GLOSSARY

The Glossary applies to the following documents:

1. VeriSign Gatekeeper ABN-DSC CP
2. VeriSign Gatekeeper Individual CP
3. VeriSign Gatekeeper Non-Individual CP
4. VeriSign Gatekeeper CPS
5. VeriSign Gatekeeper Type 3 CP
6. VeriSign Gatekeeper Type 3 Host CP

In these documents, the following capitalised words and phrases have the following meanings unless a contrary intention is evident:

Term	Definition
ABN-DSC Subscriber Agreement	VeriSign's Approved Document of that name which sets out key responsibilities of the Subscriber in relation to an ABN-DSC, and associated Keys.
Accept (a Certificate)	The process whereby a Certificate Applicant demonstrates his/her approval of a Certificate and its informational contents, in accordance with the relevant CP.
Administrative Entities	The Competent Authority, the PAA and the PMA.
Agency	A Department of State, or a Department of the Parliament, of the Commonwealth or a State or a Territory; or 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); or A body established by the Governor-General, a State Governor, or a minister of State of the Commonwealth, a State of a Territory; or An incorporated company over which the Commonwealth, a State or Territory exercises control.
Applicant	Is the person who has applied to be issued with a Certificate and associated Private Keys, prior to the time at which the Keys and Certificate are Issued to and Accepted by the person.
Application	A request from an Applicant for a Certificate and associated Private Keys to be Issued to the Applicant.
Approved Documents	Means the following documents: Documents that are publicly available in the Repository: • this document • VeriSign Gatekeeper ABN-DSC CP • VeriSign Gatekeeper Individual CP • VeriSign Gatekeeper Non-Individual CP • VeriSign Gatekeeper Certification Practice Statement (CPS) • VeriSign ABN-DSC Subscriber Agreement • VeriSign Individual Subscriber Agreement • VeriSign Non-Individual Subscriber Agreement • VeriSign Relying Party Agreement

Term	Definition
	• VeriSign Security Policy Documents that are not publicly available: • VeriSign Concept of Operations • VeriSign Protective Security Risk Review • VeriSign Protective Security Plan • VeriSign CA Operations Manual • VeriSign RA Operations Manual • VeriSign Key Management Plan • VeriSign Disaster Recovery and Business Continuity Plan
Australian Business Number – Digital Signature Certificate (ABN-DSC)	A Certificate that identifies an individual with an associated entity that has an ABN, as more fully described in the VeriSign Gatekeeper ABN-DSC CP.
Australian Business Number (ABN)	The Australian Business Number (ABN) is a single identifier used primarily for dealings between a Business Entity and the Australian Taxation Office, and for dealings with other government agencies.
Australian Business Register (ABR)	The Australian Business Register contains all the publicly available information provided by businesses when they register for an Australian Business Number (ABN). The Australian Business Register is established under s.24 of the A New Tax System (Australian Business Number) Act 1999.
Authorised Officer	In the context of an ABN-DSC Certificate is an individual authorised by his or her Organisation to perform the functions described in **section 3.1.11.2** of the VeriSign Gatekeeper ABN-DSC CP. In the context of a Type 3 Certificate is the individual authorised by his or her Organisation to perform the functions described in **section 3.1.11.2** of the VeriSign Gatekeeper ABN-DSC CP and **section 3.1.11.2** of the VeriSign Gatekeeper Type 3 CP.
Business Entity	An entity entitled to have an ABN within the meaning of s.8 of the A New Tax System (Australian Business Number) Act 1999 (Cth).
CA	See Certification Authority.
CA Operations Manual	VeriSign's Approved Document of that name which describes in greater detail than the VeriSign Gatekeeper CPS how VeriSign operates its CAs.
CEO, NOIE	The Chief Executive Officer of the National Office for the Information Economy.
Certificate	A set of information which at a minimum: (a) identifies the Certification Authority who issued the Certificate; (b) names or identifies the person and/or organisation to whom the Certificate was issued; (c) contains the public key issued to the person and/or organisation to whom the Certificate was issued; is digitally signed by the Certificate Authority who issued the Certificate; and conforms with a Certificate profile.
Certificate Chain	The chain of CAs constituted by the CA listed as the issuer in the Certificate Profile and all superior CAs (CAs who have signed the Certificate of the Subordinate CA). In a Public Hierarchy the Certificate Chain will begin with the CA who Issued the Certificate to the Key Holder and end in the VGR.
Certificate Directory	The published directory containing all Gatekeeper Certificates issued by the VeriSign CA. The Certificate Directory for all VeriSign CA issued Gatekeeper Certificates can be found at the VeriSign Gatekeeper Website http://www.verisign.com.au/gatekeeper
Certificate Extension	A field in a Certificate that is not defined in Amendment 1 to ISO/IEC 9594-8:1995 (X.509).
Certificate Grade	Means a specified level of trust (eg grade 1, 2 or 3) as described in the

Term	Definition
	relevant Certificate Policy. The grade relates to the extent to which the identity of the Subscriber is Verified (and can therefore be trusted). Grade 3 is the highest level of trust.
Certificate Information	Information needed to complete a Certificate as required by the Certificate Profile.
Certificate Policy (CP)	A named 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 Certificate Type to the authentication of electronic transactions with a particular Agency or Government transactions up to a certain financial value. VeriSign has a number of CPs which can be viewed and downloaded from the Repository, for example: • the VeriSign Gatekeeper Individual CP • the VeriSign Gatekeeper Non-Individual CP; and • the VeriSign Gatekeeper ABN-DSC CP. • the VeriSign Gatekeeper Type 3 CP.
Certificate Profile	The specification of the fields to be included in a Certificate and the contents of each, as set out in **section 7.1** of the relevant Certificate Policy.
Certificate Revocation List (CRL)	A list of Revoked Certificates. The CRL may form part of the Certificate Directory or may be published separately. The Certificate Extension field named "CRL Distribution Point" specifies the address at which the CRL for a Certificate is published.
Certificate Signing Request (CSR)	A request from a person generating Keys, for a CA to generate a Certificate and sign that Certificate.
Certificate Type	Means an Individual Gatekeeper Certificate, a Non-Individual Gatekeeper Certificate, an ABN Digital Signature Certificate (ABN-DSC) or other type of Certificate.
Certification Authority (CA)	Means an entity which signs and issues Certificates. In the VeriSign Public and Private Gatekeeper hierarchies, the CAs are the VeriSign Gatekeeper Root, the VeriSign CA, Subordinate CAs and Hosted CAs. The VGR, the VeriSign CA and Subordinate CAs are operated by VeriSign Australia Pty Ltd.
Certification Practice Statement (CPS)	A statement of the practices that a Certification Authority employs in issuing Certificates (eg Gatekeeper Certificates). The VeriSign Gatekeeper CPS describes the operational practices of VeriSign in relation to its CA and RA services and is published in the Repository.
Challenge Phrase	A set of numbers and/or letters that are chosen by an Applicant, communicated to the CA with an Application, and used by the CA to authenticate the Key Holder for specific purposes set out in the VeriSign Gatekeeper CPS or the relevant Certificate Policy (such as to determine the Key Holder's ability to Renew or Revoke a Certificate).
Commonwealth	The Commonwealth of Australia, including the Competent Authority and the evaluators and auditors appointed by the Competent Authority that are subject to the Financial Management and Accountability Act 1997 or the Commonwealth Authorities and Companies Act 1997, and includes their employees, servants and agents.
Commonwealth Protective Security Manual	The Commonwealth manual which sets out the policies, practices and procedures that must be put in place by Agencies to provide a protective security environment in which to conduct their activities, and in particular, to protect their information, personnel and assets.
Community of Interest	The group of entities who are eligible to apply for the issue of Certificates as specified in the relevant CP.
Competent Authority	The entity which approves the VeriSign CA and RA's infrastructure and practices (including the Approved Documents and any changes to them) as meeting the criteria for Gatekeeper Accreditation. The Competent Authority

Term	Definition
	for this PKI is AGIMO, Finance.
Compromise	A violation of the security of a system such that unauthorised disclosure of sensitive information may have occurred, e.g. if there has been unauthorised access to the Cryptographic Module in which a Private Key is stored or used, or unauthorised access to or loss or theft of media on which the Private Key is stored.
Concept of Operations	VeriSign's Approved Document which provides an overview of VeriSign's CA and RA operations.
Confidential Information	Information which by its nature is confidential and which the Party holding the information knows or should know is confidential.
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 the Public Key embedded in the Certificate corresponds to the Private Key.
CP	*See Certificate Policy.*
CPS	*See Certification Practices Statement.*
CRL	See Certificate Revocation List.
Cryptographic Module	A Cryptographic Module is hardware, software or firmware or any combination of them which uses Cryptography to protect the information stored therein.
Cryptography	(a) The mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and Key. (b) A discipline that embodies the principles, means, and methods for transforming data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorised use.
Device	Software (eg an application such as an automated software process) or hardware (eg a router) on which a Certificate may be installed.
Device (Type 3) Certificate	A Certificate that identifies an application, Device, process or service that is owned, operated or controlled by an Organisation.
Digital Signature	An electronic signature created using a Private Key (and specifically in the case of Dual Key Pairs, the Private Key of the Signing Certificate) consisting of data appended to, or a Cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.
DigitalSignature Bit	The digitalSignature Bit is a data flag in the "key usage" extension in a Certificate that is used to identify that the Certificate can be used for signing communications (but not other Certificates or CRLs). Digital signature mechanisms are often used for entity authentication and data origin authentication with integrity.
Disaster Recovery and Business Continuity Plan	VeriSign's Approved Document which sets out VeriSign's disaster recovery and business continuity plans.
Distinguished Name	A unique identifier of a person or thing having the structure required by the relevant Certificate Profile. A Distinguished Name is assigned to each Subscriber.
DSD	Defence Signals Directorate. The Australian national authority for information security.
Encryption Certificate	A Certificate that has the "Key Usage" Certificate Extension set to enable it to be used to encrypt messages.
End Entity	Subscribers and Relying Parties.
EOI	See Evidence of Identity.
EPL	See Evaluated Product List.
Escrow	Escrow is the process of entrusting material (for example a Key) to a third party (such as an Organisation or government) ('**Escrow Agent**') and providing another third party with a legal right to obtain the material from the Escrow Agent in certain circumstances.

Term	Definition
eSign	eSign Gatekeeper Services is a business name owned by VeriSign Australia Pty Ltd (ABN 88 088 021 603).
Evaluated Product	A hardware or software product that is on the EPL.
Evaluated Product List (EPL)	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: (1) AISEP criteria E1 to E6; or (2) Common Criteria EAL1 to EAL4, with an additional review of Cryptography by DSD. The EPL is published at http://www.dsd.gov.au.
Evidence of identity	Evidence to a particular level of the identity or truth of a particular person or thing.
Expiration Date	The time and date stated in a Certificate as the end of the Operational Period, after which the Certificate will expire.
Expiry (of a Certificate)	When the current date passes the Expiration Date, a Certificate is said to have expired.
Force Majeure	A circumstance beyond the reasonable control of a Party which results in the Party being unable to observe or perform on time one or more of its obligations, such circumstances including but not limited to: (a) acts of God, lightening strikes, earthquakes, floods, storms, explosions, fires and any natural disaster; (b) acts of war, acts of public enemies, terrorism, riots, civil commotion, malicious damage, sabotage and revolution; and (c) strikes (other than by the Party's personnel).
Gatekeeper	The Commonwealth Government strategy for the use of Public Key Technology in the delivery of Commonwealth Government services and in all business dealings with Commonwealth Agencies.
Gatekeeper Accreditation	Accreditation by the CEO, NOIE, granted on the basis that: (a) in the case of a CA – the CA meets the criteria set out in the Gatekeeper Criteria for Accreditation of Certificate Authorities; or; (b) in the case of a RA – the RA meets the Gatekeeper Criteria for Accreditation of Registration Authorities. The Gatekeeper Accreditation process involves: (a) an examination of the ability of the applicant to protect the privacy of Key Holder's Personal Information; (b) an examination of the financial viability of the applicant as part of that entity obtaining endorsement under the Endorsed Supplier Arrangements administered by the Commonwealth Department of Finance and Administration; and (c) evaluation of the Approved Documents. Accreditation is granted by the CEO, NOIE once the evaluation of the applicant's operation has been successfully completed.
Gatekeeper Report	Gatekeeper: A strategy for public key technology use in the Government published by the Office for Government Information Technology – now NOIE. Also available at http://www.noie.gov.au.
Highly Protected	A protective marking and a level of security clearance as defined in the Commonwealth Protective Security Manual. This level of security clearance is higher than In-Confidence.
Hosted CA	A hosted CA is a CA that VeriSign operates for and on behalf of another Gatekeeper accredited CA. In the case of a hosted CA, VeriSign provides the infrastructure to enable a hosted CA to control the Certificate issuing process for their customers. The Gatekeeper accredited CA can determine its own policies (including certificate policies) and procedures for managing certificates although these must be consistent with those employed by VeriSign in so far as VeriSign provides the infrastructure.
In-Confidence	A protective marking and a level of security clearance as defined in the Commonwealth Protective Security Manual.
Individual (Type 1)	A Certificate that identifies an individual only as its Subject with no

Term	Definition
Certificate	associated entity, as more fully described in the VeriSign Gatekeeper Individual CP.
Individual Subscriber Agreement	VeriSign's Approved Document which summarises the obligations and responsibilities of a Subscriber who has been issued with an Individual Certificate.
Information Privacy Principles	Means the principles set out at section 14 of the *Privacy Act 1988*.
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.
Issue (a Certificate)	A process whereby the CA, based on the Registration Information, generates a Certificate and distributes this to the Key Holder (or in the case of a Type 3 Certificate, to the person or Device authorised by the Organisation).
Key	A data element used to encrypt or decrypt a message – includes both Public Keys and Private Keys. A sequence of symbols that controls the operation of a Cryptographic transformation (eg. encipherment, decipherment, Cryptographic check function computation, signature generation, or signature authentication).
Key Holder	An individual (including the Authorised Officer) who holds and uses Keys or Certificates on behalf of themselves or an Organisation.
Key Management Plan	VeriSign's Approved Document titled "Cryptographic Security Policy" which sets out the technical security controls on the generation, distribution and use of the VeriSign CA Key Pairs.
Key Pair	A pair of asymmetric cryptographic Keys (ie. one decrypts messages which have been encrypted using the other) consisting of a Public Key and a Private Key.
Multi Person Control	Multi Person Control is a method of guarding against the risk that the integrity of the PKI could be compromised by misuse of a Key by, for example, splitting a Key into parts and giving different parts to different individuals. A minimum number of parts (which may be less than the total number) is required to fully reconstitute the Key, but having less than the minimum number of parts gives no information about the Key.
Finance (formerly NOIE)	Means the Commonwealth Department of Finance and Administration
Non-Individual (Type 2) Certificate	A Certificate that identifies an individual and the Organisation on whose behalf the individual acts, as more fully described in the VeriSign Gatekeeper Non-Individual CP.
Non-Individual Subscriber Agreement	VeriSign's Approved Document which summarises the obligations and responsibilities of a Subscriber (Key Holder and an Organisation) that has been issued with a Non Individual Certificate.
Non-Verified Subscriber Information (NSI)	Information submitted by an Applicant, and included within a Certificate, which has not been confirmed by an RA and for which the RA and CA provides no assurances other than that the information was submitted by the Applicant. Information such as titles, professional degrees, accreditations are considered NSI unless otherwise indicated.
Object Identifier (OID)	A number that identifies a particular document or thing. Australian Standard MP 59-2000 describes the standard that applies to the allocation of OIDs in Australia.
OCSP	Online Certificate Status Protocol. A protocol to enable real time checking of the validity of a Certificate (ie whether it is during the Operational Period of the Certificate and the Certificate has not been Revoked).
OID	See Object Identifier.
Operational Period	The operative period of the Certificate, as can be determined from the

Term	Definition
	Certificate (being the time between the 'Valid From' and 'Valid To' fields), unless it is earlier Suspended or Revoked.
Organisation	A non-individual entity (eg company, trust, partnership, charitable organisation, association, Agency etc).
Personal Information	Has the meaning given to that term in the Privacy Act 1988 (Cth), that is "information or an opinion (including information or opinion forming part of a database) whether true or not, and whether recorded in a material form or not, about a natural person whose identity is apparent, or can reasonably be ascertained, from the information or opinion."
PKI	See Public Key Infrastructure.
PKI Entity	The VGR, the VeriSign CA, Subordinate CAs, Hosted CAs, RAs, Subscribers, Relying Parties and the entity which provides Repository services (if it is not one of these entities).
PKI Service Provider	Any entity other than an End Entity. PKI Service Providers include the Specification Administration Organisations, the VGR, Subordinate CAs, Hosted CAs and RAs.
Policy Approval Authority (PAA)	The Authority which proposes changes to a CP and other Approved Documents, which changes are subject to approval by the Competent Authority. The PAA comprises members of VeriSign senior management.
Policy Management Authority (PMA)	The Authority which oversees and manages compliance by the CAs and RAs with the relevant CP and other Approved Documents, and is made up of VeriSign's Operations Manager, Security Manager, Engineering Services Manager and Key Manager.
Position of Trust	A role or responsibility which is sensitive requiring the person performing that role or responsibility to be highly trustworthy. Specific roles that are Positions of Trust are set out in the Protective Security Plan and include such roles as the system administrator, system security officer, and system auditor.
Private Key	The half of a Key Pair which must be kept secret to ensure confidentiality, integrity, authenticity and non-repudiation of messages.
Protective Security Plan	Comprises the following Approved Documents: the Physical Security Plan, the Information Systems Security Plan, the Trusted Employee Policy, the Tour Policy, and the Threat and Risk Assessment). These set out appropriate network security controls for VeriSign's systems (including firewalls) and specifies appropriate system as well as development controls for VeriSign's and Subordinate Entities' systems, including: (a) use of the trusted computing base concept; (b) discretionary access control; (c) labels; (d) mandatory access controls; (e) object reuse; (f) audit; (g) identification and authentication; (h) trusted path; (i) security testing; (j) penetration testing; (k) product assurance; (l) security controls in relation to the development environment, development facility and development personnel; (m) controls in relation to: a. configuration management security during product maintenance; b. software engineering practices; and c. software development methodology; (n) use of failsafe design and implementation techniques; and (o) use of trusted products and systems that have been Gatekeeper evaluated. (p) execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools

Term	Definition
	and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.
Protective Security Risk Review	A process initially undertaken by DSD which evaluated the threats and risks associated with VeriSign operating as an Accredited CA and RA. VeriSign maintains a threat and risk assessment document which is updated on a regular basis which sets out security controls implemented by VeriSign and safeguards to secure VeriSign's operations.
Public Key	The half of a Key Pair which may be made public, and is published in the Certificate.
Public Key Infrastructure (PKI)	The combination of hardware, software, people, policies and procedures needed to create, manage, store, distribute and revoke Public Key Certificates based on public key Cryptography.
Public Signing Key	The Public Key of the Encryption Certificate used to Verify a Digital Signature.
RA	See Registration Authority.
RA Operations Manual	VeriSign's Approved Document which sets out in greater detail the operations of the VeriSign RA.
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). RAs may have other functions or obligations specified in the relevant CP. The contact details for each RA (including physical address, postal address, email and facsimile) will be published in the Repository.
Registration Information	Information about Applicants which is required for the issue and use of Certificates, including: In relation to Individual Certificates – information needed to verify the identity of the Applicant; In relation to Non-Individual Certificates and ABN-DSCs – information needed to verify the identity of the Key Holder and Organisation, and to confirm that the Key Holder is authorised to use a Certificate on behalf of the Organisation.
Relevant RA	Means the Gatekeeper Accredited RA that is performing the relevant RA functions. This may be: the VeriSign RA; or another entity that has been granted Gatekeeper Accreditation to act as a Registration Authority.
Relying Party	A person who acts in reliance on a Certificate and/or Digital Signature(s) Validated using that Certificate.
Relying Party Agreement	VeriSign's Approved Document which summarises the obligations and responsibilities of a Relying Party.
Renew (a Certificate)	The process whereby a new Certificate is issued to a Key Holder at the end of the Operational Period of a Certificate.
Repository	The section on the VeriSign Gatekeeper Website, at which can be found a copy of all VeriSign's Gatekeeper Approved Certificate Policies, CPS, Subscriber Agreements, Relying Party Agreement and other documentation currently located at: https://www.verisign.com.au/repository/gatekeeper/
Revoke (a Certificate)	To terminate the effectiveness of a Certificate before the end of the scheduled Operational Period of a Certificate.
Security Policy	VeriSign's Approved Document which sets out its various policies and procedures that relate to security of its premises and infrastructure.
Signer	A person who affixes their Digital Signature to information to enable a third party to confirm that the information was sent by them.
Signing Certificate	A Certificate that has the "Key Usage" Certificate Extension set to enable it to be used to apply a Digital Signature.
Specification	The PAA and the PMA.

Term	Definition
Administration Organisation	
Subject	The subject as identified in the "Subject" field in a Certificate. The Subject must contain a distinguished name identifying the Certificate.
Subordinate CAs	A Subordinate CA is an entity owned and operated by VeriSign, either for the purposes of issuing Certificates under a Public Gatekeeper Hierarchy or issuing Certificates on behalf of a customer under the Private Gatekeeper Hierarchy. Subordinate CAs Issue, Suspend, and Revoke Certificates. All Subordinate CAs within the VeriSign Public Gatekeeper PKI are subordinate to the VeriSign Gatekeeper Root eg all VeriSign CAs. A Hosted CA is also a Subordinate CA.
Subscriber	The person named in the Subject field in a Certificate and who has Accepted that Certificate. Prior to Accepting a Certificate, the Subject is referred to as an Applicant. In relation to Non-Individual Certificates and ABN-DSCs, the Subscriber includes both the individual Key Holder and his or her Organisation. In relation to Type 3 Certificates, the Subscriber includes both the Authorised Officer and the Organisation on whose behalf the Device is operated.
Subscriber Agreement	An agreement between a Subscriber and VeriSign in relation to the responsibilities of the Subscriber. Separate Subscriber Agreements exist for: • Individual Certificates – Individual Subscriber Agreement; • Non-Individual Certificates – Non-Individual Subscriber Agreement; • ABN-DSCs – ABN-DSC Subscriber Agreement; and • Type 3 Certificates – Type 3 Subscriber Agreement. A Subscriber Agreement is a user-friendly form of the relevant obligations, responsibilities and liabilities of the Subscriber and VeriSign. It incorporates by reference the CP under which the Subscriber's Certificate has been issued.
Suspend (a Certificate)	To temporarily suspend the effectiveness of a Certificate before the end of the Operational Period of a Certificate.
Time Stamp	A Time Stamp is a record that indicates (at least) the correct date and time of an action (expressly or implicitly) and the identity of the person or device that created the notation. The VeriSign CA uses time stamps that reflect Greenwich mean time (GMT) and adopt the Universal Time Conventions (UTC). Any two-digit year in the range 00-69 means 2000-2069, and in the range 70-99 means 1970-1999.
Trustworthy Systems	In relation to PKI Service Providers - Systems which meet the system security requirements of the Approved Documents. In relation to End Entities - computer hardware, software, and procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability and correct operation; (c) are reasonably suited to performing their intended functions; and (d) adhere to generally accepted security procedures. In relation to Key generation, it is recommended that Subscribers use products from the Evaluated Products List.
Type 1 Certificate	*See Individual Certificate.*
Type 2 Certificate	*See Non-Individual Certificate.*
Type 3 Certificate	*See Device Certificate.*
Type 3 Subscriber Agreement	VeriSign's Approved Document which summarises the obligations and responsibilities of a Subscriber who has been issued with a Type 3 Certificate.
Validate	The process that must be undertaken by a Relying Party to determine whether they may rely on a Certificate (and associated information) that involves checking that: (a) the Digital Signature was created by the Private Key Corresponding

Term	Definition
	to the Public Key listed in the Certificate of the person affixing their Digital Signature to the information; and (b) the associated information has not been altered since the Digital Signature was created. See further **section 2.1.4.1** of the relevant CP.
Verify	The process whereby the identity of a person or thing or relationship is confirmed by reference to external documentation.
VeriSign	VeriSign Australia Pty Ltd (ABN 88 088 021 603) of Level 5, 6-10 O'Connell St, Sydney, NSW 2000, Australia.
VeriSign (Gatekeeper) ABN-DSC CP	VeriSign's Approved Document which is the Certificate Policy applying to ABN-DSCs.
VeriSign (Gatekeeper) Individual CP	VeriSign's Approved Document which is the Certificate Policy applying to VeriSign's Individual Gatekeeper Certificates.
VeriSign (Gatekeeper) Non-Individual CP	VeriSign's Approved Document which is the Certificate Policy applying to VeriSign's Non-Individual Gatekeeper Certificates.
VeriSign (Gatekeeper) Type 3 CP	VeriSign's Approved Document which is the Certificate Policy applying to Type 3 Certificates.
VeriSign Gatekeeper Certification Practices Statement (CPS)	VeriSign's Approved Document which is the Certification Practices Statement applying to all Gatekeeper Certificate Types and Certificate Grades issued by the VeriSign CA, Subordinate CAs or Hosted CAs. In a Private Hierarchy, certain provisions of the VeriSign Certification Practices Statement may be altered to meet the needs of the organisation for which the Private Hierarchy is established.
VeriSign Gatekeeper Root (VGR)	The VeriSign Gatekeeper Root is a VeriSign owned and operated entity that Issues Certificates for Subordinate CAs that are part of VeriSign's Public Gatekeeper PKI. The VGR approves the Distinguished Names of public Subordinate CAs and serves as the apex of trust within the VeriSign Public Gatekeeper PKI. Each Subordinate CA within the VeriSign Public Gatekeeper PKI has its Certificate signed by its superior CA.
VeriSign Gatekeeper Website	VeriSign's web site at which it provides information relating to its Gatekeeper Services (http://www.verisign.com.au/gatekeeper/) or the website that replaces that website from time to time.
VeriSign Private (Gatekeeper) Hierarchy	A PKI created by VeriSign to meet the requirements of an Agency or other customer. An VeriSign Private Gatekeeper Hierarchy generally uses the same infrastructure and practices as the VeriSign Gatekeeper Public Hierarchy but may have additional rules and limitations on the use of Certificates as set out in the relevant CP. Certificates issued under a Private Gatekeeper Hierarchy will not have a Certificate Chain ending in the VeriSign Gatekeeper Root.
VeriSign Public (Gatekeeper) Hierarchy	A PKI established by VeriSign and accredited under Gatekeeper, as defined in the VeriSign Gatekeeper CPS and relevant CPs. Certificates issued under this hierarchy will have a Certificate Chain that ends in the VeriSign Gatekeeper Root.
VGR	See VeriSign Gatekeeper Root.

2. In any document to which this Glossary applies, unless the contrary intention is evident:

(a) words importing a gender include any other gender;
(b) the singular includes the plural and vice versa;
(c) headings and notes (including headnotes, footnotes, endnotes and marginal notes) are for convenient reference only and have no effect in limiting or extending the language of the provisions to which they refer;

(d) words importing persons include a partnership and a body whether corporate or otherwise; and

(e) where any word or phrase is given a defined meaning, any other part of speech or other grammatical form in respect of that word or phrase has a corresponding meaning.