DoE CA

Certification Practice Statement

Document Identifier	Digital Certification Procedures Statement 2.1.docx
Document ID	
Document Author	Irga, Bill
Version No.	2.1 Final
Status	Final
Version Date	1 September 2015 10:36 AM
Source	DoE ITD
Copyright	NSW Department of Education 2015

Contents

Document Control

Document Acceptance

	Distributed List		
Name/Title	**Version**	**Role (Approve / Endorse)**	**Date**
Philip Sherwin, Senior Manager Enterprise Architecture	1.2	Endorse	29 Oct 2013
Dave Smith, Manager Directory Services	1.4	Endorse	1 May 2014
Malcolm Desmarchelier, R/Director, Service Delivery and Support	2.0	Approve	11/12/2014
Scott Thomson, Director Service Delivery and Support	2.1	Approve	28 Aug 2015

Revision History

Reviewer	Date	Version	Comments
Bill Irga`	21/08/2015	2.1	Changed organisation name to Depertemnt of Education and updated sections 4.2, 5.7.1 and 7.1.6

Review History

Reviewer	Date	Version	Comments

Referenced Documents

Title	Version	Document Location
Globalsign CA CPS Template	2.0a	ISU network share

Inclusions

Item	Description
1	
2	

Exclusions

Item	Description
1	
2	

Acknowledgments

This DOE CA CPS endorses in whole or in part the following industry standards:

- RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.

This CPS is created according to the requirements of the following schemes and endorses these in whole or in part:

- AICPA/CICA, WebTrust 2.0 Program for Certification Authorities.
- AICPA/CICA, WebTrust For Certification Authorities – Extended Validation Audit Criteria.
- CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

1 Introduction

This Certification Practice Statement (CPS) applies to the products and services of NSW Department of Education (DoE). Primarily this pertains to the issuance and lifecycle management of Certificates including validity checking services. This CPS may be updated from time to time as outlined in Section 1.5 *Policy Administration*. The latest version may be found on the following URL http://www.dec.nsw.gov.au/footer/digital-certificate-authority.

A CPS highlights the *"procedures under which a Digital Certificate is issued to a particular community and/or class of application with common security requirements"*. This CPS meets the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, dated November 2003 with regard to content, layout and format *(RFC 3647 obsoletes RFC 2527).* An RFC issued by IETF is an authoritative source of guidance with regard to standard practices in the area of electronic signatures and Certificate management. While certain section titles are included in this CP according to the structure of RFC 3647, the topic may not necessarily apply to Services of DOE CA. These sections state *'No stipulation'*. Where necessary, additional information is presented in subsections to the standard structure. Meeting the format requirements of RFC 3647 enhances and facilitates the mapping and interoperability with other third party CAs and provides Relying Parties with advance notice of DoE practices and procedures. Additional assertions on standards used in this CPS can be found under section *"Acknowledgements"* on the previous page.

This CPS is final and binding between DoE, a NSW Government Department, with registered office at 35 Bridge St, Sydney NSW Australia, (Hereinafter referred to as "DOE CA")

and

the Subscriber and/or Relying Party, who uses, relies upon or attempts to rely upon certification services made available by the Certification Authority referring to this CPS.

This CPS addresses the technical, procedural and personnel policies and practices of the DOE CA during the complete life cycle of Certificates issued by the DOE CA.

The DOE CA operates within the scope of activities of DoE. This CPS addresses the requirements of the CA that issues Certificates of various types under the Certificate Policy of GlobalSign nv-sa and its Trusted Root Program. The chaining to any particular Issuing CA may well vary depending on the choice of intermediate Certificate and/or Cross Certificate used or provided by a platform or client.

For Subscribers, this CPS becomes effective and binding by accepting a Subscriber Agreement or Terms of Use. For Relying Parties, this CPS becomes binding by relying upon a Certificate issued under this CPS. In addition, Subscribers are required by the Subscriber Agreement to inform their Relying Parties that the CPS is itself binding toward those Relying Parties.

1.1 Overview

This CPS applies to the complete hierarchy of Certificates issued by DOE CA. The purpose of this CPS is to present the practices and procedures in managing Certificates and to demonstrate compliance with requirements pertaining to the issuance of Certificates according to DOE CA's own and industry requirements pursuant to the standards set out above. This CPS aims at facilitating the DOE CA in delivering certification services and managing the Certificate lifecycle of any issued client, server and other-purpose end entity Certificates. The Certificate types addressed in this CPS are the following:

SMIME/Client Authentication	A personal certificate of medium assurance with

	reference to professional context
SMIME/Client Authentication (Department)	A role certificate of medium assurance with reference to a professional context
SSL/TLS	A certificate to authenticate web servers

These Certificates shall be issued and managed in accordance with CA/Browser Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (the "Baseline Requirements"). An indication of compliance is the inclusion of CA/Browser Forum Policy OIDs as detailed in Section 1.2.

DOE CA Certificates:

- Can be used for digital signatures in order to replace handwritten signatures where transacting parties choose for them
- Can be used for encryption of data
- Can be used to authenticate web resources, such as servers and other devices

This CPS identifies the roles, responsibilities and practices of all entities involved in the lifecycle, use, reliance upon and management of DOE CA Certificates. The provisions of this CPS with regard to practices, level of services, responsibilities and liability bind all parties involved, including DOE CA, their nominated RA, Subscribers and Relying Parties. Certain provisions might also apply to other entities such as the certification service provider, application provider etc.

A GlobalSign Certificate Policy (CP) complements this CPS. The purpose of the GlobalSign CP is to state the *"what is to be adhered to"* and, therefore, set out an operational rule framework for the broad range of GlobalSign products and services. The latest version of the CP governing this CPS can be found on https://www.globalsign.com/repository

This CPS states *"how the Certification Authority adheres to the Certificate Policy".* In doing so, this CPS features a greater amount of detail and provides the end user with an overview of the processes, procedures and conditions that the DOE CA uses in creating and maintaining the Certificates that it manages. In addition to this CPS DOE CA maintains additional documented polices addressing such issues as:

- Business continuity and disaster recovery
- Security policy
- Personnel policies
- Key management policies
- Registration procedures

A Subscriber or Relying Party of a Certificate must refer to this CPS in order to establish trust in a Certificate issued by DOE CA as well as for information about the prevailing practices of DOE CA. It is also essential to establish the trustworthiness of the entire Certificate chain of the hierarchy. This includes the Root CA Certificate as well as any operational Certificates. This can be established on the basis of the assertions within this CPS.

1.1.1 Certificate Naming

The exact names of the DOE CA Certificates that make use of this CPS are:

- NSW-DEC-ISS-CA1 with serial number `357d5ae709f8465a4b4cacfeec869a3d3e`

Certificates allow entities that participate in an electronic transaction to prove their identity to other participants or sign data digitally. By means of a Certificate, DOE CA provides confirmation of the relationship between a named entity (Subscriber) and its Public Key. The process to obtain a Certificate includes the identification, naming, authentication and registration of the Subscriber as well as aspects of Certificate management such as the issuance, revocation and expiration of the Certificate. By means of this procedure to issue Certificates, DOE CA provides adequate and positive confirmation about the identity of the user of a Certificate and a positive link to the Public Key that the Subscriber uses. DOE CA makes available Certificates that can be used for non-repudiation, encryption and authentication.

1.2 Document Name and Identification

This document is the DOE CA Certification Practice Statement.

The OID for DoE (DOE CA) is a 1.2.36.1.1.1. DOE CA organises its OID arcs for the various certificates and documents described in this CPS (Which may be updated from time to time) as follows:

1.2.36.1.1.1.1.7	SMIME Client Authentication Policy
1.2.36.1.1.1.1.1	SSL/TLS Policy

The OID for GlobalSign nv-sa (GlobalSign CA) is an iso (1) identified-organisation (3) dod (6) internet (1) private (4) enterprise (1) GlobalSign nv-sa (4146). GlobalSign CA organises its OID arcs for the various Certificates and documents described in its CP as follows:

1.3.6.1.4.1.4146.1.60	CA Chaining Policy – Trusted Root

In addition to these identifiers, all Certificates that comply with the Baseline Requirements will include the following additional identifiers:-

2.23.140.1.2.2	Organization Validation Certificates Policy

1.3 PKI participants

1.3.1 Certification Authorities

DOE CA is a Certification Authority (CA) that issues trusted Certificates in accordance with this CPS. As a Certification Authority, DOE CA performs functions related to Certificate lifecycle management such as Subscriber registration, Certificate issuance, Certificate renewal, Certificate distribution and Certificate revocation. DOE CA also provides Certificate status information using an online repository in the form of a Certificate Revocation List (CRL) distribution point and/or Online Certificate Status Protocol (OCSP) responder.

DOE CA ensures the availability of all services pertaining to the management of Certificates, including without limitation the issuing, revocation and status verification of a Certificate, as they may become

available or required in specific applications. DOE CA also manages a core online registration system and assorted API's for all Certificate types issued under DOE CA Subordinate/Issuing CAs

1.3.2 Registration Authorities

In addition to identifying and authenticating Applicants for Certificates. A Registration Authority (RA) may also initiate or pass along revocation requests for Certificates and requests for reissuance and renewal (sometimes referred to as re-key) of Certificates. DOE CAs may act as a Registration Authority for Certificates it issues in which case they are responsible for:

- Accepting, evaluating, approving or rejecting the registration of Certificate applications;
- Registering Subscribers for certification services;
- Providing systems to facilitate the identification of Subscribers (according to the type of Certificate requested);
- Using officially notarised or otherwise authorised documents or sources of information to evaluate and authenticate an Applicant's application;
- Requesting issuance of a Certificate via a multifactor authentication process following approval of an application; and

  Initiating the process to revoke a Certificate from the applicable GlobalSign subordinate Issuing CA

1.3.3 Subscribers

Subscribers to DOE CA are either Legal Entities or natural persons that successfully apply for and receive a Certificate to support their use in transactions, communications and the application of Digital Signatures.

A Subscriber, as used herein, refers to both the Subject of the Certificate and the entity that contracted with the DOE CA for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an Applicant.

Legal Entities are identified on the basis of the published by-laws and appointment of director as well as the subsequent government gazette or similar official government publication or other Qualified Independent Information Source (QIIS) or Qualified Government Information Source (QGIS) third party databases. Self-employed Subjects are identified on the basis of proof of professional registration supplied by the competent authority in the Country in which they reside.

For all categories of Subscribers, additional credentials are required as explained in the online process for the application for a Certificate.

Subscribers of end entity Certificates issued under the DOE CA include employees and agents involved in day-to-day activities within GlobalSign that require access to GlobalSign network resources. Subscribers are also sometimes operational or legal owners of signature creation devices that are issued for the purpose of generating a Key Pair and storing a Certificate.

1.3.4 Relying Parties

To verify the validity of a Certificate, Relying Parties must always refer to DOE CA's revocation information either in the form of a CRL distribution point or an OCSP responder.

1.3.5 Other Participants

DOE CA is cross signed by GlobalSign nv-sa via its Trusted Root program as detailed within the GlobalSign CP on https://www.globalsign.com/repository

1.4 Certificate Usage

A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transactions. Certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1 Appropriate certificate usage

End entity Certificate use is restricted by using Certificate extensions on key usage and extended key usage. Certificates issued by DOE CA can be used for public domain transactions that require:

- **Non-repudiation:** A party cannot deny having engaged in the transaction or having sent the electronic message.
- **Authentication:** The assurance to one entity that another entity is who he/she/it claims to be.
- **Confidentiality:** The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended.
- **Integrity:** The assurance to an entity that data has not been altered intentionally or unintentionally) from sender to recipient and from time of transmission to time of receipt.

Digital signature: Digital (Electronic) signature can only be used for specific transactions that support digital signing of electronic forms, electronic documents, or electronic mail. The Certificate is only warranted to produce Digital Signatures in the context of applications that support Certificates. Certificates that are appropriate for Digital Signatures are the following:

- SMIME/Client Authentication**:** authentication of a natural person (medium level assurance)
- SMIME/Client Authentication (Department) **:** authentication of a natural person within an organisational context or a role within an organisational context (medium level assurance)

Authentication (Users): User authentication Certificates can be used for specific electronic authentication transactions that support accessing web sites and other online content, electronic mail, etc. The authentication function of a Certificate can be ascertained in any transaction context for the purpose of authenticating the end user Subscriber to a Certificate. To describe the function of authentication, the term Digital Signature is often used.

- SMIME/Client Authentication**:** authentication of a natural person (medium level assurance)
- SMIME/Client Authentication (Department) **:** authentication of a natural person within an organizational context or a role within an organizational context (medium level assurance)

Authentication (Devices and objects): Device authentication Certificates can be used for specific electronic authentication transactions that support the identification of web sites and other on line

resources, such as software objects. The authentication function of a Certificate can be ascertained in any transaction context with the purpose of authenticating a device that the Subscriber seeks to secure through a Certificate. To describe the function of authentication, the term Digital Signature is often used.

- SSL/TLS: authentication of a remote Domain Name and associated organisational context and webservice and encryption of the communication channel
- SMIME/Client Authentication: authentication of a natural person (medium level assurance)
- SMIME/Client Authentication (Department) : authentication of a natural person within an organisational context or a role within an organisational context (medium level assurance)

Assurance levels: Subscribers should choose an appropriate level of assurance to which Relying Parties will confidently transact. For example, Subscribers with an unknown brand name should positively assure Relying Parties of their identity with a high assurance (EV) certificate where as a closed community with a well-known URL may chose a low assurance option.

- **Low assurance:** (Class 1) Certificates are not suitable for identity verification as no authenticated identity information is included within the Certificate. These Certificates do not support non-repudiation.
- **Medium assurance:** (Class 2) Certificates are individual and organisational Certificates that are suitable for securing some inter- and intra-organisational, commercial, and personal email requiring a medium level of assurances of the Subject identity contained within the Certificate.
- **High assurance:** (Class 3) Certificates are individual and organisational Certificates that provide a high level of assurance of the identity of the Subject in comparison with Class 1 and 2.

Confidentiality: All Certificate types can be used to ensure the confidentiality of communications effected by means of Certificates. Confidentiality may apply to business and personal communications as well as personal data protection and privacy.

Any other use of a Certificate is not supported by this CPS. When using a Certificate the functions of electronic signature (non-repudiation) and authentication (Digital Signature) are permitted together within the same Certificate. The different terms relate to different terminologies used by IETF and the vocabulary adopted within the legal framework of the European Union Directive 1999/93/EC (a community framework on electronic signatures).

1.4.2 Prohibited certificate usage

Certificate use is restricted by using Certificate extensions on key usage and extended key usage. Any usage of the Certificate inconsistent with these extensions is not authorised.

Certificates issued under this CPS do not guarantee that the Subject is trustworthy, operating a reputable business or that the equipment into which the Certificate has been installed is not free from defect, malware or virus.

Certificates issued under this CPS may not be used:-

- for any application requiring fail safe performance such as
    - the operation of nuclear power facilities
    - air traffic control systems
    - aircraft navigation systems
    - weapons control systems
    - any other system whose failure could lead to injury, death or environmental damage; or
- where prohibited by law.

1.4.2.1 Certificate extensions

Certificate extensions comply with X.509 v.3 standards.

- SSL/TLS: Client and Server Authentication EKU
- SMIME/Client Authentication: Client Authentication and Secure email EKU
- SMIME/Client Authentication (Department): Client Authentication and Secure email EKU

1.4.2.2 Critical Extensions

DOE CA also uses certain critical extensions in the Certificates it issues such as:

- A basic constraint in the key usage to show whether a Certificate is meant as a CA or not;
- To show the intended usage of the key; and
- To show the number of levels in the hierarchy under a CA Certificate.

1.5 Statement Administration

1.5.1 Organisation Administering the Document

Request for information on the compliance of Issuing CAs with accreditation schemes as well as any other inquiry associated with this CPS can be addressed to:

DoE's Information Security Unit at information.security@det.nsw.edu.au

1.5.2 Contact Person

Bill Irga, Information Security Officer, Information Technology Directorate, Departmeny of Education

1.5.3 Person Determining CPS Suitability for the Statement

Bill Irga, Information Security Officer

1.5.4 CPS Approval Procedures

The CPS will be prepared by the DoE Information Security Unit.

Approval to publish will be the responsibility of the Director Service Delivery and Support, DoE ITD. (DOC15/662245)

1.5.4.1 Changes with notification

Updated versions of this CPS are notified to parties that have a legal right to receive such updates, for example, auditors with a specific mandate.

1.5.4.2 Version management and denoting changes

Changes are denoted through new version numbers for the CPS. New versions are indicated with an integer number followed by one decimal that is zero. Minor changes are indicated through one decimal number that is larger than zero. Minor changes include:

- Minor editorial corrections
- Changes to contact details

1.6 Definitions

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Legal Entity is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate Request.

Application Software Supplier: A supplier of Internet browser software or other Relying Party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Identity Information is correct.

Audit Criteria: The requirements described in this document and any requirements that an entity must follow in order to satisfy the audit scheme selected under section 16.1.

CDS (Certified Document Services): A document signing architecture created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 6.0.

Certificate: An electronic document that uses a Digital Signature to bind a Public Key and an identity.

Certificate Beneficiaries: The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate, all Application Software Suppliers with whom GlobalSign CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier, and all Relying Parties who reasonably rely on a Valid Certificate.

Certificate Data: Certificate Requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Request: Communications described in Section 10 requesting the issuance of a Certificate.

Certificate Revocation List: A regularly updated timestamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Compromise: A violation of a security policy that results in loss of control over sensitive information.

Country: Either a member of the United Nations OR a geographic region recognized as a sovereign nation by at least two UN member nations.

Cross Certificate: A certificate that is used to establish a trust relationship between two Root CAs.

Digital Signature: To encode a message by using an asymmetric cryptosystem and a Hash function such that a person having the initial message and the signer's Public Key can accurately determine whether the transformation was created using the Private Key that corresponds to the signer's Public Key and whether the initial message has been altered since the transformation was made.

Domain Authorization: Correspondence or other documentation provided by a Domain Name Registrant attesting to the authority of an Applicant to request a certificate for a specific Domain Namespace.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Domain Name System: An Internet service that translates Domain Names into IP addresses.

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a Country, or political subdivision within such Country (such as a state, province, city, county, etc.).

Hash (e.g. SHA1 or SHA256): An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:

- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.
- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

Hardware Security Module (HSM): An HSM is type of secure crypto processor targeted at managing digital keys, accelerating crypto processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications.

Internal Server Name: A server name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Incorporate by Reference: To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.

Independent Audit: An audit that is performed by a Qualified Auditor and that determines an entity's compliance with the Baseline Requirements and one or more of the audit schemes listed in Section 17.1 of the Baseline Requirements

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a Country's legal system.

Object Identifier (OID): A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables Relying Party application software to determine the status of an identified Certificate. See also OCSP Responder.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure (PKI): A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2 (Identity/ Qualifications of Assessor).

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the Certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such supplier merely displays information relating to a Certificate.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the Baseline Requirements when the Applicant/Subscriber is an Affiliate of the CA.

Trusted Platform Module (TPM): A hardware cryptographic device which is defined by the Trusted Computing Group. https://www.trustedcomputinggroup.org/specs/TPM.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialists: Someone who performs the information verification duties specified by the Baselines Requirements.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

WebTrust Program for CAs: The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities.

WebTrust Seal of Assurance: An affirmation of compliance resulting from the WebTrust Program for CAs.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

X.509: The standard of the ITU-T (International Telecommunications Union-T) for Certificates

1.2 Acronyms

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
ETSI	European Telecommunications Standards Institute
FIPS	(US Government) Federal Information Processing Standard

FQDN	Fully Qualified Domain Name
GSCA	GlobalSign Certification Authority
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ISO	International Standards organisation
ITU	International Telecommunications Union
LRA	Local Registration Authority
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VAT	Value Added Tax
VOIP	Voice Over Internet Protocol

2.0 Publication and Repository Responsibilities

2.1 Repositories

DOE CA publishes all CA Certificates revocation data for issued Certificates, CPS, and any Relying Party agreements or Subscriber Agreements in Repositories. DOE CA ensures that revocation data for issued Certificates is available through a Repository 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled downtime that does not exceed 0.5% annually.

DOE CA may publish submitted information on publicly accessible directories for the provision of Certificate status information.

DOE CA refrains from making publicly available sensitive and/or confidential documentation including security controls, operating procedures, and internal security policies. These documents are, however, made available to Qualified Auditors as required during any WebTrust or ETSI audit performed on GlobalSign CA.

2.2 Publication of Certificate Information

DOE CA publishes its CPS, Subscriber Agreements, Relying Party agreements on the following URL http://www.dec.nsw.gov.au/footer/digital-certificate-authority. CRLs are published in Repositories. The CRLs contain entries for all revoked un-expired Certificates with a validity period that depends on Certificate type and/or position of the Certificate within the Certificate chain.

2.3 Time or Frequency of Publication

Delta CRLs for end user Certificates are issued every 24 hours. CRLs for CA Certificates are issued at least every 6 months and within 24 hours if a CA Certificate is revoked. Each CRL includes a monotonically increasing sequence number for each CRL issued.

New or modified versions of this CPS, Subscriber Agreements, or Relying Party agreements are published within seven days.

2.4 Access control on repositories

ITD Directories team (MaD) maintain access control of CA repositories.

- Multi-factor authentication has been implemented for access to CA repositories.
- Trusted roles have been created for management of CA PKI.

3.0 Identification and Authentication

DOE CA acts as an RA that verifies and authenticates the identity and/or other attributes of an Applicant and that the Applicant is either a subsidiary or parent of DOE CA.

Applicants are prohibited from using names in their Certificate that infringe upon the intellectual property rights of others.

RAs authenticate the requests of parties wishing to revoke Certificates.

3.1 Naming

3.1.1 Types of Names

DOE CA Certificates are issued with subject DNs (Distinguished Names) which meet the requirements of X.500 naming, RFC-822 naming and X.400 naming. CNs (Common Names) respect name space uniqueness and are not misleading.

Non wildcard SSL Certificates are issued with a Fully Qualified Domain Name (FQDN).

Wildcard SSL Certificates **must** first be approved by DoE Security Unit.

Wildcard SSL Certificates include a wildcard asterisk character. Before issuing a Certificate with a wildcard character (*) DOE CA follows best practices to determine if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix”. (e.g. “*.com.au”, “*.edu.au”, see RFC 6454 Section 8.2 for further explanation.) and if it does, it will reject the request as the Domain Namespace must be owned or controlled by the Subscriber. e.g. *.globalsign.com

In the case of SSL Certificates, whilst the FQDN or authenticated domain name is placed in the Common Name (CN) attribute of the Subject field, it **must** be duplicated into the Subject Alternative Name extension along with a www version of the DNS-ID. Subject Alternative Names are marked non critical in accordance with RFC5280.

3.1.2 Need for Names to be Meaningful

Where possible, DOE CA uses distinguished names to identify both the Subject and the Issuing CA of a Certificate. In cases where a DOE CA product allows the use of role or departmental name then additional unique elements may be added to the DN within the OU field to allow differentiation between Certificates with common DN elements by Relying Parties.

3.1.3 Anonymity or Pseudonymity of Subscribers

DOE CAs may issue end entity anonymous or pseudonymous Certificates provided that such Certificates are not prohibited by applicable policy and where possible name space uniqueness is preserved. DOE CA reserves the right to disclose the identity of the Subscriber if required by law.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished names in Certificates are interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in Certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5 Uniqueness of Names

DOE CA enforces the uniqueness of each Subject name in a Certificate as follows.

- SSL/TLS: A Domain Name within the Common Name attribute as approved as unique by ICANN.

• SMIME/Client Authentication:	A unique email address coupled with an organisation's name and address plus either the name of an individual or a department associated with the organisation.
• SMIME/Client Authentication (Department):	A unique email address coupled with an organisation's name and address plus either the name of an individual or a department associated with the organisation..

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers may not request Certificates with any content that infringes the intellectual property rights of another entity. DOE CA does not require that an Applicant's right to use a trademark be verified. DOE CA reserves the right to revoke any Certificate that is part of a dispute.

3.2 Initial Identity Validation

DOE CA may perform identification of the Applicant using any legal means of communication or investigation necessary to identify the Legal Entity or individual.

3.2.1 Method to Prove Possession of Private Key

Subscribers must prove possession of the Private Key corresponding to the Public Key being registered either as a Certificate Signing Request (CSR) in PKCS#10 format or as a Signed Public Key and Challenge (SPKAC).

3.2.2 Authentication of Organisation Identity

For all Certificates that include an organisation identity, Applicants are required to indicate the organisation's name and registered or trading address. For all Certificates, the legal existence, legal name, legal form and requested address of the organisation is verified using one of the following:

- A government agency in the jurisdiction of the Applicant;
- A third party database that is periodically updated and has been evaluated by GlobalSign to determine that it is reasonably accurate and reliable; or
- An attestation letter confirming that Subject Identity Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

The authority of the Applicant to request a Certificate on behalf of the organisation is verified in accordance with Section 3.2.5 below.

For SSL/TLS Certificates, the Applicant's ownership or control of all requested Domain Name(s) is authenticated by one of the following methods;

- Using GlobalSign's OneClickSSL protocol whereby the Applicant is required to demonstrate control of a Domain Name by installing a non publicly trusted test Certificate of GlobalSign's specification;
- By uploading specific metadata to a defined page on the domain;
- By direct confirmation with the contact listed by the Domain Name Registrar in the WHOIS record;
- By successfully replying to a challenge response email sent to one or more of the following email addresses:
    - webmaster@domain.com, postmaster@domain, admin@domain.com, administrator@domain.com, hostmaster@domain, or
    - any e-mail address listed as a contact field of the WHOIS record, or
    - any address previously used for the successful validation of the control of the domain subject to the re-verification requirements of Section 3.3.1; or

- By receiving a reliable communication from the Domain Name Registrar stating that the Registrant gives the Applicant permission to use the Domain Name.

Further information may be requested from the Applicant and other information and or methods may be utilised in order to demonstrate an equivalent level of confidence.

3.2.2.1Role Based Certificate Authentication

DOE CA ensures that requests for role based Certificates are authenticated and that role based names relating to an organisation and its business are accurate and correct.

3.2.3 Authentication of Individual identity

DOE CA authenticates individuals depending upon the class of Certificate as indicated below.

3.2.3.1Class 1

Class 1 certificates are not supported.

3.2.3.2Class 2 (SMIME/Client Authentication)

The Applicant is required to demonstrate control of any email address to be included within a certificate.

The Applicant is required to submit a legible copy of a valid government issued identity document or photo ID (Driver's Licence, passport or equivalent). A suitable non-government issued identity document or photo ID may also be required for additional proof. DOE CA verifies to a reasonable level of assurance that the email address matches the requested name and that other Subject information such as Country and/or state and locality fields are correct.

DOE CA also authenticates the Applicant's identity through one of the following methods;

- Performing a telephone challenge/response to the Applicant using a telephone number from a reliable source;
- Performing a postal challenge to the Applicant using an address obtained from a reliable source;
- Receiving an attestation from an appropriate notary, trusted third party that they have met the individual, and have inspected their national Photo ID document, and that the application details for the order are correct; or
- The Applicant's seal impression (in jurisdictions that permit their use to legally sign a document) is included with any application received in writing.

DOE CA may request further information from the Applicant. Other information and/or methods may be utilized in order to demonstrate an equivalent level of confidence.

3.2.4 Non Verified Subscriber Information

DOE CA validates all information to be included within the Subject DN of a Certificate except where highlighted within this section of the CPS.

- For all Certificate types where DOE CA can explicitly identify a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity DOE CA verifies the information and omits any disclaimer notice.
- For all Certificate types where DOE CA cannot explicitly verify the identity, e.g. a generic term such as "Marketing" then DOE CA omits any disclaimer that this item is classified as non-verified Subscriber Information as described herein.

3.2.5 Validation of Authority

- **SMIME/Client Authentication -** Verification through a reliable means of communication with the organisation or individual Applicant together with verification that the Applicant has control over the email address to be listed within the Certificate.
- **SMIME/Client Authentication (Department) -** Verification through a reliable means of communication with the organization Applicant together with verification that the Applicant has control over the email address to be listed within the Certificate.
- **SSL/TLS -** Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has ownership or control of the Domain Name by either a challenge response mechanism or direct confirmation with the contact listed with the Domain Name Registrar or WHOIS.

3.2.6 Criteria for Interoperation

Not applicable

3.3 Identification and Authentication for Re-key Requests

Not Supported

3.3.1 Identification and Authentication for Re-key After Revocation

No stipulation

3.4 Identification and Authentication for Revocation Request

All revocation requests are authenticated by DOE CA. Revocation requests may be granted following a suitable challenge response such as, logging into an account with the username and password, proving possession of unique elements incorporated into the Certificate e.g. Domain Name or email address or authentication of specific information which is authenticated out of band.

DOE CA may also perform revocation on behalf of Subscribers in accordance with the requirements of its Subscriber Agreement. Examples of reasons for revocation include a breach of the Subscriber Agreement or non-payment of applicable fees.

4.0 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

DOE CA maintains its own blacklists of individuals from whom and entities from which it will not accept Certificate applications. In addition, other external sources such as government denied lists or internationally recognized denied persons lists which are applicable to the jurisdictions in which DOE CA operates are used to screen out unwanted Applicants.

DOE CA does not issue Certificates to entities that reside in Countries where the laws of a DOE CA office location prohibit doing business.

Applications are accepted as follows:-

- **On-line**: Via a web interface over an https session. An Applicant must submit an application via a secure ordering process according to a procedure maintained by DOE CA.

4.1.2 Enrolment Process and Responsibilities

DOE CA maintains systems and processes that sufficiently authenticate the Applicant's identity for all Certificate types that present the identity to Relying Parties. Applicants must submit sufficient information to allow DOE CA and any RA to successfully perform the required verification. DOE CAs and RAs shall protect communications and securely store information presented by the Applicant during the application process in compliance with the DOE CA Privacy Policy.

Generally, the application process includes the following steps (but not necessarily in this order as some workflow processes generate Key Pairs after the validation has been completed):-

- Generating a suitable Key Pair using a suitably secure platform;
- Generating a Certificate Signing Request (CSR) using an appropriately secure tool;
- Submitting a request for a Certificate type and appropriate information;
- Agreeing to a Subscriber Agreement or other applicable terms and conditions; and
- Paying any applicable fees

4.2 Certificate Application Processing

DOE CA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this documentand those Requirements, those Requirements take precedence over this document.

4.2.1 Performing Identification and Authentication Functions

DOE CA maintains systems and processes to sufficiently authenticate the Applicant's identity in compliance with this CPS. Initial identity vetting may be performed by DOE CA's validation team as set forth in Section 3.2 or by Registration Authorities under contract.

4.2.2 Approval or Rejection of Certificate Applications

DOE CA shall reject requests for Certificates where validation of all items cannot successfully be completed. DOE CA may also reject requests based on potential brand damage to DOE CA in accepting the request. DOE CA may also reject applications for Certificates from Applicants who have previously been rejected or have previously violated a provision of their Subscriber Agreement or Terms of Use.

DOE CA may also reject requests for wildcard Certificates that are deemed to be a security risk or could negatively impact other subscribers.

Assuming all validation steps can be completed successfully following the procedures within this CPS then DOE CA shall approve the Certificate Request.

DOE CA is under no obligation to provide a reason to an Applicant for rejection of a Certificate Request.

4.2.3 Time to Process Certificate Applications

DOE CA shall ensure that all reasonable methods are used in order to evaluate and process Certificate applications. Where issues outside of the control of DOE CA occur, DOE CA shall strive to keep the Applicant duly informed.

The following approximations are given for processing and issuance.

- **SMIME/Client Authentication -** Approximately 1 business day.
- **SMIME/Client Authentication (Department) -** Approximately 1 business day.
- **SSL/TLS -** Approximately 1 business day.

DOE CA may be expedite urgent requests.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

DOE CA shall ensure it communicates with any RA accounts capable of causing Certificate issuance using multi-factor authentication. This includes RAs directly operated by DOE CA or RAs contracted by DOE CA. RAs shall perform validation of all information sent to the CA and ensure that any database used to store any information is suitably protected from unauthorised modification or tampering.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

DOE CA shall notify the Subscriber of the issuance of a Certificate at an email address which was supplied by the Subscriber during the enrolment process or by any other equivalent method. The email may contain the Certificate itself or a link to download depending upon the workflow of the Certificate requested.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

DOE CA shall inform the Subscriber that s/he may not use the Certificate until the Subscriber has reviewed and verified the accuracy of the data incorporated into the Certificate. Unless the Subscriber notifies DOE CA within one (1) business day from receipt, the Certificate is deemed accepted.

4.4.2 Publication of the Certificate by the CA

DOE CA publishes the certificate by delivering it to the Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs, Local RA or partners/resellers or DOE CA may be informed of the issuance if they were involved in the initial enrolment.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers must protect their Private Key taking care to avoid disclosure to third parties. DOE CA provides a suitable Subscriber Agreement or Terms of Use, which highlights the obligations of the Subscriber with respect to Private Key protection. Private Keys must only be used as specified in the appropriate key usage and extended key usage fields as indicated in the corresponding Certificate.

Where it is possible to make a backup of a Private Key, Subscribers must use the same level of care and protection attributed to the live Private Key. At the end of the useful life of a Private Key, Subscribers must securely delete the Private Key and any fragments that it has been split into for the purposes of backup.

4.5.2 Relying Party Public Key and Certificate Usage

Within this CPS DOE CA provides the conditions under which Certificates may be relied upon by Relying Parties, including the appropriate Certificate services to verify Certificate validity, such as CRL and/or OCSP. DOE CA provides a Relying Party agreement to Subscribers, the content of which should be presented to the Relying Party prior to reliance upon a Certificate from the DOE CA. Relying Parties should use the information to make a risk assessment and as such are solely responsible for performing the risk assessment prior to relying on the Certificate or any assurances made.

Software used by Relying Parties should be fully compliant with X.509 standards including best practice for chaining decisions around policies and key usage.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Not Supported

4.6.2 Who May Request Renewal

No stipulation

4.6.3 Processing Certificate Renewal Requests

No stipulation

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

Not Supported

4.7.2 Who May Request Certification of a New Public Key

No stipulation

4.7.3 Processing Certificate Re-Keying Requests

No stipulation

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

No stipulation

4.7.6 Publication of the Re-Keyed Certificate by the CA

No stipulation

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification is defined as the production of a new Certificate that has details which differ from a previously issued Certificate. The new modified Certificate will have a new Public Key and will have a new 'Not After' date.

- DOE CA treats modification the same as 'New' issuance.
- Old Certificate will be revoked with Revocation reason as 'superseded'

4.8.2 Who May Request Certificate Modification

As per 4.1

4.8.3 Processing Certificate Modification Requests

As per 4.2

4.8.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

As per 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

As per 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Certificate revocation is a process whereby the serial number of a Certificate is effectively blacklisted by adding the serial number and the date of the revocation to a Certificate Revocation List (CRL). The CRL itself will then be digitally signed with the same Private Key, which originally signed the Certificate to be revoked. Adding a serial number allows Relying Parties to establish that the lifecycle of a Certificate has ended. DOE CA may remove serial numbers when revoked Certificates pass their expiration date to promote more efficient CRL file size management. Prior to performing a revocation DOE CA will verify the authenticity of the revocation request. Revocation of a Subscriber Certificate shall be performed within twenty-four (24) hours under the following circumstances:-

- The Subscriber requests in writing to DOE CA that they wish to revoke the Certificate;
- The Subscriber notifies DOE CA that the original Certificate Request was not authorized and does not retroactively grant authorization;
- DOE CA obtains reasonable evidence that the Subscriber's Private Key has been Compromised, no longer complies with the requirements for algorithm type and key size of the Baseline Requirements, or that the Certificate has otherwise been misused;
- DOE CA receives notice or otherwise becomes aware that the Subscriber violated any of its material obligations under the Subscriber Agreement or Terms of Use;
- DOE CA is made aware of any circumstance indicating that used of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- DOE CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- DOE CA receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
- DOE CA is made aware that the Certificate was not issued in accordance with the Baseline Requirements or DOE CA's CP or this CPS;
- If DOE CA determines that any of the information appearing in the Certificate is not accurate or is misleading;
- DOE CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
- DOE CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless DOE CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- DOE CA is made aware of a possible Compromise of the Private Key of the Subordinate CA used for issuing the Certificate;
- Revocation is required by DOE CA's CP and/or CPS;
- The technical content of format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/B Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time);

Revocation of a Subscriber Certificate may also be performed within twenty-four (24) hours under the following circumstances:-

- The Subscriber or organization administrator requests revocation of the Certificate through a GCC account which controls the lifecycle of the Certificate;
- The Subscriber requests revocation of the Certificate via a OneClickSSL revocation workflow process;
- The Subscriber requests revocation through an authenticated request to DOE CA's support team or DOE CA's Registration Authority;
- DOE CA receives notice or otherwise become aware that the Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of DOE CA's jurisdiction of operation; and
- DOE CA determines the continued use of the Certificate is harmful to the business of DOE CA and Relying Parties.

When considering whether Certificate usage is harmful to DOE CA then DOE CA considers, among other things, the following:

- The nature and number of complaints received;
- The identity of the complainant(s);
- Relevant legislation in force; and
- Responses to the alleged harmful use from the Subscriber.

Revocation of a Subordinate CA Certificate shall be performed within seven (7) days under the following circumstances:-

- The Subordinate CA requests in writing to the GlobalSign entity which provided the Subordinate CA Certificate or the authority detailed in Section 1.5.2 of this CPS, that GlobalSign CA revoke the Certificate;
- The Subscriber notifies the Issuing CA that the original Certificate Request was not authorized and does not retroactively grant authorization;
- The Issuing CA obtains reasonable evidence that the Subordinate CA's Private Key has been Compromised, no longer complies with the requirements for algorithm type and key size of the Baseline Requirements, or that the Certificate has otherwise been misused;
- The Issuing CA is made aware that the Certificate was not issued in accordance with or that the Subordinate CA has not complied with the Baseline Requirements or the applicable CP or this CPS;
- The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The Issuing CA or Subordinate CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
- The Issuing CA's or Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless the issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by the Issuing CA's CP and/or CPS;
- The technical content of format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/B Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

4.9.2 Who Can Request Revocation

DOE CA and RAs shall accept authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the Subscriber or an affiliated organization named in the Certificate. DOE CA may also at its own discretion revoke Certificates.

4.9.3 Procedure for Revocation Request

Subscriber logs an Remedy Request with Manager's approval requesting for a Certificate to be revoked. If the user does not have access to Remedy, an email will be sent to information.security@det.nsw.edu.au.

DOE CA verifies subscribers identity.

DoE Directory Team revokes certificate.

Once revoked, the serial number of the Certificate and the date and time shall be added to the appropriate CRL. CRL reason codes may be included. CRLs are published according to this CPS.

4.9.4 Revocation Request Grace Period

The 'revocation request grace period' is the time available for a Subscriber to take any necessary actions themselves in order to request revocation of a suspected Key Compromise, use of a weak key or discovery of inaccurate information within an issued Certificate. Subscribers are given 48 hours to take appropriate actions otherwise DOE CA may revoke the Certificate. A risk analysis shall be completed and recorded for any revocations that cannot be processed by either party for any reason.

4.9.5 Time Within Which CA Must Process the Revocation Request

DOE CA will begin investigation procedures for a suspected Key Compromise or misuse of a Certificate within 24 hours of receipt of the report.

All revocation requests for end entity Certificates, both those generated automatically via user accounts and those initiated by DOE CA itself must be processed within a maximum of 24 hours of receipt.

4.9.6 Revocation Checking Requirements for Relying Parties

Prior to relying upon a Certificate, Relying Parties must validate the suitability of the Certificate to the purpose intended and ensure the Certificate is valid. Relying Parties will need to consult CRL or OCSP information for each Certificate in the chain as well as validating that the Certificate chain itself is complete and follows IETF PKIX standards. This may include the validation of Authority Key Identifier (AKI) and Subject Key Identifier (SKI). DOE CA will include all applicable URIs within the Certificate to aid Relying Parties in performing the revocation checking process such as:-

- http://crl.globalsign.com/gs/
- http://ocsp2.globalsign.com
- http://publiccrl.det.nsw.edu.au/CRL/
- http://publicocsp.det.nsw.edu.au/ocsp

4.9.7 CRL Issuance Frequency

DOE CA publishes full CRL every 7 days.

Delta CRL is published every 24 hours

4.9.8 Maximum Latency for CRLs

DOE CA ensures that online CA CRLs are published every 24 hours. A request for revocation received from DOE CA's RA system during the 24 hour period prior to the next scheduled CRL is included within the CRL if received up to 30 minutes prior.

4.9.9 On-Line Revocation/Status Checking Availability

DOE CA supports OCSP responses in addition to CRLs. Response times are no longer than 10 seconds under normal network operating conditions.

4.9.10 On-Line Revocation Checking Requirements

Relying parties must confirm revocation information.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation

4.9.12 Special Requirements Related to Key Compromise

DOE CA and any of its Registration Authorities shall use commercially reasonable methods to inform Subscribers that their Private Key may have been Compromised. This includes cases where new vulnerabilities have been discovered or where DOE CA at its own discretion decides that evidence suggests a possible Key Compromise has taken place. Where Key Compromise is not disputed, DOE CA shall revoke Issuing CA Certificates or Subscriber end entity Certificates within 24 hours and publish online CRL.

4.9.13 Circumstances for Suspension

DOE CA does not support suspension

4.9.14 Who Can Request Suspension

Not applicable

4.9.15 Procedure for Suspension Request

Not applicable

4.9.16 Limits on Suspension Period

Not applicable

4.10 Certificate Status Services

4.10.1 Operational Characteristics

DOE CA provides a certificate status service either in the form of a CRL distribution point or an OCSP responder or both. These services are presented to relying parties within the Digital Certificate and may refer to any of the following URLs

- http://crl.globalsign.com/gs/
- http://ocsp2.globalsign.com
- http://publiccrl.det.nsw.edu.au/CRL/
- http://publicocsp.det.nsw.edu.au/ocsp

4.10.2 Service Availability

DOE CA maintains 24x7 availability of Certificate status services.

4.10.3 Operational Features

No stipulation

4.10.4 End of Subscription

Subscribers may end their subscription to certificate services by having their certificate revoked or naturally letting it expire.

4.11 Key Escrow and Recovery

4.11.1 Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed.

DOE CA does not offer Key Escrow Services to Subscribers.

4.11.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5.0 Facility, Management, and Operational Controls

5.1 Physical Controls

DOE CA maintains physical and environmental security policies for systems used for Certificate issuance and management which cover physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking & entering, and disaster recovery.

5.1.1 Site Location and Construction

DOE CA ensures that critical and sensitive information processing facilities are housed in secure areas with appropriate security barriers and entry controls. These are physically protected from unauthorized access, damage and interference and the protections provided are commensurate with the identified risks in risk analysis plans.

5.1.2 Physical Access

DOE CA ensures that the facilities used for Certificate lifecycle management are operated in an environment that physically protects the services from Compromise through unauthorized access to systems or data. An authorized employee will always accompany any unauthorized person entering a physically secured area. Physical protections are achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the systems hosting the CA operations. No parts of the CA premises are shared with other organisations within this perimeter.

5.1.3 Power and Air Conditioning

DOE CA ensures that the power and air conditioning facilities are sufficient to support the operation of the CA system.

5.1.4 Water Exposures

DOE CA ensures that the CA systems are protected from water exposure.

5.1.5 Fire Prevention and Protection

DOE CA ensures that the CA system is protected with a fire suppression system

5.1.6 Media Storage

DOE CA ensures that any Media used is securely handled to protect it from damage, theft and unauthorised access.

5.1.7 Waste Disposal

DOE CA ensures that all media used for the storage of information is declassified or destroyed in a generally accepted manner before being released for disposal.

5.1.8 Off-Site Backup

DOE CA ensures that a full system backup of the Certificate issuance system is sufficient to recover from system failures and is made on a regular basis. Back-up copies of essential business information and software are also taken on a regular basis. All backups are stored off site.

5.2 Procedural Controls

5.2.1 Trusted Roles

DOE CA ensures that all operators and administrators including vetting agents are acting in the capacity of a Trusted Role. Trusted roles are such that no conflict of interest is possible and the roles are distributed such that no single person can circumvent the security of the CA system.

Trusted Roles include but are not limited to the following:

- **Security Officer:** Overall responsibility for administering the implementation of the security practices;
- **Administrator**: Approves the generation/revocation/suspension of certificates;
- **System Engineer**: Authorised to install, configure and maintain the CA systems used for certificate life cycle management;
- **Operator**: Responsible for operating the CA systems on a day to day basis. Authorised to perform system backup and recovery;
- **Auditor**: Authorised to view archives and audit logs of the CA trustworthy systems;
- **CA activation data holder**: authorised person that holds CA activation data that is necessary for CA hardware security module operation.
- **Vetting Agent**: Responsible for validating the authenticity and integrity of data to be included within digital certificates via a suitable RA system

5.2.2 Number of Persons Required per Task

DOE CA requires at least two people per task. The goal is to guarantee the trust for all CA services (Key Pair generation, Certificate generation, revocation) so that any malicious activity would require collusion. Where multiparty control is required, at least one of kthe participants shall be an Administrator. All participants shall serve in a trusted role as defined in Section 5.2.1 above..

5.2.3 Identification and Authentication for Each Role

Before appointing a person to a trusted role, DOE CA performs a background check. Each role described above is identified and authenticated in a manner to guarantee that the right person has the right role to support the CA.

5.2.4 Roles Requiring Separation of Duties

DOE CA enforces role separation either by the CA equipment or procedurally or by both means.

Individual CA personnel are specifically assigned to the roles defined in Section 5.2.1 above. It is not permitted for any one person to serve in the following roles at the same time:

- Security Officer and System Engineer or Operator;
- Auditor and Security Officer or Operator or Administrator or System Engineer;
- System Engineer and Operator or Administrator.

No individual shall be assigned more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

DOE CA employs a sufficient number of personnel that possess the expert knowledge, experience and qualifications necessary for the offered services, as appropriate to the job function. DOE CA personnel fulfil the requirement through expert knowledge, experience and qualifications with formal training and education, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in Section 5.2.1, are documented in job descriptions. DOE CA personnel (both temporary and permanent) have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. DOE CA personnel are formally appointed to trusted roles by senior management responsible for security.

The job descriptions include skills and experience requirements. Managerial personnel are employed who possess experience or training in electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions..

5.3.2 Background Check Procedures

All DOE CA personnel in trusted roles are free from conflicting interests that might prejudice the impartiality of the CA operations. DOE CA does not appoint to a trusted role or management position any person who is known to have a conviction for a serious crime or another offence, if such conviction affects his/her suitability for the position. Personnel do not have access to the trusted functions until any necessary checks are completed and results analysed. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation.

5.3.3 Training Requirements

DOE CA ensures that all personnel performing duties with respect to the operation of the CA receive comprehensive training in:

- CA/RA security principles and mechanisms;
- Software versions in use on the CA system;
- Duties they are expected to perform; and
- Disaster recovery and business continuity procedures.

DOE CA and RA personnel are retrained when changes occur in DOE CA or RA systems. Refresher training is conducted as required and DOE CA shall review refresher-training requirements at least once a year.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for trusted roles are aware of changes in the DOE CA or RA operations, as applicable. Any significant change to the operations has a training (awareness) plan, and the execution of such plan is documented.

5.3.5 Job Rotation Frequency and Sequence

DOE CA ensures that any change in the staff will not affect the operational effectiveness of the service or the security of the system.

5.3.6 Sanctions for Unauthorised Actions

Appropriate disciplinary sanctions are applied to personnel violating provisions and policies within this CPS or CA related operational procedures.

5.3.7 Independent Contractor Requirements

Contractor personnel employed for DOE CA operations are subjected to the same process, procedures, assessment, security control and training as permanent CA personnel.

5.3.8 Documentation Supplied to Personnel

DOE CA makes available to its personnel this CPS, any corresponding CP and any relevant statutes, policies or contracts. Other technical, operational and administrative documents (e.g., administrator manuals, user manuals, etc.) are provided in order for the trusted personnel to perform their duties.

Documentation is maintained identifying all personnel who received training and the level of training completed.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit log files shall be generated for all events relating to the security and services of the CA. Where possible, the security audit logs shall be automatically generated. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non- electronic, shall be retained and made available during compliance audits.

DOE CA ensures all events relating to the lifecycle of Certificates are logged in a manner to ensure the traceability to a person in a trusted role for any action required for CA services. At a minimum, each audit record includes the following (either recorded automatically or manually) elements:

- The type of event;
- The date and time the event occurred;
- Success or failure where appropriate;
- The identity of the entity and/or operator that caused the event;
- The identity to which the event was targeted; and
- The cause of the event.

5.4.2 Frequency of Processing Log

Audit logs are reviewed periodically and reasonably for any evidence of malicious activity and following each important operation.

5.4.3 Retention Period for Audit Log

Audit log records are held for a period of time as appropriate to providing necessary legal evidence in accordance with any applicable legislation. Records may be required at least as long as any transaction relying on a valid certificate can be questioned.

5.4.4 Protection of Audit Log

The events are logged in a way that they cannot be deleted or destroyed (except for transfer to long term media) for any period of time that they are retained.

The events are logged in a manner to ensure that only individuals with authorized trusted access are able to perform any operations regarding their profile without modifying integrity, authenticity and confidentiality of the data.

The events are protected in a manner to keep them readable during the time of their storage.

The events are date stamped in a secure manner that guarantees, from the date of creation of the record to the end of the archive period that there is a trusted link between the event and the time of its realisation.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries are backed-up in a secure location (for example, a fire proof safe), under the control of an authorized trusted role, and separated from their component source generation. Audit log backup is protected to the same degree as originals.

5.4.6 Audit Collection System (Internal vs. External)

Audit processes are initiated at system start up and finish only at system shutdown. The audit collection system ensures the integrity and availability of the data collected. If necessary, the audit collection system protects the data confidentiality. In the case of a problem occurring during the process of the audit collection DOE CA determines whether to suspend DOE CA operations until the problem is resolved, duly informing the DOE CA impacted asset owners.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

DOE CA performs regular vulnerability assessments covering all DOE CA assets related to Certificate issuance, products and services. Assessments focus on internal and external threats that could result in unauthorised access, tampering, modification, alteration or destruction of the Certificate issuance process.

5.5 Records Archival

5.5.1 Types of Records Archived

DOE CAs and RAs archive records with enough detail to establish the validity of a signature and of the proper operation of the CA system. At a minimum, the following data is archived:

DOE CA key lifecycle management events, including:-

- Key generation, backup, storage, recovery, archival, and destruction;
- Cryptographic device lifecycle management events; and
- CA System equipment configuration.

DOE CA issuance system management events including:-

- System start-up and shutdown actions;
- Attempts to create, remove, or set passwords or change the system; and
- Changes to Issuer CA keys.

DOE CA and Subscriber Certificate lifecycle management events, including:-

- Certificate requests, renewal, and re-key requests, and revocation for both successful and unsuccessful attempts;
- All verification activities stipulated in this CPS;
- Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
- Acceptance and rejection of Certificate requests;
- Issuance of Certificates; and
- Generation of Certificate Revocation Lists and OCSP entries including failed read-and-write operations on the certificate and CRL directory.

Security events, including:-

- Successful and unsuccessful PKI system access attempts;
- PKI and security system actions performed;
- Security profile changes;
- System crashes, hardware failures, and other anomalies;
- Firewall and router activities; and
- Entries to and exits from the CA facility.

Documentation and Auditing:-

- Audit documentation including all work related communications to or from DOE CA and compliance auditors;
- Certificate Policy and previous versions;
- Certification Practice Statement and previous versions; and
- Contractual agreements between subscribers and the DOE CA

Time stamping:-

- Clock synchronisation.

Miscellaneous

- Other data or applications sufficient to verify archive contents;
- Equipment failure
- UPS failure or Electrical power outages; and
- Violations of the CP or this CPS

5.5.2 Retention Period for Archive

The minimum retention period for archive data is 7 years.

5.5.3 Protection of Archive

The archives are created in such a way that they cannot be deleted or destroyed (except for transfer to long term media) within the period of time for which they are required to be held. Archive protections ensure that only authorized trusted access is able to make operations without modifying integrity, authenticity and confidentiality of the data. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site.

5.5.4 Archive Backup Procedures

Archive Backups are made which are either of the online DOE CA system or the offline system.

Online backups are duplicated weekly and each backup is stored in a location which is different to original online system. One backup is stored in a fire rated media safe.

An Offline backup is taken at the end of any key ceremony (with the exception of any encrypted material which is store separately in line with key ceremony procedures) and stored in an off site location within 30 days of the ceremony.

5.5.5 Requirements for Time-Stamping of Records

If a time-stamping service is used to date the records, then it has to respect the requirements defined in section 6.8. Irrespective of time-stamping methods, all logs must have data indicating the time at which the event occurred.

5.5.6 Archive Collection System (Internal or External)

The archive collection system respects the security requirements defined in section 5.3.

5.5.7 Procedures to Obtain and Verify Archive Information

Media storing of DOE CA archive information is checked upon creation. Periodically, statistical samples of archived information are tested to check the continued integrity and readability of the information.

Only authorised DOE CA equipment, trusted role and other authorised persons are allowed to access the archive. Requests to obtain and verify archive information are co-ordinated by operators in trusted roles (internal auditor, the manager in charge of the process and the Security Officer)

5.6 Key Changeover

DOE CA may periodically change over key material for Issuing CAs in accordance with Section 6.3.2. Certificate Subject information may also be modified and Certificate profiles may be altered to adhere to new best practices. Private Keys used to sign previous Subscriber Certificates are maintained until such time as all Subscriber Certificates have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Please contact us immediately if you encounter a DOE CA secure site seal, SSL Certificate or Code Signing Certificate that you believe is being used inappropriately of for malicious purposes (such as malware). Note that DOE CA agreements prohibit the use of GlobalSign Certificates for harmful purposes. Email information.security@det.nsw.edu.au.

DOE CA establishes business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data that could disturb or Compromise the DOE CA services. DOE CA carries out risk assessments to evaluate business risk and determine the necessary security requirements and operational procedures to be taken as a consequence of its disaster recovery plan. This risk analysis is regularly reviewed and revised if necessary (threat evolution, vulnerability evolution, etc.). This business continuity is included in the scope of the audit process as described in Section 8 to validate which operations should first be restored after a disaster and the recovery plan.

DOE CA personnel that serve in a trusted role and operational role are specially trained to operate according to procedures defined in the disaster recovery plan for business critical operations.

If DOE CA detects a potential hacking attempt or another form of Compromise, it should perform an investigation in order to determine the nature and the degree of damage. Otherwise, DOE CA assesses the scope of potential damage in order to determine whether the CA or RA system needs to be rebuilt, whether only some Certificates need to be revoked, and/or whether a CA hierarchy needs to be declared as Compromised. The CA disaster recovery plan highlights which services should be maintained (for example, revocation and Certificate status information).

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

If any equipment is damaged or rendered inoperative but the Private Keys are not destroyed, the operation should be re-established as quickly as possible, giving priority to the ability to generate Certificate status information according to DOE CA's disaster recovery plan.

5.7.3 Entity Private Key Compromise Procedures

In case a DOE CA signature key is compromised, lost, destroyed or suspected to be compromised:

- DOE CA, after investigation of the problem decides whether the DOE CA certificate should be revoked. If so then:-
    - All the subscribers who have been issued a Certificate will be notified at the earliest feasible opportunity; and
    - A new DOE CA Key Pair shall be generated or an alternative existing CA hierarchy shall be used to create new subscriber certificates;

5.7.4 Business Continuity Capabilities After a Disaster

The disaster recovery plan deals with the business continuity as described in Section 5.7.1. Certificate status information systems should be deployed so as to provide 24 hours per day, 365 days per year availability (with a rate of 99.95% availability excluding planned maintenance operations).

5.8 CA or RA Termination

In the event of termination of a DOE CA or RA, DOE CA provides notice to all customers prior to the termination and:

- Stops delivering Certificates according to and referring to this CPS;
- Archives all audit logs and other records prior to termination;
- Destroys all Private Keys upon termination;
- Ensures archive records are transferred to an appropriate authority such as another DOE CA that delivers identical services; and
- Uses secure means to notify customers and Application Software Suppliers to delete all trust anchors.

6.0 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

DOE CA generates all issuing key pairs in a physically secure environment by personnel in trusted roles under, at least, dual control. DOE CA key generation is carried out within a device, which is at least certified to FIPS 140-2 level 3 or above.

6.1.2 Private Key Delivery to Subscriber

No stipulation.

6.1.3 Public Key Delivery to Certificate DOE CA

DOE CA only accepts Public Keys from RAs that have been protected during transit and have had the authenticity and integrity of their origin from the RA suitably verified. RA's shall only accept Public Keys from Subscribers in accordance with Section 3.2.1 of this CPS.

6.1.4 CA Public Key Delivery to Relying Parties

DOE CA relies on the processes of GlobalSign nv-sa (the Root Authority) to deliver Root Certificates to Relying Parties, and upon chain verification mechanisms within the Relying Parties' software platform to establish the chain of trust for the Relying Party.

6.1.5 Key Sizes

DOE CA follows NIST recommended timelines and best practice in the choice of size of its Key Pairs for Root CAs and Issuing CAs and only signs end entity Certificates following best practices.

The following key sizes and Hashes are used for Root Certificates, Issuing CA Certificates and end entity Certificates and CRL/OCSP Certificate status responders in accordance with the Baseline Requirements:-

- 2048 bit RSA key with Secure Hash Algorithm 2 (SHA-256)

Where possible, the entire Certificate chain and any Certificate status responses use the same level of security and cryptography. Exceptions due to cross-certified Certificates are acceptable.

Existing Certificates with an unsuitable cryptographic strength are replaced in sufficient time as to protect Relying parties, Subscribers and Issuing CAs.

6.1.6 Public Key Parameters Generation and Quality Checking

DOE CA generates Key Pairs in accordance with FIPS 186 and uses reasonable techniques to validate the suitability of Public Keys presented by Subscribers. Known weak keys shall be tested for and rejected at the point of submission.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

DOE CA sets Key Usage of certificates depending on their proposed field of application via the v3 Key Usage Field for X.509 v3 (See section 7.1).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

DOE CA ensures that all systems signing Certificates and CRLs or generating OCSP responses use FIPS 140-2 level 3 as the minimum level of cryptographic protection.

6.2.2 Private Key (n out of m) Multi-Person Control

DOE CA activates Private Keys for cryptographic operations with multi-person control (using CA activation data) performing duties associated with their trusted roles. The trusted roles permitted to participate in this Private Key multi-person controls are strongly authenticated (i.e. token with PIN code). The CA Private Key is always protected through 3 of 5.

6.2.3 Private Key Escrow

DOE CA does not escrow Private Keys for any reason.

6.2.4 Private Key Backup

If required for business continuity DOE CA backs up private keys under the same multi-person control as the original Private Key.

6.2.5 Private Key Archival

DOE CA does not archive Private Keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

DOE CA Private Keys are generated, activated and stored in Hardware Security Modules (HSM). When Private Keys are outside of a Hardware Security Module (either for storage or transfer), they are encrypted. Private Keys never exist outside of a cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

DOE CA stores Private Keys on at least a FIPS 140-2 level 3 device.

6.2.8 Method of Activating Private Key

DOE CA is responsible for activating the Private Key in accordance with the instructions and documentation provided by the manufacturer of the Hardware Security Module. Subscribers are responsible for protecting Private Keys in accordance with the obligations that are presented in the form of a Subscriber Agreement or Terms of Use.

6.2.9 Method of Deactivating Private Key

DOE CA ensures that Hardware Security Modules that have been activated are not left unattended or otherwise available to unauthorized access. During the time a DOE CA's Hardware Security Module is on-line and operational, it is only used to sign Certificates and CRL/OCSPs from an authenticated RA. When a CA is no longer operational, Private Keys are removed from the Hardware Security Module.

6.2.10 Method of Destroying Private Key

DOE CA Private Keys are destroyed when they are no longer needed or when the Certificates to which they correspond have expired or have been revoked. Destroying Private Keys means that DOE CA destroys all associated CA secret activation data in such a manner that no information can be used to deduce any part of the Private Key.

6.2.11 Cryptographic Module Rating

See section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

DOE CA archives Public Keys from certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

DOE CA certificates have a maximum validity period of:-

Type	Private Key Usage	Certificate Term
• **SMIME Certificates -**	No stipulation	3 years

- **SSL/TLS Certificates -** No stipulation 3 years

GlobalSign CA complies with the Baseline Requirements with respect to the maximum Validity Period. In some cases, the maximum Validity Period may not be realized by the Subscriber in the event the current or future Baseline Requirements impose requirements on Certification Authorities relative to Certificate issuance that were not in place at the time the Certificate was originally issued, particularly in the case of a request for reissuance, e.g., additional requirements are included for identification and authentication for certain Certificate type, or maximum Validity Period is decreased.

Effective April 1, 2015, in no event shall GlobalSign issue an SSL/TLS Certificate with a Validity Period greater than 39 months whether as initial issue, re-key, reissue or otherwise

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of DOE CA activation data used to activate DOE CA Private Keys are made during a key ceremony (Refer to Section 6.1.1). Activation data is either generated automatically by the appropriate HSM or in such a way that meets the same needs. It is then delivered to a holder of a share of the key who is a person in trusted role. The delivery method maintains the confidentiality and the integrity of the activation data.

6.4.2 Activation Data Protection

Issue CA activation data is protected from disclosure through a combination of cryptographic and physical access control mechanisms. DOE CA activation data is stored on smart cards.

6.4.3 Other Aspects of Activation Data

DOE CA activation data may only be held by DOE CA personnel in trusted roles.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards. The DOE CA PKI components must include the following functions:

- Require authenticated logins for trusted role;
- Provide discretionary access control;
- Provide security audit capability (protected in integrity);
- Prohibit object re-use;
- Require use of cryptography for session communication;
- Require trusted path for identification and authentication;
- Provide domain isolation for process; and
- Provide self-protection for the operating system.

When DOE CA PKI equipment is hosted on an evaluated platform in support of computer security assurance requirements then the system (hardware, software, operating system), when possible, operates in an elevated configuration. At a minimum, such platforms use the same version of the computer operating system as that which received the evaluation rating. The computer systems are configured with minimum of the required accounts, network services, and no remote login without mulit factor authentication.

6.5.2 Computer Security Rating

All the DOE CA PKI component software is compliant with the requirements of the protection profile from a suitable entity.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development controls for the DOE CA are as follows:

- Use software that has been designed and developed under a formal, documented development methodology;
- Hardware and software procured are purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase);
- Hardware and software are developed in a controlled environment, and the development processes are defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software;
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location;
- The hardware and software are dedicated to performing CA activities. There are no other applications, hardware devices, network connections, or component software installed which are not part of the CA operation;
- Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the CA operations installed on the equipment and are obtained from sources authorized by local policy. DOE CA hardware and software are scanned for malicious code on first use and periodically thereafter; and
- Hardware and software updates are purchased or developed in the same manner as original equipment and are installed by trusted and trained personnel in a defined manner

6.6.2 Security Management Controls

The configuration of the DOE CA system as well as any modifications and upgrades are documented and controlled by the DOE CA management. There is a mechanism for detecting unauthorised modification to the DOE CA software or configuration. A formal configuration management methodology is used for installation and on-going maintenance of the DOE CA system. The DOE CA software, when first loaded, is checked as being that supplied from the vendor, with no modifications, and is the version intended for use

6.6.3 Life Cycle Security Controls

DOE CA maintains a maintenance scheme to ensure the level of trust of software and hardware that are evaluated and certified,

6.7 Network Security Controls

DOE CA PKI components implement appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of security guards, firewalls and filtering routers. Unused network ports and services are turned off. Boundary control devices, used to protect the network on which PKI equipment are hosted, deny all but the necessary services to the PKI equipment, even if those services are enabled for other devices on the network

6.8 Time-Stamping

All DOE CA components are regularly synchronised with a reliable time service. DOE CA uses one GPS source & one DCF77 source & 3 non-authenticated NTP source clocks *(ntp.det.nsw.edu.au)* to establish the correct time:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates;
- Issuance of Subscriber End Entity certificates.

Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.

7.0 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

DOE CA issues Certificates in compliance with X.509 Version 3

7.1.2 Certificate Extensions

DOE CA issues Certificates in compliance with RFC 5280 and applicable best practice. Criticality also follows best practice to prevent unnecessary risks to Relying Parties when applied to name constraints.

7.1.3 Algorithm Object Identifiers

DOE CA issues Certificates with algorithms indicated by the following OIDs

SHA1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 5}
SHA256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
ECDSAWithSHA1	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) 1 }
ECDSAWithSHA224	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ECDSAWithSH256	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 2 }
ECDSAWithSHA384	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ECDSAWithSHA512	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 4 }

7.1.4 Name Forms

DOE CA issues Certificates with name forms compliant to RFC 5280. Within the domain of each Issuing CA, DOE CA includes a unique non-sequential Certificate serial number that exhibits 80 bits of entropy.

7.1.5 Name Constraints

Name constraints are mandated by GlobalSign

Name constraints are constantly updated through signing ceremonies with GlobalSign

7.1.6 Certificate Policy Object Identifier

SSL certificates	2.23.140.1.2.2
SMIME certificates	1.3.6.1.5.5.7.3.4

The Subscriber certificates DOE CA issues are managed in accordance with these policy Requirements.

7.1.7 Usage of Policy Constraints Extension

No Stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

DOE CA issues Certificates with a policy qualifier and suitable text to aid Relying Parties determine applicability.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

7.2.1 Version Number(s)

DOE CA issues Version 2 CRLs in compliance with RFC 5280. CRLs have the following fields:-

- **Issuer** NSW-DEC-ISS-CA1
- **Effective date** Date and Time
- **Next update** Date and Time
- **Signature Algorithm** sha256RSA
- **Signature Hash Algorithm** sha256
- **Serial Number(s)** List of revoked serial numbers
- **Revocation Date** Date of Revocation

7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:-

- **CRL Number**
- **Authority Key Identifier** AKI of the issuing CA for chaining/validation requirements

7.3 OCSP Profile

DOE CA operates an Online Certificate Status Profile (OCSP) responder in compliance with RFC 2560 or RFC5019 and highlights this within the AIA extension via an OCSP responder URI.

7.3.1 Version Number(s)

DOE CA issues Version 1 OCSP responses

7.3.2 OCSP Extensions

No stipulation

8.0 Compliance Audit and Other Assessments

The procedures within this CPS encompass all relevant portions of currently applicable PKI standards. DOE CA is constrained by GlobalSign nv-sa using dNSNameConstraints and therefore external independent auditing is not applicable.

8.1 Frequency and Circumstances of Assessment

The Certificates issued by DOE CA are assessed on an annual basis by GlobalSign nv-sa or an affiliated GlobalSign company as part of the contractual obligation in using Trusted Root chaining services. The assessment covers all CA related activities as recommended by the Baseline Requirements.

8.2 Identity/Qualifications of Assessor

GlobalSign nv-sa or an affiliated GlobalSign company determines through an annual assessment that the provisions of the contract and adherence to the Baseline Requirements are maintained using suitably qualified and trained GlobalSign staff members.

8.3 Assessor's Relationship to Assessed Entity

DOE CA is a cross-signed entity under contract with GlobalSign nv-sa or an affiliated company under the Trusted Root program.

8.4 Topics Covered by Assessment

The audit meets the requirements of the Baseline Requirements.

8.5 Actions Taken as a Result of Deficiency

DOE CA follows the same process if presented with a material non-compliance by GlobalSign nv-sa or an affiliated company. DOE CA creates a suitable corrective action plan to remove the deficiency. Corrective action plans which directly affect policy and procedure as dictated by GlobalSign's CP and this CPS are referred to the GlobalSign Policy Authority for discussion and resolution.

8.6 Communications of Results

Results of the audit are reported to DOE CA for analysis and resolution of any deficiency through a subsequent corrective action plan.

9.0 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

DOE CA may charge fees for certificate issuance.

9.1.2 Certificate Access Fees

DOE CA may charge for Access to any Database which stores issued certificates.

9.1.3 Revocation or Status Information Access Fees

DOE CA may charge fees for Revocation or Status Information.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

DOE CA maintains Commercial General Liability insurance. Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

9.2.2 Other Assets

No stipulation

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following items are classified as being confidential information and therefore are subject to reasonable care and attention by DOE CA staff including vetting agents and administrators.

- Personal information as detailed in Section 9.4;
- Audit logs from CA and RA systems;
- Activation data used to active CA Private Keys as detailed in Section 6.4;
- Internal GlobalSign business process documentation including Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP); and
- Audit reports from an independent auditor as detailed in Section 8.0

9.3.2 Information Not Within the Scope of Confidential Information

Any information not defined as confidential within this CPS shall be deemed public. Certificate status information and Certificates themselves are deemed 'public'.

9.3.3 Responsibility to Protect Confidential Information

DOE CA protects confidential information through training and enforcement with employees, agents and contractors.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

DOE CA protects personal information through internal policy in accordance with legal requirements where DOE CA operates.

9.4.2 Information Treated as Private

DOE CA treats all information received from Applicants that will not ordinarily be placed into a Certificate as private. This applies both to those Applicants who are successful in being issued a Certificate and those who are unsuccessful and rejected. DOE CA periodically trains all RA and vetting staff as well as anyone who has access to the information about due care and attention that must be applied.

9.4.3 Information Not Deemed Private

Certificate status information and any Certificate content is deemed not private.

9.4.4 Responsibility to Protect Private Information

DOE CA protects Personal Information in line with legal requirements where DOE CA operates.

9.4.5 Notice and Consent to Use Private Information

Personal Information obtained from Applicants during the application and enrolment process is deemed private and permission is required from the Applicant to allow the use of such information. DOE CA includes any required consents in the Subscriber Agreement including any permission required for additional information to be obtained from third parties that may be applicable to the validation process for the product or service being offered by DOE CA.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

DOE CA may disclose Private Information without notice to Applicants or Subscribers where required to do so by law or regulation.

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property rights

DOE CA does not knowingly violate the intellectual property rights of third parties. Public and Private Keys remain the property of Subscribers who legitimately hold them. DOE CA retains ownership of Certificates; however, it grants permission to reproduce and distribute Certificates on a non-exclusive, royalty free basis, provided that they are reproduced and distributed in full.

GlobalSign and the GlobalSign logo are the registered trademarks of GMO GlobalSign K.K.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

DOE CA uses this CPS and applicable Subscriber Agreements to convey legal conditions of usage of issued Certificates to Subscribers and Relying Parties. All parties including the DOE CA, any RAs and Subscribers warrant the integrity of their respective Private Key(s). If any such party suspects that a Private Key has been Compromised they will immediately notify the appropriate RA.

DOE CA represents and warrants to Certificate Beneficiaries during the period when the Certificate is valid, DOE CA has complied with its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate:-

- **Right to Use Domain Name or IP Address**: That, at the time of issuance, DOE CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's Subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in DOE CA's Certificate Policy and/or Certification Practice Statement (see Section 3.2);
- **Authorisation for Certificate:** That, at the time of issuance, DOE CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii)

followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in DOE CA's Certificate Policy and/or Certification Practice Statement (see Section 3.2.5);

- **Accuracy of Information:** That, at the time of issuance, DOE CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in DOE CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);
- **No Misleading Information:** That, at the time of issuance, DOE CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in DOE CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in DOE CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);
- **Subscriber Agreement:** That, if DOE CA and Subscriber are not Affiliates, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if DOE CA and Subscriber are Affiliates, the Applicant Representative acknowledged and accepted the Terms of Use (see Section 4.5.1);
- **Status:** That DOE CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
- **Revocation:** That DOE CA will revoke the Certificate for any of the reasons specified in the Baseline Requirements (see Section 4.9.1)

9.6.2 RA Representations and Warranties

RAs warrant that:-

- Issuance processes are in compliance with this CPS and the relevant GlobalSign CP.
- All information provided to DOE CA does not contain any misleading or false information. and
- All translated material provided by the RA is accurate

9.6.3 Subscriber Representations and Warranties

Unless otherwise stated in this CPS, subscribers are responsible for:

- Having knowledge and, if necessary, seeking training on using digital certificates.
- Generating securely their private-public key pair, using a trustworthy system.
- Providing correct and accurate information in their communications with DOE CA.
- Ensuring that the public key submitted to the DOE CA correctly corresponds to the private key used.
- Accepting all terms and conditions in any subscriber agreement, GlobalSign CP and associated policies published in the DOE CA repository.
- Refraining from tampering with an issued certificate.
- Using certificates only for legal and authorised purposes in accordance with this CPS.
- Notifying the DOE CA or RA of any changes in the information submitted.
- Ceasing to use a certificate if any featured information becomes invalid.
- Ceasing to use a certificate when it becomes invalid.
- Removing a certificate when invalid from any applications and/or devices they have been installed on.
- Using a certificate, as it may be reasonable under the circumstances.
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private key.
- For any acts and omissions of partners and agents subscribers use to generate, retain, escrow, or destroy any private keys.

- Refraining from submitting any material that contains statements that violate any law or the rights of any party.
- Requesting the revocation of a certificate in case of an occurrence that materially affects the integrity of a certificate.
- Notifying the appropriate RA immediately, if a subscriber becomes aware of or suspects the compromise of a private key.
- Submit accurate and complete information to DOE CA in accordance with the requirements of this CPS particularly with regards to registration.
- Only use the key pair for digital signatures and in accordance with any other limitations notified to the subscriber according to this CPS or any Trusted Root CA Chaining agreement.
- Exercise absolute care to avoid unauthorised use of its private key.
- Use a key length and algorithm as indicated in this CPS.
- Notify DOE CAs without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
    - The subscriber's private key has been lost, stolen, potentially compromised; or
    - Control over the subscribers private key has been lost due compromise of activation data (e.g. PIN code or Pass Phrase); or
    - Inaccuracy or changes to the certificate content, as notified to the Subscriber.

The Subscriber is ultimately liable for the choices he or she makes when applying for a certificate. The applicant and DOE CA must designate the usage of a trustworthy device as well as the choice of organisational context.

9.6.4 Relying Party Representations and Warranties

A party relying on a DOE CA's Certificate warrants to:

- Have the technical capability to use Certificates;
- Receive notice of the DOE CA and associated conditions for Relying Parties;
- Validate a DOE CA's Certificate by using Certificate status information (e.g. a CRL or OCSP) published by the DOE CA in accordance with the proper Certificate path validation procedure;
- Trust a DOE CA's Certificate only if all information featured on such Certificate can be verified via such a validation procedure as being correct and up to date;
- Rely on a DOE CA's Certificate, only as it may be reasonable under the circumstances; and
- Notify the appropriate RA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been Compromised.

The obligations of the Relying Party, if it is to reasonably rely on a Certificate, are to:

- Verify the validity or revocation of the CA Certificate using current revocation status information as indicated to the Relying Party;
- Take account of any limitations on the usage of the Certificate indicated to the Relying Party either in the Certificate or this CPS; and
- Take any other precautions prescribed in the DOE CA's Certificate as well as any other policies or terms and conditions made available in the application context a Certificate might be used.

Relying Parties must at all times establish that it is reasonable to rely on a Certificate under the circumstances taking into account circumstances such as the specific application context a Certificate is used in.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

EXCEPT TO THE EXTENT PROHIBITED BY LAW OR AS OTHERWISE PROVIDED HEREIN, DOE CA DISCLAIMS ALL WARRANTIES INCLUDING ANY WARRANTY OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.

9.8 Limitations of Liability

TO THE EXTENT DOE CA HAS ISSUED AND MANAGED THE CERTIFICATE IN ACCORDANCE WITH THE BASELINE REQUIREMENTS AND THIS CPS, DOE CA SHALL NOT BE LIABLE TO THE SUBSCRIBER, RELYING PARTY OR ANY THIRD PARTIES FOR ANY LOSSES SUFFERED AS A RESULT OF USE OR RELIANCE ON SUCH CERTIFICATE. OTHERWISE, DOE CA'S LIABILITY TO THE SUBSCRIBER, RELYING PARTY OR ANY THIRD PARTIES FOR ANY SUCH LOSSES SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS ($1,000).

THIS LIABILITY CAP LIMITS DAMAGES RECOVERABLE OUTSIDE OF THE CONTEXT OF THE DoE WARRANTY POLICY. AMOUNTS PAID UNDER THE WARRANTY POLICY ARE SUBJECT TO THEIR OWN LIABILITY CAPS.

IN NO EVENT SHALL DOE CA SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA OR OTHER INDIRECT, INCIDENTAL, CONSEQUENTIAL DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, RELIANCE UPON, LICENSE, PERFORMANCE OR NON PERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS CPS.

9.9 Indemnities

9.9.1 Indemnification by DOE CA

DOE CA shall indemnify each Application Software Supplier against any claim, damage, or loss suffered by the Application Software Supplier related except where the claim, damage, or loss suffered by the Application Software Supplier was directly caused by the Application Software Supplier's software displaying as trustworthy (i) a Certificate that has expired or (ii) a revoked Certificate where the revocation status is available online but the Application Software Supplier's software failed to check or ignored the status.

9.9.2 Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify DOE CA, GlobalSign nv-sa and any related entity providing services to DOE CA, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CPS, or applicable law; (iii) the Compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence; or (iv) Subscriber's misuse of the Certificate or Private Key.

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify DOE CA, GlobalSign nv-sa and any related entity providing services to DOE CA, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, this CPS, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

9.10 Term and Termination

9.10.1 Term

This CPS remains in force until notice of the opposite is communicated by the DOE CA on its web site or repository.

9.10.2 Termination

Notified changes are appropriately marked by an indicated version. Changes become effective immediately upon publication.

9.10.3 Effect of Termination and Survival

DOE CA will communicate the conditions and effect of this CPS termination via the appropriate repository.

9.11 Individual Notices and Communications with Participants

DOE CA will communicate with Participants via the appropriate repository.

9.12 Amendments

9.12.1 Procedure for Amendment

Changes to this CPS are indicated by appropriate numbering.

9.12.2 Notification Mechanism and Period

DOE CA will post appropriate notice on its web sites of any major or significant changes to this CPS as well as any appropriate period by when the revised CPS is deemed to be accepted.

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation

9.13 Dispute Resolution Provisions

Disputes will be resolved by DOE CA and appropriate DoE management

9.14 Governing Law

This CPS is governed, construed and interpreted in accordance with the laws of State of New South Wales and the Commonwealth of Australia.

9.15 Compliance with Applicable Law

DOE CA complies with applicable laws of State of New South Wales and the Commonwealth of Australia. Export of certain types of software used in certain DOE CA public certificate management products and services may require the approval of appropriate public or private authorities. Parties (including the DOE CA, subscribers and Relying Parties) agree to conform to applicable export laws and regulations as pertaining to the Commonwealth of Australia.

9.16 Miscellaneous Provisions

9.16.1 Compelled Attacks

DOE CA is subject to NSW and Australian jurisdiction and regulatory framework. DOE CA will use all reasonable legal defence against being compelled by a third party to issue certificates in violation of this CPS.

9.16.2 Entire Agreement

DOE CA will contractually obligate every RA involved with Certificate issuance to comply with this CPS and all applicable Industry guidelines. No third party may rely on or bring action to enforce any such agreement.

9.16.3 Assignment

Entities operating under this CPS cannot assign their rights or obligations without the prior written consent of DOE CA

9.16.4 Severability

If any provision of this CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CPS will be interpreted in such manner as to effect the original intention of the parties

9.16.5 Enforcement (Attorney's Fees and Waiver of Rights)

DOE CA may seek indemnification and attorneys' fees from a party for damages, losses and expenses related to that party's conduct. DOE CA's failure to enforce a provision of this CPS does not waive DOE CA's right to enforce the same provisions later or right to enforce any other provisions of this CPS. To be effective any waivers must be in writing and signed by DOE CA

9.17 Other Provisions

No Stipulation