



**GATEKEEPER
SERVICES**

WHITEPAPER

ESIGN GATEKEEPER SERVICES

WHITEPAPER

Version 0.4

Date of Publication: January 2003



Copyright © 2001-2003 VeriSign Australia Limited. All rights reserved.

No part of this publication may be reproduced, stored in, or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of eSign Australia Limited. Notwithstanding the above, permission is granted to reproduce and distribute this document for an individual or organisation's own uses on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to VeriSign Australia Limited.

The eSign thumbprint and logo is a trademark of VeriSign Australia Limited. eSign Gatekeeper Services is a registered business name of VeriSign Australia Limited under which VeriSign Australia Limited provides Gatekeeper services.

VeriSign® is a registered trademark of VeriSign, Inc. VeriSign Trust Network™ is a trademark of VeriSign, Inc. All other trademarks and service marks are the property of their respective owners.

Preface

Many people fear implementing public key infrastructure (PKI) because of its perceived complexity or simply because they do not understand what it is all about. However, fundamentally it is not only simple but an extremely useful tool for business that solves many of the key problems in communicating in our increasingly online world.

Just as credit cards revolutionised consumer spending by allowing merchants to trust that by accepting a credit card they would ultimately receive payment by a bank, PKI and digital certificates are set to revolutionise broader business (and Government) transactions by enabling one to confidently do business online with business partners, government authorities and other online businesses. The analogy is not perfect but highly useful to understanding how PKI works. There are people who apply for the issue of the credential (in the case of PKI, Certificates rather than credit cards) (**Applicants**), organisations who examine the identity of the person applying for the credential (**Registration Authorities** not banks), organisations who issue the credential (in this case **Certification Authorities** not banks), and those who will accept the credential (in this case **Relying Parties** not merchants accepting credit cards). There are also those who set the rules of how and when credentials may be issued or cancelled and who is able to provide these services (in this case the **Competent Authority** (NOIE) not the scheme operators such as Visa or Mastercard).

PKI does even more than giving you a credential that can be accepted by the wider community. It also allows you to communicate securely by encrypting your communications.

Neither is PKI necessarily expensive. Today an Applicant can purchase a Certificate for slightly more than the annual fees of a credit card (the fees are slightly more as the PKI is not funded through charging fees on money loaned). A Relying Party (equivalent to a merchant) does not have to pay any fee for using certificates (unlike the merchant in a credit card operation who will pay set fees and a percentage (usually between 2-4%) of every transaction conducted) using the credential.

This paper aims at demystifying the PKI mandated and overseen by Government, Gatekeeper. Further information can be obtained from our web site (gatekeeper.verisign.com.au) which also contains most up to date policy documents.

This paper has three sections. The first is a general primer on PKI. The second discusses the business considerations in implementing a PKI and should be useful for the business owner responsible for determining the appropriate Certificates to order (Part 1) or when determining how your application should support Certificates (Part 2). The third contains the technical considerations from the point of view of a developer or organisation that wishes to be able to design an application that uses Certificates. There is some overlap between sections 2 and 3; section 3 is more technically focussed.

The main topics covered under each section are as follows:

Section 1: PKI Primer - Basic PKI concepts explained (PKI, Trust Hierarchies, Key Pairs, Dual Certificates)

Section 2: Business Considerations – Part 1: Purchasing Certificates - Types of Certificates, choosing the right certificate, applying for Certificates. Part 2: Using Certificates – what can certificates do for your business.

Section 3: Technical Considerations – matters relevant to developing an application using Certificates.

The final section of this document provides further reference information and resources for further reading.

Having worked at the forefront of providing certificate and PKI solutions (including Gatekeeper) for many years we are now at a point where we can point to real applications using PKI solutions to deliver a business benefit. I hope you find this paper a useful guide whether you need to quickly come up to speed with the terminology, understand the business benefits or implementing solutions using Gatekeeper Certificates.

Business Manager – Gatekeeper
VeriSign Australia Limited
January 2003

1. PKI Primer

1.1 Gatekeeper

The Gatekeeper strategy was developed by the Federal Government to increase confidence in the online economy by providing a Government endorsed online trust framework using public key technology.

The outcome of this strategy is an accreditation process operated by the National Office of the Information Economy (NOIE) which involves a thorough evaluation of all aspects of an organisation that seeks to either check that people applying for Gatekeeper credentials (**Applicants**) meet the identification requirements to be issued with Gatekeeper Certificates (**Registration Authorities or RAs**) or then issue applicants with Gatekeeper Certificates (**Certification Authorities or CAs**). NOIE uses evaluators such as ASIO, DSD and AGS to examine different aspects of those providers (*see further www.noie.gov.au for further information regarding NOIE's accreditation criteria*).

The outcome of this process is that if an organisation, such as VeriSign, achieves Gatekeeper accreditation from NOIE you can be assured that that organisation has met rigorous standards in relation to security, operational procedures and technical requirements. VeriSign operates the eSign CA and the eSign RA.

Gatekeeper Certificates can be used by business, Government or individuals.

1.2 PKI

PKI is the holistic name given to the combination of software, hardware, people policies and procedures needed to create, manage, store, distribute, and revoke Public Key certificates (digital certificates). Different organisations perform different roles in providing the PKI. A purchaser of Certificates or a person who relies on Certificates is only required to perform a limited role, and can expect the other PKI Entities (*see section 1.6 below*) to perform their roles.

Simple technical solutions exist that enable information to be communicated using encryption. The main benefits provided by PKI is it provides a system for distributing, and more importantly, trusting, those Certificates.

1.3 Certificates

A Certificate is a digital document or file that identifies someone or something and contains a Public Key (*see Key Pairs below*). Where a Certificate is issued to a person it is like an electronic passport which identifies that person. A certificate has a specific format and content. Of particular importance is the name the certificate is issued to (who is identified by the Certificate), the CA that issued the certificate (who issued the Certificate) and any restrictions (business or technical) on the use that can be made of the certificate, or what another person receiving a certificate (a **Relying Party**) can assume.

VeriSign can issue the following Gatekeeper Certificates:

- Individual Certificates (grades 1-3) – these identify an individual only, for example, Joe Smith.
- Non-Individual Certificates (grades 1-3) – these identify an individual which is related to an organisation, for example Joe Smith of Greenpeace or Mary Doe of IBM.
- ABN-DSCs (the only grade supported is grade 2) – these identify an individual which is related to an organisation with an Australian Business Number – for example Mary Doe of IBM with an ABN xxx xxx xxx. As the ABN is a unique identifier for business this has some significant advantages.

Gatekeeper also supports Device Certificates (Type 3 Certificates) for use by processes and devices (eg routers).

VeriSign can also issue a range of non-Gatekeeper certificates (*see Trust Hierarchies*).

1.3.1 Certificate Grades

Certificates may have particular limits put on their use and Gatekeeper certificates have different Grades which relate to the amount of checking the RA has performed on an Applicant's identity. Under Gatekeeper, checking of identity is based on a points system using documents recognised by the *Financial Transactions Reporting Act* (the points systems used by banks to determine whether they can trust you and open a bank account in your name). The higher the Grade the more certain you can be that the person is who they say they are. Grade 1 requires 50 points of evidence of identity, Grade 2, 100 points and Grade 3 (the highest grade) 150 points.

1.3.2 Dual Certificates

One Certificate can be used for multiple purposes (eg for signing correspondence, for encrypting information, or for authenticating oneself to gain access to a system). Dual Certificates are where the "Key Usage" Certificate extension (in the Certificate) is used to notify programs to restrict the functionality of a Certificate. The result is to split functionality between two Certificates. For most Gatekeeper certificates, one Certificate is used for authentication (the **Signing Certificate**) and the other for encryption (the **Encryption Certificate**). Each Certificate has its own Key Pair.

1.4 Key Pairs

A Key Pair is a pair of asymmetric cryptographic Keys (ie. one decrypts messages which have been encrypted using the other). One Key in the Key Pair is known as the Private Key and the other as the Public Key. The Private Key is only known to the Certificate user and must be kept private and secured by password or other protection. The Public Key on the other hand can be made widely known and indeed is embedded in the user's Certificate.

The Keys typically consist of 1024 bit prime numbers that are mathematically related.

When a person encrypts and sends a message using the Public Key of the recipient, only the recipient (who holds the Private Key) can read that message. When a message is sent signed using a person's Private Key, the person who receives the message can ascertain that the person who sent the message is who they say they are and that the message has not been altered in transit by checking it against that person's Public Key.

1.5 Trust Hierarchies

A trust hierarchy is a PKI that is established for a particular purpose and for particular people to use. There are many PKIs operated in the world today. Gatekeeper is the Government's mandated PKI. There are other PKIs for the banking industry (Identrus), for global trust of organisations operating on the internet (the VeriSign Trust Network or VTN), or even for an individual company's own internal purposes.

Each trust hierarchy may set its own rules for admission and to what extent certificates can be relied on. Based on these choices the level of trust one may place in certificates issued under that trust hierarchy will be set.

To determine whether to trust a Certificate you need to ascertain that you can trust the CA that issued that Certificate, and the CA that issued that CA Certificate, etc. The certificate at the top of the hierarchy is known as the Root Certification Authority (RCA).

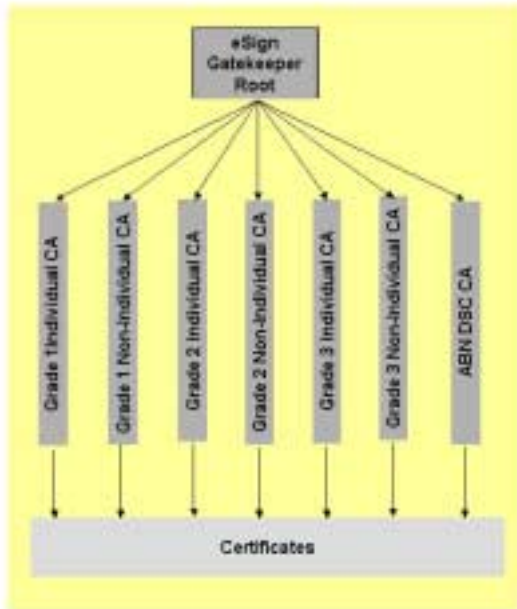
There are two main types of hierarchies: Public Hierarchies which are open to the general public (like Gatekeeper and the VTN) and Private Hierarchies which usually have restrictive entry requirements.

To participate in a Public Hierarchy you must adhere to the policies, procedures and standards defined by the hierarchy's governing body. In the case of the Gatekeeper hierarchy the governing body is the National Office of the Information Economy (NOIE). These policies cannot be changed for individuals or one member; there is only one set of rules that apply to all participants. The choice of a public hierarchy should be carefully considered and a total understanding of the requirements for membership obtained, prior to commitment, as some requirements may have a significant effect on business processes and interaction with the hierarchy.

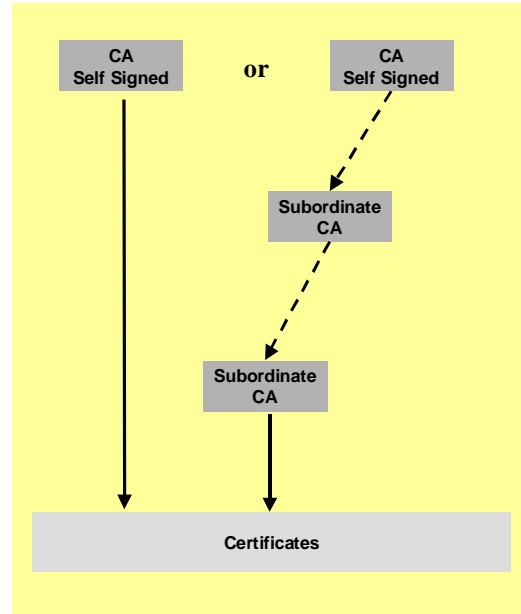
On the other hand under a Private Hierarchy an organisation has the ability to define their own policies, procedures and standards. This enables an organisation to support specific business and trust requirements. Private Hierarchies are trusted only within the organisation and not readily trusted in by the public. Typically a Private Hierarchy is used when there is a clearly defined closed user group for specific applications. For example secure intranet and extranet services would fall into this category.

The diagram below indicates VeriSign's Public Gatekeeper trust hierarchy and how Private Trust Hierarchies may be established.

VeriSign Gatekeeper Public Hierarchy



VeriSign Gatekeeper Private Hierarchy



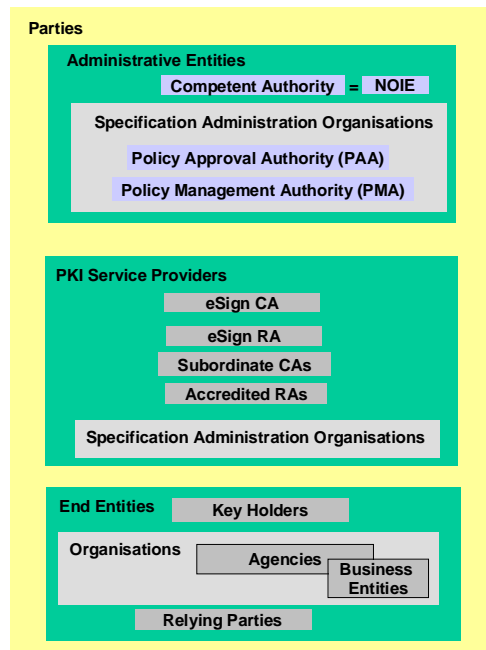
1.6 Subscribers

Subscribers are the people who are issued with Certificates and/or the organisation that has authorised the issuance of a certificate to that person. Ultimately if a problem results from using the Certificate the Subscriber will be the one who bears responsibility. For individual certificates that is the individual, for non-individual, ABN-DSC and device certificates that will be the organisation. Subscribers are required to agree to comply with the rules of the Trust Hierarchy. *See further Certificate Types below.*

1.7 PKI Entities

The following entities and roles exist in VeriSign’s Gatekeeper PKI.

Entities and Roles



The functions of each entity is summarised below:

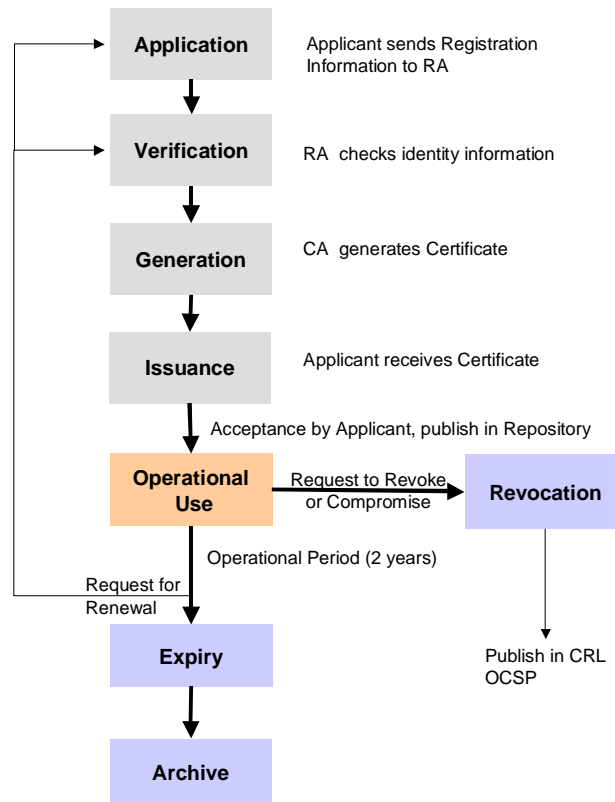
PKI Service Providers – the providers of services to End Entities	
eSign RA	The eSign RA verifies the information provided by Applicants for Certificates and then informs the eSign CA to generate and issue Certificates to the Applicant.
eSign CA	The eSign CA issues Certificates to Applicants once the Registration Authority has verified the identity of the Applicant.
eSign Gatekeeper Root (Root Certification Authority)	The self-signed certificate that identifies the eSign CA that is at the apex of trust of the eSign Public Gatekeeper Hierarchy. Subordinate CAs are signed by the eSign Gatekeeper Root.
Subordinate Certificate Authority (Subordinate CA)	An organisation that issues Certificates under its own name under VeriSign’s Gatekeeper hierarchy.
Registration Authority (RA)	An organisation that verifies the information provided by Applicants for Certificates.
End Entities – the user community	
Key Holders	People who have been issued with Certificates and Keys.
Subscribers	The people who are bound to follow the rules of the Trust Hierarchy by virtue of having a Certificate issued to them.

	virtue of having a Certificate issued to them.
Organisations	An organisation that has requested Certificates be issued to one or more Key Holders.
Agencies	An organisation that is a government entity.
Business Entities	Organisations that have an Australian Business Number (ABN).
Relying Parties	People who receive a message containing a Certificate who may want to rely on the contents of that message as being binding against the Key Holder.
Administrative Entities – the administrators of the scheme	
Competent Authority	The National Office of the Information Economy (NOIE) which oversees the Government’s Gatekeeper Strategy, including accrediting organisations to act as Certificate Authorities and Registration Authorities.
Specification Administration Organisations	Entities that are responsible for managing changes to accredited documents.
Policy Approval Authority (PAA)	A body comprising of eSign management that proposes changes to eSign’s Accredited Documents, which changes are subject to approval by the Competent Authority.
Policy Management Authority (PMA)	A body comprising of eSign personnel that oversees and manages compliance by eSign and Subordinate CAs with the CP and other Accredited Documents.

1.8 Certificate Life Cycle

Like a passport, there are various processes that are undertaken before a person is issued with a Certificate, and various other processes that occur after a Certificate has been issued. During the operational period of a Certificate the Certificate can be used for signing and encrypting data. The following is a diagrammatic representation of these main processes.

Certificate Lifecycle



2. Business Considerations

2.1 Purchasing Certificates

This information contains some information and considerations in choosing which Certificate is appropriate for your organisation. For up to date information regarding prices for Gatekeeper Certificates please see gatekeeper.verisign.com.au or contact us for volume purchase pricing.

The main consideration when buying Certificates is to determine what you want to achieve. You may be constrained in your choice by factors such as your technical environment or by your business partners.

2.1.1 Business Considerations

If you are buying Certificates to primarily deal with a particular party who now requires you to use a Gatekeeper Certificate to deal with them (eg to accept your electronically lodged tax return) you should ascertain whether they have particular requirements. For example, they may only accept a particular type of Certificate such as one that contains your ABN or even require a particular Grade of Certificate so they know that you have had to identify yourself to a certain standard.

Usually the business considerations will come out of the type of application that the business partner is providing. For example, minimal requirements may apply for providing access to public information, but more stringent requirements will apply before access is granted to tax or health records.

2.1.2 Technical Considerations

You should determine whether your mail client or IT environment can use the particular Certificate you are applying for. Some mail clients (and devices) may not support Dual Certificates.

Gatekeeper requires 1024 bit RSA encryption keys and 128 bit symmetric encryption keys, therefore certificate applicants must have browsers that are capable of supporting these encryption strengths. Older versions of browsers are not capable of supporting these requirements and will need to be upgraded prior to applying for a Gatekeeper certificate of any type. Most common mail clients will also need to be upgraded to take advantage of the higher encryption strengths.

You will need to obtain the certificate of the root CA to enable these certificates to be trusted by end user applications. VeriSign has already embedded its Gatekeeper root CA in the Microsoft browser. However, not all applications support this. Therefore, to enable the chain of trust within an end user application, such as a web browser or mail client, the Relying Party (recipient) may be required to import the appropriate root certificates into the application. This operation need only be performed once.

The eSign Gatekeeper Root Certificate can be found at gatekeeper.verisign.com.au.

The result of not importing the CA root certificates will be that the first time an end users application is required to validate a certificate (an example of this would be receiving a signed email) the user will be notified that the certificate is not valid. This does not mean that the certificate is not trusted, but this is an issue of setting up an organisation's Standard Operating Environment to cater for the implementation of all relevant CA root certificates within the user's environment.

2.1.3 Browser Versions

VeriSign strongly recommend that users upgrade to the latest browser versions to take advantage of their advanced security and certificate handling capabilities.

The minimum acceptable browser versions are:

- Microsoft Internet Explorer Version 4.1 – 128 bit encryption
- Netscape Navigator Version 4.1 – 128 bit encryption

2.1.4 Certificate Types

Certificate Type	Identifies	Responsibility	Sample Applications
Individual (Type 1)	The individual	The individual assumes responsibility and liability for key usage.	Personal transactions with a government agency <ul style="list-style-type: none"> • Claiming a benefit • Enrolling to vote • Lodging a personal tax return • Applying for a job
Non-Individual (Type 2)	The individual An organisation as a valid entity The individual as a person able to act on behalf of the organisation	The organisation assumes responsibility and liability for key usage.	<ul style="list-style-type: none"> • Business transactions • Purchasing on-line • Extranets for key suppliers
ABN-DSC	The individual An organisation as a valid entity The organisations right to use the associated ABN The individual is able to act on behalf of the entity with the ABN	The organisation assumes responsibility and liability for key usage.	Several people conducting electronic transactions on behalf of company <ul style="list-style-type: none"> • BAS lodgement • Lodging company tax returns • Ordering • Accounts payable • Customer relations • Regulatory forms
Device (Type 3)	An automated process or device An organisation as the owner/operator of the process/device	The organisation assumes responsibility and liability for key usage.	Signing company mail Signing receipts

2.1.4.1 Individual (Type 1)

Individual certificates are used by individuals who wish to identify themselves electronically to a Government agency or any organisation that will accept Gatekeeper certificates. The individual, also known as the key holder, is the only person identified in the certificate and therefore assumes sole responsibility for any and all transactions undertaken using the certificate's private key.

Typically these certificates will be used for personal transactions involving the delivery of government services; e.g. claiming benefits, enrolling to vote.

An individual must complete a "face to face" identification process by a Gatekeeper RA in order to obtain a Certificate. The individual will be required to show various forms of evidence of identity to secure a certificate.

For further information about Individual Certificates see our Individual Certificate Policy.

2.1.4.2 Non-Individual (Type 2)

Non-Individual certificates identify:

- An individual; and
- An organisation for which that individual works

The fact that an organisation has approved the Certificate to the individual means that, at least in some cases, the individual is authorised to act on behalf of the organisation.

Non-individual certificates place the responsibility for any and all transactions with the organisation.

Three grades of Non-Individual certificates are available and relate to the evidence of identity (EOI) points required during the face-to-face identification process.

In addition to the standard EOI documents, Non-individual certificates require that the applicant produce documentation identifying the organisation. This includes a statement by the requesting organisation nominating the individual as the authorised Key Holder and providing proof that the organisation exists.

For further information about Non-Individual Certificates see our Non Individual Certificate Policy.

2.1.4.3 ABN-DSC

The Australian Business Number Digital Signature Certificate (ABN – DSC) is a digital certificate linked to an entity's Australian Business Number (ABN). It has been designed to facilitate online service delivery and foster the use of digital certificates and e-commerce among Australian businesses.

ABN-DSCs identify:

- An organisation; and
- An authorised key holder acting on behalf of the organisation

As well as having the ABN in the Certificate, ABN-DSCs differ from Non-Individual Certificates in the process for issuing and managing those Certificates. An Organisation appoints one or more Authorised Officers who are entitled to act on behalf of the Organisation in relation to requests for Certificates. These Authorised Officers have to undergo a face to face identity check and provide 100 points of evidence of identity.

Authorised Officers then communicate to the CA to request further Certificates for individuals within the Organisation without the requirement that these applicants undergo a face to face (or any other kind of) identity check by the RA. The only verification performed on the applicant by the CA is to confirm that the Authorised Officer requested the person be issued with a Certificate.

The organisation takes full responsibility for the management of its ABN-DSCs. The organisation can set its own internal policies regarding who is to be issued with certificates are allocated, what delegations are held by holders of ABN-DSCs, how new certificates need to be issued or existing ones revoked.

ABN-DSCs are the easiest certificates to use and manage when an organisation has many staff.

For further information about ABN-DSC Certificates see our ABN-DSC Certificate Policy.

2.1.4.4 Device Certificates (Type 3)

Device certificates are specifically designed to be used in conjunction with a device or an automated process. For example, you may install a device certificate on a router to allow automated encryption of data to that router. Similarly, organisations may wish to have an application such as a service that provides online information (eg client statements, statements of entitlement, regular communications to business partners) to automatically sign documents using a device certificate on behalf of the organisation.

NOIE has developed a broad specification for device certificates. For further information about how a type 3 certificate will work with your particular device or application please contact us as we have experience in configuring devices and applications to use these certificates.

2.1.5 Applying for a Certificate

Below is the basic process for applying for a certificate that requires evidence of identity (EOI). Face-to-face identification is required for Individual, Non-Individual and ABN-DSCs that are to be issued to Authorised Officers.

The process varies slightly depending on the type of certificate. For example, once an Authorised Officer (for an ABN-DSC) has been issued with a certificate they may request additional ABN-DSCs for people working for that company by sending a signed and encrypted email authorising the person to be issued with a certificate.

Full details are contained on the gatekeeper web site (gatekeeper.verisign.com.au).

2.1.6 Process for Applying for a Certificate (other than an ABN-DSC)

1. Applicant enrolls via the web, prints the enrolment form, subscriber agreement and evidence of identity requirements.

2. Applicant attends at the RA location and presents:

- Evidence of Identity (EOI)
- Copies of EOI
- Enrolment form
- Subscriber Agreement

3. This is checked and certified by the RA that:

- Confirms supporting identification of entity
- Confirms details through third party sources if required

4. If all details are correct the RA informs the CA that it has performed the verification process and a certificate can be issued by the CA.

5. The CA issues the certificate.

6. The CA notifies the Applicant by email that the certificate has been issued and it is available for collection.

2.1.7 Information Verified

Not all information that will be placed in the Certificate is verified by the RA. For example the User defined OU field in the Subject Distinguished Name is non verified information provided by the Certificate owner at the time of registration. Similarly, the user's email address or entitlement to use that email address is not verified (although if the user does not have access to that email address they will not be able to pick up their certificate).

2.1.8 Other alternatives

If you determine that a Gatekeeper solution is not appropriate or too restrictive for your business application please contact us. As the most experienced operator of PKI services in the Australian we have a range of solutions that provide greater functionality to allow an organisation to effectively set itself up as a CA and determine its own verification requirements. We also have automated tools to accept applications based on specific criteria and that support roaming using certificates and the recovery of lost keys.

2.2 Using Certificates

Before implementing a solution using Gatekeeper certificates you will need to consider to what extent you wish to trust the various forms of certificates available. To make this decision you will need to understand the different identity verification processes undertaken for each certificate.

You will also need to consider whose Gatekeeper certificates you will accept, as there are other Gatekeeper accredited CAs beside VeriSign. Each of these CAs will have their own trust hierarchy and certificate format (although they all must be compliant with the standards mandated by NOIE).

2.2.1 Business Benefits

The main advantage in using Gatekeeper certificates is that you know that a set process has been followed that is designed to identify a person; you do not need to develop a special application process to ensure that you know who you are dealing with. There may be reasons why you wish to collect certain additional information from someone through a registration page.

To build organisational support for PKI you may have to demonstrate:

- Cost savings
- Improvements in efficiency
- Improvements in security and privacy

You may also be required to develop a business case to support the deployment of PKI. It must be remembered that PKI is an infrastructure that supports business applications. On its own, PKI does not provide any additional business application; it provides the ability to integrate confidentiality, integrity, authentication and non-repudiation into an

organisation's electronic business initiatives. Therefore an organisation must consider the applications and services it wishes to implement to take advantage of PKI and its associated benefits.

Identifying and documenting the desired business outcomes in advance will ensure the ultimate success of any project involving PKI and digital certificates.

2.2.2 Trust

PKI provides a foundation for trust. The level of trust associated with a specific PKI hierarchy or framework depends on the people, policies, procedures and standards that support it.

A gym membership card and a drivers licence are both used to identify an individual in different contexts. Both contain similar information: the individual's name, address, signature, and photograph. At face value the two seem to be equivalent. However, we place more value and a higher level of assurance on the drivers licence. This is due to several factors:

- There is a stringent process required to obtain a drivers licence
- Proof of your identity is needed to obtain a drivers licence
- Society has placed a certain level of trust in the issuing government authority, such as VicRoads in Victoria.

These factors combine to build trust in the drivers licence as an identity credential. On the other hand the gym membership card only indicates to us that the holder may be a member of a gym; minimal trust is associated with the card. The gym membership card is necessary and is fit for its purpose ie to provide access to the gym facilities.

It is the responsibility of organisations to determine what is an acceptable level of trust for their particular business needs. Business applications involving online transactions will demand different levels of trust to a secure email implementation.

The higher the level of trust that is required the more impact it will have on the business and on its policies and procedures. A trade-off will always occur between the trust provided and ease of use.

2.2.3 Trusting Certificates

If we are to trust someone presenting a certificate is who is identified in the Certificate we require to be reassured that the process of obtaining a certificate was done in a manner that could guarantee the end party identity. This is what an RA does.

2.2.4 Electronic Commerce

The Gatekeeper hierarchy establishes a base level of trust in certificates by establishing a Government controlled PKI. Organisations can build on this base level of trust to develop applications to participate in business and commerce in an electronic environment.

In order to better understand the requirements of secure electronic commerce it is helpful to first look at the five key requirements necessary for commerce to occur in the real world.

Requirement	Explanation	Example
Authentication	We must know who it is we are transacting with	Credit card contains the card holder's name and signature
Authorisation	We must know to what level the person is able to engage in a transaction	Credit limit of the card
Integrity	We must know that the transaction has not been modified in any way	Card holder is issued with a copy of the transaction receipt
Confidentiality	Contents of the transaction must only be known to those involved	Card receipts are transferred securely from the merchant to the bank
Non-Repudiation	Parties to the transaction must not be able to repudiate their involvement at a later date	Card holder signs the transaction receipt

These five requirements are also required for commerce to be undertaken in an electronic environment. Much like credit organisations, such as VISA have established a base level of trust in their cards, through a range of policies, procedures, legal agreements and practices, so too the Federal Government has established Gatekeeper to provide a base level of trust in digital certificates issued within the Gatekeeper framework.

The five requirements, in an electronic environment, can only be achieved through the deployment and management of PKI. Using Gatekeeper certificates will address many of the issues an organisation faces when creating a secure network or engaging in secure transactions.

The following are typical applications implemented using PKI:

Securing Web Applications – Certificates can be used in conjunction with Secure Sockets Layer (SSL) to provide authentication and communications encryption for web based applications and users.

Secure Mail and form signing – Provide the ability to ensure the information, which is the subject of the signature, has not been modified and also identifies the signer. Through identifying the signer, digital signatures provide non-repudiation. Digital signatures are used extensively in secure email systems (S/MIME).

Information Encryption – Information that has been encrypted using public key technology can only be decrypted and viewed by the intended recipients of the information, therefore ensuring the confidentiality of the information. Encryption is also used extensively in secure email systems.

Strong Authentication – For an end user to fully utilise PKI they must possess: a Certificate, the corresponding private key and the password that protects the private key. These requirements combine to provide strong “two-factor” authentication. The use of smart cards as a certificate and private key storage device provides an even higher level of security. This level of authentication compliments for usage within secure remote access mechanisms.

Secure Communications – Through the use of common security protocols such as Secure Sockets Layer and IP Security Protocol (IPSec), private communications can be transmitted across public networks, such as the internet, without fear of interception. IPSec is predominately used within Virtual Private Networks (VPNs), which can either be Client-to-Host or Host-to-Host.

A solid PKI implementation will enable an organisation to build other business applications, such as:

- Online tendering systems
- Dissemination of or access to sensitive information
- Securities trading
- Extranet access
- International money exchange

2.3 What PKI can not do

It is important to note what PKI does not provide to ensure that there are no misconceptions.

Business Applications: PKI provides infrastructure that supports confidentiality, integrity, authentication and non-repudiation. Applications that take advantage of these benefits must be developed in order to provide tangible business benefits.

Perfect Security Systems: The technology components of PKI, when viewed theoretically, provide extremely high levels of assurance. When introduced into an operational business environment it becomes susceptible to risks that cannot be accounted for within a theoretical environment. These risks include such things as:

- Fraud and other criminal or malicious activities
- System malfunctions and data corruption
- Breakdown in procedures
- Human error or incompetence

These risks must be identified and addressed through a combination of:

- Contingency and business continuity plans

- Risk mitigation strategies
- Insurance
- Policy, procedures and standards
- Education

Organisations should understand these risks prior to deploying PKI to ensure that the risks are commercially acceptable.

3. Technical Considerations

Many opportunities exist for developers to either develop applications that rely on certificates or assist Government agencies migrate their applications to use certificates. By using certificates you can take advantage of the investment people and organisations have already made in acquiring the credential.

3.1 Certificate Lifecycle

Unless otherwise revoked, Gatekeeper certificates are valid for two years after issuance. Further, if the current owner of the certificate wishes to renew their certificate (have another certificate issued in the same distinguished name) for a further period of two years, they may do so provided that they can prove they are in possession of the Private Key for the certificate and that they know the pass phrase initially used when applying for the certificate.

Two renewals of a certificate are allowed before a person must again undergo an evidence of identity check.

3.2 Certificate Validity Checking

It is necessary to check a Certificate or a digital signature created using a certificate is valid before acting on it. For example, you need to check that the Certificate has not expired and that it was not revoked (eg because someone has lost control of the certificate).

If you perform these checks and you are not aware of other circumstances why you can't rely on the certificate or digital signature you are entitled to rely on the fact that Certificate is used and operated by the person and organisation identified in the certificate.

Certificates offer a higher level of security and functionality than usernames and passwords. With so many different username/password combinations used today people tend to select duplicate passwords, easily remembered passwords or write down their passwords. All these events reduce the security offered by username and passwords and also affect an organisation's ability to rely on the fact that the person using the username and password is the person who originally registered.

There are three methods of checking the status of VeriSign's Gatekeeper certificates. Two use a certificate revocation list (CRL) and one uses an online certificate status protocol (OCSP) responder.

The three methods available to check certificates are:

- make a request of the OCSP responder
- access the CRL made available on the VeriSign Gatekeeper website (gatekeeper.verisign.com.au) by means of an http file request (eg by means of a web browser)
- access the CRL by means of a LDAP query.

3.2.1 Certificate Revocation List (CRL)

A CRL is a list of certificates that have been revoked prior to their expiration dates. VeriSign issues CRLs on a scheduled basis (typically nightly or hourly) and digitally signs them to ensure integrity and authenticity. CRLs include the certificate serial numbers and the times and reasons for revocation. End-user applications should download the latest copy of the CRL when they need to validate a certificate. Provisions are made for CRL timestamp-checking and downloading of partial CRLs to minimise the network traffic required to perform revocation-checking.

The LDAP directory server makes available the CRL (and certificates) through means of a properly formed LDAP query.

VeriSign provides CRLs with daily updates for all of the CAs that it creates. This service is provided free of charge.

The hourly CRL update service is a premium validation service for which a fee applies.

3.2.2 Online Certificate Status Protocol (OCSP)

OCSP enables users and applications to determine the status (valid, revoked, suspended, expired, or unknown) of a particular certificate in real time. In practice, an end-user application implements an OCSP client that issues a status

request to an OCSP responder at VeriSign. The client suspends acceptance of the certificate until the responder sends a response (digitally signed by VeriSign) indicating the certificate's validity status.

Because OCSP determines only the status of the certificate, the application program must still verify that the end user represented by the certificate has proper authorisation to access the resource. Using our OCSP API toolkit, a developer can create an application that sends an OCSP request for certificate status to VeriSign's OCSP responder, whenever an end user requests access to protected web sites or other resources. If the OCSP responder indicates that the certificate is valid, the application determines whether the user presenting the certificate is allowed access to the resource. If the response is revoked, suspended, expired or unknown, the application denies access to the resource.

VeriSign's OCSP service presents some advantage over basic CRL-checking:

1. There is no need to store CRLs.
2. An application that encounters certificates from multiple CAs must store at least one CRL for each CA.
3. OCSP can be configured to log all OCSP transactions and provide a report of these transactions to the certificate administrator.
4. OCSP services enable the certificate administrator to suspend a certificate as an alternative to revocation. A suspended certificate appears as a revoked certificate to an OCSP request, and does not appear in a CRL. Unlike a revoked certificate, a suspended certificate can be returned to valid status.

3.2.3 Further information

There are obvious business benefits in having automated certificate validity checking and getting the most up to date information available. Accordingly, we strongly recommend using the OCSP responder to ascertain certificate revocation information as CRLs can be up to 24 hours out of date.

In either case you will need to know where to find the appropriate CRL, OCSP responder or LDAP directory. This information can be obtained from the certificate itself in the "CRL Distribution Point" field. *See section 3.4 below for an example.*

DEWR (the Department of Workplace Relations) is developing a system which will be made available to Government to enable Government to make an enquiry of one system to determine the status of a certificate. It will effectively aggregate certificate information for multiple certificates and multiple CAs. Current indications are that this will not be made available to the private sector.

3.2.4 Process

Validation of a certificate or digital signature is performed by applications following this process:

- 1. Check that the certificate is valid** – This involves checking that the current date is between the certificate's valid from and valid to fields. If the Certificate is outside of these dates it has expired, and no-one can rely on the Certificate as binding the certificate owner.
- 2. Establishing a Certificate chain for the Certificate used to sign the information** – In the case of a Public Hierarchy this involves confirming that the CA who issued the Certificate is a Subordinate CA of the RCA. In the case of a Private Hierarchy it involves confirming that the CA who issued the Certificate is trusted by the Relying Party.
- 3. Checking the Repository for Revocation of Certificates in this Chain** – The Relying Party must determine if any of the Certificates along the chain from the signer to an acceptable root within the eSign Gatekeeper PKI has been Revoked, because a revocation has the effect of prematurely terminating the operational period during which verifiable digital signatures can be created. This may be ascertained by querying the CRL or OCSP responder to determine whether any Certificates in the Certificate chain have been revoked.

At this stage the Certificate has been validated (eg if you were using presentment of the Certificate to gain secure web access), however that does not mean that the signed message sent has not been altered. To do this you need to complete the last two steps.

- 4. Applying the hash function to the signed data** – Apply the same hash function as was originally applied by the signer.
- 5. Compare the hash functions** – If the value created by step 4 is the same as the value appended to the signed information, then the information is validated and the same as that sent originally.

3.3 Certificate Repository

VeriSign's Gatekeeper repository, gatekeeper.verisign.com.au/repository, contains publicly available information regarding certificates including:

- all the policy documents;
- information how to revoke a certificate;
- information on how to check the validity of a certificate;
- a publicly available directory of certificates issued.

The directory provided is a searchable LDAP directory. Internet users can query this directory for a particular user and obtain their certificate. Once obtained this certificate can be used to send encrypted messages to the owner of that certificate.

3.4 Parsing Certificate Information

All Certificates have a particular format and information content. This information is set out either in the Certificate Policy (for certificates issued to end users) or the Certification Practice Statement (for certificates issued to the CA). In each case section 7 of that document will contain the certificate format and content information.

Knowing this format allows you to extract information from the certificate. For example to ascertain the name of the person applying for a Certificate, the CA that has issued the certificate, where to go to look up information about whether the certificate has been revoked, the operational period of the certificate and the public key of the certificate owner.

Below is the Certificate Profile for ABN-DSC Certificates (Signing Certificate and Encryption Certificate).

There are several noteworthy points.

The information that identifies the owner/user of the certificate in an ABN-DSC is contained in the Subject Distinguished Name (the person's information, employer and location), the Subject Alt Name (the email address of the certificate owner) and the Private Extension for the ABN-DSC (the ABN number of the organisation). With this information one can implement a database to determine access based on these attributes.

Allowance has been made in the first OU field in the Subject Distinguished Name for user defined data to be entered that is not verified by the RA (for example information to allow access to a particular application or general information that a certificate owner enters during the certificate application process). We suggest that in general reliance is not made on information contained in the user defined field as this information is not checked or restricted. Further, another organisation may also make use of this field which could lead to confusion. Instead we suggest implementing a database routine that stores access privileges or other information relevant to the application against the subject distinguished name.

Type	Value
Subject Distinguished Name	E = rsmith@xyz.com.au CN = Richard Smith OU = user defined OU = XYZ Employee O = XYZ Ltd L = Melbourne S = Vic C = AU
Issuer Distinguished Name	CN = Gatekeeper Grade 2 ABN-DSC CA OU = Gatekeeper PKI OU = Terms of use at https://www.esign.com.au/GKRPA/ O = eSign Australia
Version	3
Serial Number	Serial number value
Signature Algorithm	md5 RSA
Public Key	min RSA 1024 bit key
Valid From	dd/mm/yy hh/mm/ss
Valid To	dd/mm/yy hh/mm/ss
Basic Constraints	CA: FALSE Max Path Len: N/A (critical)
Key Usage	[For Signing Certificate] DigitalSignature, NonRepudiation (critical) [For Encryption Certificate] KeyEncipherment, DataEncipherment (critical)
Certificate Policies	OID: 1.2.36.88021603.333.2.2 (Certificate Policy) OID: 1.3.6.1.5.5.7.2.1 (Policy Qualifier) https://www.esign.com.au/GKRPA/
Netscape Cert Type	OID 2.16.840.1.113730.1.1 Value 03 02 07 80
Private Extension (ABNDSC)	OID 1.2.36.1.333.1 Value <ABN number (IA5 String)>
CRL Distribution Point	URL= http://onsitecrl.esign.com.au/GatekeeperABNDSCCA/LatestCRL.crl URL=ldap://directory.esign.com.au/cn=Gatekeeper ABN-DSC CA,ou=Terms of use at https://www.esign.com.au/GKRPA/,ou=Gatekeeper PKI,o=eSign Australia?certificaterevocationlist;binary
Authority Information Access	OID 1.3.6.1.5.5.7.48.1 (Online Certificate Status Protocol) URL=https://ocsp.esign.com.au
Subject Alt Name	RFC822 Name=rsmith@xyz.com.au
Subject Key Identifier	Set (sha1 hash of Public Key)
Authority Key Identifier	Set (sha1 hash of issuer's Public Key)
Thumbprint algorithm	sha1
Thumbprint	Thumbprint value

3.5 Backup and Archival of Keys and Certificates

An organisation may wish to back up their users' Encryption Certificate (and obtain the Private Key for this certificate). Without this, if the user leaves the organisation or loses their certificate it may not be possible to view messages (eg historical messages) that were encrypted to the user. This can present problems complying with requirements to produce documents or obtain information that may have been sent to the individual. Similarly an individual may wish to back up their own certificate and Private Keys because if they are lost it will not be able to access private information that was intended for the recipient.

The Signing Certificate on the other hand does not need to be backed up as if it is lost another certificate can be obtained to sign documents. The important thing here is that the certificate is revoked so that it is not possible for another to use that certificate.

4. Further information

4.1 Policy Documents

Each organisation that achieves Gatekeeper accreditation is required to develop policy documents that describe in detail how it ensures trust and security.

These policy documents are reviewed by NOIE and its accredited evaluators (including ASIO, DSD and AGS) against NOIE's accreditation criteria (see www.noie.gov.au).

Further, in our case we are also audited by an external audit firm that performs a Webtrust audit which is specifically tailored to examining the practices and procedures of an organisation providing PKI services.

Some of the policy documents are not publicly available as they contain detail that is unnecessary for others to know, or could be used to reverse engineer or circumvent security safeguards.

Various documents describe different aspects of what we do. Your starting point should always be the Certificate Policy for the type of Certificate you are interested in, or if you want to know details about how VeriSign operates its own CA, the Certificate Practices Statement.

Here is a brief explanation of our policy documents. All these documents are available from our website gatekeeper.verisign.com.au.

Document	Content
Glossary	Contains information about defined terms and key concepts used in all our Gatekeeper documents.
Subscriber Agreements	Summarise the responsibilities of people who are issued with Certificates. Separate Subscriber Agreements exist for: <ul style="list-style-type: none"> • Individual Certificates – Individual Subscriber Agreement; • Non-Individual Certificates – Non-Individual Subscriber Agreement; and • Australian Business Number – Digital Signature Certificates (ABN-DSCs) – ABN-DSC Subscriber Agreement.
CPS (Certification Practices Statement)	A statement of the practices which a Certification Authority employs in issuing Certificates (eg Gatekeeper Certificates). The eSign Gatekeeper CPS describes the operational practices of VeriSign in relation to its Gatekeeper services and is published in the Repository.
CP (Certificate Policy)	A set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements. For example, a particular Certificate Policy might indicate applicability of a type of certificate to the authentication of electronic transactions with a particular Commonwealth agency or Government transactions up to a certain financial value. <p>VeriSign has three CPs which can be viewed and downloaded from the Repository:</p> <ul style="list-style-type: none"> • the eSign Gatekeeper Individual CP • the eSign Gatekeeper Non-Individual CP; and • the eSign Gatekeeper ABN-DSC CP.
Relying Party Agreement	The agreement between a person who wishes to rely on an eSign issued Gatekeeper Certificate and the other Parties.
Repository	The location gatekeeper.verisign.com.au/repository at which can be found a copy of all our publicly available policy documents.

4.2 How do I quickly find the information I need in the CP/CPS?

The CPS and the CP have been written to follow the format set out in RFC2527 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, the established standard for drafting of CPSs and CPs. The RFC2527 format has eight sections:

1. **Introduction** – this contains a general overview of the contents of the document and the PKI Entities involved.

-
2. **General Provisions** – relates primarily to obligations of the PKI Entities and legal issues including liability and IP.
 3. **Identification and Authentication** – how people apply for certificates and the checks on Certificate Applicants that are conducted.
 4. **Operational Requirements** – how the CA and RA operates such as how it issues certificates and when it suspends and revokes them.
 5. **Physical, Procedural and Personnel Security Controls** – the controls applied by the CA and RA in relation to their physical infrastructure, procedures and personnel to ensure security.
 6. **Technical Security Controls** – details regarding key management, the generation and protection of Private Keys.
 7. **Certificate and CRL profiles** – the format of Certificates and the information that must be included in a Certificate and CRL.
 8. **Specification Administration** – the change management process for changes to the operation of the PKI.

4.3 Why are there so many documents?

Gatekeeper is meant to establish a public hierarchy, where the rules and procedures that the participants followed are revealed for all to see. Accordingly, there are a number of documents often covering the same area with different levels of detail. Most users will never need to refer to these documents once they understand how the PKI works. Some of the material covered in these documents is beyond the interest of a majority of users.

4.4 Further Reading

The NOIE website: www.noie.gov.au

The following NOIE publications:

Trusting the Internet - A small business guide to E-security. The guide is aimed at helping Australian small and medium businesses understand the key issues of Internet security. Businesses need to be aware of security issues when they are browsing a website, sending emails, conducting e-commerce transactions, dealing with government agencies online and conducting e-business activities. 16/7/02 [Browse Report](#)

Online Authentication - A guide for Government Managers. The Minister for Communications, Information Technology and the Arts released an Online Authentication guide for Government Managers. It provides agencies with advice and guidance on key issues to consider when implementing authentication solutions in their e-business strategies. 16/7/02. [Browse Report](#)

4.5 Suggestions

If you have suggestions or corrections you believe should be made to this document please email them to us at support@verisign.com.au.