to a Key Pair by specifying the Public Key of that Key Pair; and (3) should contain any other information required by the Certificate Profile
Distinguished Name	A unique identifier assigned to each Key Holder, having the structure required by the Certificate Profile.
electronic signature	A data element associated with a message which identifies a person and indicates his or her approval of the contents of the message.
End Entity	An entity which uses Keys and Certificates for creating or verifying digital signatures or for confidentiality. End Entities are Key-Holders, Organisations or Relying Parties.
Evaluated Product	A hardware or software product which is on the EPL.

Evaluated Product List (EPL)	<p>A list, maintained by DSD, of hardware and software products which are considered to provide an adequate level of information security. Products are added to the EPL if they meet the requirements of:</p> <ol style="list-style-type: none"> 1. AISEP criteria E1 to E6; or 2. Common Criteria EAL1 to EAL4, with an additional review of cryptography by DSD. <p>The EPL is published at www.dsd.gov.au</p>
Evidence of Identity (EOI)	Documents that evince the identity of an entity.
Gatekeeper Accreditation	Accreditation by NOIE, granted on the basis that the CA meets the criteria set out in the <i>Gatekeeper Report</i> .
Government to Consumer (G2C)	Denotes online communication between Government and consumer/individuals.
Intellectual property rights (IP rights)	Copyright and neighbouring rights, all rights in relation to inventions (including patent rights), plant varieties, registered and unregistered trademarks (including service marks), registered designs, confidential information (including trade secrets and know how), databases, and circuit layouts, and all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields.
Key	A data element used to encrypt or decrypt a message - includes both Public Keys and Private Keys.
Key Pair	A pair of asymmetric cryptographic Keys (i.e. one decrypts messages which have been encrypted using the other) consisting of a Public Key and a Private Key.
Key Holder	An individual who holds and uses Keys and Certificates on behalf of a Business Entity, including an Authorised Officer.
NOIE	The National Office for the Information Economy- An Executive Agency of the Commonwealth of Australia
PKI Entity	<p>A PKI Entity one of the following:</p> <ol style="list-style-type: none"> 1. CA 2. Subordinate Entity 3. A Subscriber 4. Relying Party 5. RA
PKI Service Provider	Any entity which has roles, functions, obligations or rights under the CP, other than an End Entity. PKI Service Providers include Registration Authorities (RA) and Certification Authorities (CA).

Private Certificate-signing Key	The Private Key used by the CA to digitally sign Certificates.
Private Confidentiality Decryption Key	The Private Key used by the addressee to decrypt messages which have been encrypted using the corresponding Public Confidentiality Encryption Key.
Private Key	The half of a Key Pair which must be kept secret to ensure confidentiality, integrity, authenticity and non-repudiation of messages.
Private Signing Key	The Private Key used by a Key Holder to digitally sign messages on behalf of an Organisation.
Public Certificate-verification Key	The Public Key corresponding to the CA's Private Certificate-signing Key.
Public Confidentiality Encryption Key	A Public Key, corresponding to a Private Key held by the addressee, which may be used to encrypt a message to protect the confidentiality or privacy of its contents.
Public Key	The half of a Key Pair which may be made public.
Public Key Infrastructure (PKI)	The particular implementation of public key technology described in the CP and other accredited documents, under which Keys and Certificates are issued and used.
Public Verification Key	The Public Key corresponding to a Private signing Key used to verify a digital signature.
Registration	The process for receiving and processing applications for Keys and Certificates, including collection of Registration Information.
Registration Authority (RA)	An entity which registers applicants for Keys and Certificates (see Registration).
Registration Information	Information about Key Holders or Business Entity which is reasonably required for the issue and use of Keys and Certificates, including information needed to: <ul style="list-style-type: none"> • verify the identity of the Authorised Officer or the Business Entity; • confirm that the Authorised Officer has authority to hold and use Keys and Certificates on behalf of the Business Entity; and • confirm that the Business Entity is a member of the Community of Interest
Relying Party	An individual or entity, which receives a digitally signed message and wishes to rely on the contents of that message as binding the signer.

Repository	The entity (which could be the CA or another entity) which maintains the database of Certification which is made accessible to users including the Relying Parties.
Subordinate Entity	An RA and any other entity which is subordinate to the CA and which performs functions or provides services necessary for issue and use of Keys and Certificates, or for reliance on Digital Signatures. A Subordinate Entity does not include the CA itself or an End Entity.
Subscribers	In the case of the ABN-DSC, comprises the Non-Individual (eg Business Entity), and the Individual who acts on behalf of the Business Entity, who is in possession or has control, of the Private Authentication Key and who uses that Key to digitally sign messages.
Trustworthy Systems	Systems which meet the system security requirements of the Accredited Documents.
Type 2 Grade 2	An organisational Certificate which is issued to a non-individual user who satisfies certain identity requirements of 100 points.
X.509 version 3	The international standard for the framework for public key Certificates and attribute Certificates. It is part of wider group protocols from the International Telecommunications Union-T X.500 Directory Services Standards.