



CERTIFICATION PRACTICE STATEMENT
Version 3.1

Date of publication: 2 November 2010
Effective date: 2 November 2010

Copyright © 2010 DIGICERT Sdn Bhd
All rights reserved

IMPORTANT NOTICES

This Certification Practice Statement ('CPS') describes the policies, practices and procedures employed by DIGICERT Sdn Bhd ('DIGICERT') to perform Certification Authority services.

DIGICERT maintains sole rights and property to this CPS. DIGICERT disclaims any warranty whatsoever in relation to the use of this CPS by parties not covered within DIGICERT's public key certification services described in **CPS Part 2**.

Subscribers of DIGICERT's public key certification services are advised to become familiar with public key cryptography, digital signatures and certificates; the requirements under the Digital Signature Act 1997 ('DSA') and the Digital Signature Regulations 1998 ('DSR'); and the rights, duties and liabilities of the licensed Certification Authority ('CA'), the subscriber and the relying party before applying for a certificate from DIGICERT.

Before the subscribers can communicate the certificate to others, the subscribers must accept the certificate. By accepting the certificate, they are making important representations.

Subscribers are responsible for deciding on the class of certificate that is appropriate for their needs. Relying parties are responsible for deciding on whether to rely on certificates issued by DIGICERT. DIGICERT recommends that relying parties confirm the validity of the certificates by checking with the recognised repositories before relying upon a digital signature.

Subscribers can generate their own key pair or request for the generation of key pair from DIGICERT. DIGICERT is not responsible to keep the subscribers' private keys. Subscribers must protect their private keys in a trustworthy manner and notify DIGICERT immediately upon any compromise of their private key.

Subscribers may be informed by DIGICERT of the need to re-sign the data with the digital signature, as the value of the digital signature decreases with time.

The provisions of this CPS, which may be amended from time to time, are incorporated into all certificates that refer to this CPS, and which are issued on or after the effective date of publication of this CPS.

This CPS shall not be reproduced, whether in full or in part, in any form whatsoever or be stored in any reproducible form whether electronic or otherwise without the prior consent of DIGICERT. This consent must be obtained by contacting:

DIGICERT Sdn Bhd (457608-K)
No. 3-20 & 3-22, Jalan Jalil Perkasa 14
Aked Esplanad, Bukit Jalil
57000 Kuala Lumpur, Malaysia
Tel: +603 8992 8800
Fax: +603 8992 8810
Email: cps-request@digicert.com.my

Table of Contents

1.0	Preface	6
1.1	Overview.....	6
1.2	Citation of CPS.....	7
1.3	Notation Format.....	7
1.4	Publication and Notification.....	7
1.5	Amendment of CPS	8
1.6	CPS Approval Procedures.....	9
1.7	Customer Service and Acknowledgement.....	9
1.7.1	Acknowledgement.....	9
1.7.2	Customer Service Contact Details	9
1.8	Acronyms and Abbreviations	10
2.0	DIGICERT Certification Infrastructure	11
2.1	Trust Infrastructure	11
2.2	Certificate Classes	15
2.2.1	Class 1 Certificates (Digisign ID)	15
2.2.2	Class 2 Certificates (Individuals)	15
2.2.3	Class 2 Certificates (Organisation).....	16
2.3	Certificate Profile.....	17
2.3.1	Version Number.....	18
2.3.2	Certificate Extensions.....	18
2.3.3	Algorithm Object Identifiers.....	21
2.3.4	Name Forms.....	21
2.3.5	Processing Semantics for the Critical Certificate Policy Extension	21
2.4	CRL Profile	21
2.4.1	Version Number(s).....	22
2.4.2	CRL and CRL Entry Extensions	22
3.0	DIGICERT Operational Requirements	24
3.1	Certificate Application	24
3.1.1	Key Generation and Protection	24
3.1.2	Certificate Application	24
3.1.3	Validation of Certificate Applications.....	27
3.2	Certificate Issuance.....	29
3.2.1	Certificate Acceptance.....	29
3.2.2	Refusal to Issue a Certificate	29
3.2.3	Time of Certificate Issuance	29
3.2.4	Certificate Validity and Operational Periods	31
3.2.5	Representation upon Issuance of Certificates	31
3.3	Usage of Certificates.....	32
3.4	Certificate Revocation and Suspension	33
3.4.1	Revocation by DIGICERT.....	33
3.4.2	Revocation by Subscriber	34
3.4.3	CRL Issuance Frequency.....	36
3.4.4	Revocation Status.....	36
3.5	Certificate Expiration.....	36
3.5.1	Notice of Expiration	36
3.5.2	Effect of Certificate Expiration	37
3.5.3	Renewal of Certificate.....	37
3.6	Security Audit Procedures.....	37
3.6.1	Types of Event Recorded.....	37
3.6.2	Frequency of Processing Log.....	38
3.6.3	Retention Period for Audit Log.....	38
3.6.4	Protection of Audit Log.....	38
3.6.5	Audit Log Backup Procedures	38
3.6.6	Audit Collection System.....	38
3.7	Records Archival	39
3.7.1	Retention Period for Archive	39
3.7.2	Protection of Archive	39
3.7.3	Archive Backup Procedures.....	39
3.7.4	Archive Collection System (Internal or External)	39

3.7.5 Procedures to Obtain and Verify Archive Information.....	39
3.8 Compromise and Disaster Recovery.....	40
4.0 Security Controls.....	40
4.1 Physical Controls.....	40
4.2 Procedural Controls.....	40
4.2.1 Trusted Roles.....	40
4.2.2 Number of Persons Required per Task.....	40
4.2.3 Identification and Authentication for Each Role.....	40
4.3 Personnel Controls.....	41
4.3.1 Personnel Management.....	41
4.3.2 Background Check Procedures.....	41
4.4 Key Management Controls.....	41
4.4.1 Key Pair Generation and Installation.....	41
4.4.2 Private Key Protection.....	43
4.5 Logical Access Controls.....	44
4.6 Information Security Controls.....	44
4.6.1 Computer Security Requirements.....	44
4.6.2 Computer Security Rating.....	44
4.7 Cryptographic Module Engineering Controls.....	45
5.0 General Provisions.....	45
5.1 Obligations.....	45
5.1.1 CA Obligations.....	45
5.1.2 Subscriber Obligations.....	46
5.1.3 Relying Party Obligations.....	46
5.2 Liability.....	47
5.2.1 CA Liability.....	47
5.3 Financial Responsibility.....	48
5.3.1 Fiduciary Relationships.....	48
5.4 Interpretation and Enforcement.....	48
5.4.1 Governing Law.....	48
5.4.2 Severability, Survival, Merger, Notice.....	49
5.4.3 Dispute Resolution Procedures.....	49
5.5 Fees.....	49
5.5.1 Certificate Issuance or Renewal Fees.....	49
5.6 Publication and Repository.....	49
5.6.1 Publication of CA Information.....	49
5.6.2 Frequency of Publication.....	50
5.6.3 Repositories.....	50
5.7 Compliance Audit.....	50
5.7.1 Frequency of Entity Compliance Audit.....	50
5.7.2 Identity/Qualifications of Auditor.....	50
5.7.3 Audit Coverage.....	50
5.7.5 Actions Taken as a Result of Deficiency.....	50
5.7.6 Communication of Results.....	51
5.8 Confidentiality.....	51
5.8.1 Types of Information to be Kept Confidential.....	51
5.8.2 Types of Information Not Considered Confidential.....	52
5.8.3 Disclosure of Certificate Revocation/Suspension Information.....	52
5.8.4 Release to Law Enforcement Officials.....	52
5.9 Intellectual Property Rights.....	52
5.10 Limitations on Usage of Services.....	53
5.11 Conflict of Provisions.....	53
5.12 Interpretation and Validity of this CPS.....	54
5.13 Force Majeure.....	54
5.14 Exceptions.....	54
6.0 Appendices.....	55
6.1 Glossary of Terms.....	55
6.2 List of Certificates for Enterprise CA.....	60
6.3 Document Signer Certificates Issuance - Process Flow.....	60

1.0 Preface

1.1 Overview

The purpose of this CPS is to describe the policies, practices and procedures employed by DIGICERT to perform Certificate Authority services. It outlines the procedures of issuing, managing, suspending, revoking and renewing certificates. The CPS is intended to legally bind all parties that intend to use and validate certificates; governing their rights, duties and liabilities in this contract.

The CPS is divided into 6 sections:

- Part 1 provides preliminary information pertaining to this CPS.
- Part 2 describes the trust model and the key components within DIGICERT's Public Key Infrastructure ('PKI'). This section further elaborates on the important functions of each entity and its role within the PKI.
- Part 3 explains the procedures and operational requirements for the application, issuance, revocation and renewal of certificate. A life-cycle approach is used to describe the certification process.
- Part 4 demonstrates the critical security measures and controls employed by DIGICERT in providing trustworthy certification services.
- Part 5 outlines the important legal provisions. In this section, DIGICERT's obligations, limitations and warranties will be highlighted.
- Part 6 contains the definition of specific technical and legal terminology used throughout this CPS.

It is important that potential subscribers fully understand the contents of this CPS before submitting a certificate application.

1.2 Citation of CPS

This CPS is to be cited in other documents as "DIGICERT Certification Practice Statement" or the "DIGICERT CPS". It is cited as "CPS" or "CPS Part _" within this document. The version number of the CPS must be appended after the above citation phrase (e.g. Version 1.1). A Uniform Resource Locator ('URL') which points to the latest CPS available at DIGICERT's web site must be included in the citing document.

1.3 Notation Format

The following notation format will apply throughout this CPS:

- electronic references, all email addresses, URL references and other similar items will be in italics (e.g. *customercare@digicert.com.my*, *<http://www.digicert.com.my>*)
- all references to a particular part or section of this CPS will be in bold (e.g. **CPS Part 3**); and
- the first instance of key words referred to in the Glossary of Terms in **CPS Part 6** will be underlined (e.g. digital signature, Certification Authority).

1.4 Publication and Notification

This CPS can be obtained:

- in electronic form via DIGICERT's Internet servers at <http://www.digicert.com.my>

To maintain integrity of this document, the web-based version of the CPS must be viewed using SSL-enabled browsers, e.g. Netscape Navigator 4.05 and above, or Microsoft Internet Explorer 4.73 and above.

- in electronic form via email from CPS-request@digicert.com.my

The electronic copy of this CPS is currently available in PDF format only.

- in paper form by contacting:

DIGICERT Sdn Bhd (457608-K)
No. 3-20 & 3-22, Jalan Jalil Perkasa 14
Aked Esplanad, Bukit Jalil
57000 Kuala Lumpur, Malaysia
Tel: +603 8992 8800
Fax: +603 8992 8810
Attn: CPS Request

Business Inquiries, Certification services, PKI and technical inquiries:
Email: customercare@digicert.com.my

If the CPS is requested in paper form, all costs of printing and mailing will be borne by the requestor.

From time to time DIGICERT may make changes to its practices in order to improve its services. Some of these changes may require an amendment to the CPS. These updates will be posted at DIGICERT's web site at URL <http://www.digicert.com.my/cps/updates>. Please refer to **CPS Part 1.5** for details on amendment of the CPS.

1.5 Amendment of CPS

DIGICERT reserves the right to amend this CPS at any time (prospectively and not retroactively). Amendments to the CPS will be made available either as an amended version of the CPS or retrospectively can be posted in the Notices section of DIGICERT's web site at the following URL <http://www.digicert.com.my/CPS/updates>. These amendments shall supersede any conflicting provisions of the referenced version of the CPS.

The amendments will become enforceable automatically within fourteen (14) working days of this CPS being made available at the DIGICERT's web site unless DIGICERT explicitly states otherwise or issues a notice of withdrawal prior to the end of the fourteen (14) day period.

1.6 CPS Approval Procedures

This CPS and any subsequent changes are approved by the Director of DIGICERT.

1.7 Customer Service and Acknowledgement

1.7.1 Acknowledgement

Prior to applying for a certificate and accepting the terms and conditions of this CPS, the subscribers acknowledge that they have been advised to have prerequisite knowledge regarding the following information:

- public key cryptography;
- digital signatures and certificates;
- the requirements under the DSA and the DSR; and
- the rights, duties and liabilities of the licensed Certification Authority ('CA'), subscriber and relying party.

The subscribers can obtain the above information or documentation from DIGICERT.

1.7.2 Customer Service Contact Details

Subscribers are advised to consult DIGICERT's web site at <http://www.digicert.com.my> for relevant information and assistance. A list of terms and definitions are also included in **CPS Part 6.1** to assist the subscribers.

For further assistance, please contact:

DIGICERT Sdn Bhd (457608-K)
No. 3-20 & 3-22, Jalan Jalil Perkasa 14
Aked Esplanad, Bukit Jalil,
57000 Kuala Lumpur, Malaysia
Tel: +603 8992 8800
Fax: +603 8992 8810

Business inquiries, Certification services, PKI and technical inquiries:

Email: customercare@digicert.com.my

1.8 Acronyms and Abbreviations

ARL	Authority Revocation List
CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DSA	Digital Signature Act 1997
DSR	Digital Signature Regulations 1998
DN	Distinguished Name
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
IP	Internet Protocol
ISO	International Standard Organisation
ITU	International Telecommunications Union
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RP	Registration Personnel
RSA	Rivest, Shamir, Adleman (see CPS Part 6.1 for definition)
SSL	Secure Socket Layer
URL	Uniform Resource Locator
WWW	World Wide Web
X.509	ITU-T standard for certificates format

2.0 DIGICERT Certification Infrastructure

2.1 Trust Infrastructure

DIGICERT's public key certification services are intended for local and foreign organisations and individuals (end-entities) to conduct secure electronic commerce in the open communication network. To achieve this objective, three key aspects must be adequately addressed:

- a robust PKI trust model to facilitate the management, control, issuance, revocation and renewal of digital certificates;
- the effective use of digital signatures in ensuring non-repudiation, authentication and integrity of electronic documents and transactions; and
- the uniformity of service and standards across DIGICERT and its appointed RAs.

A simplified overview of DIGICERT's PKI model can be diagrammatically represented as follows:

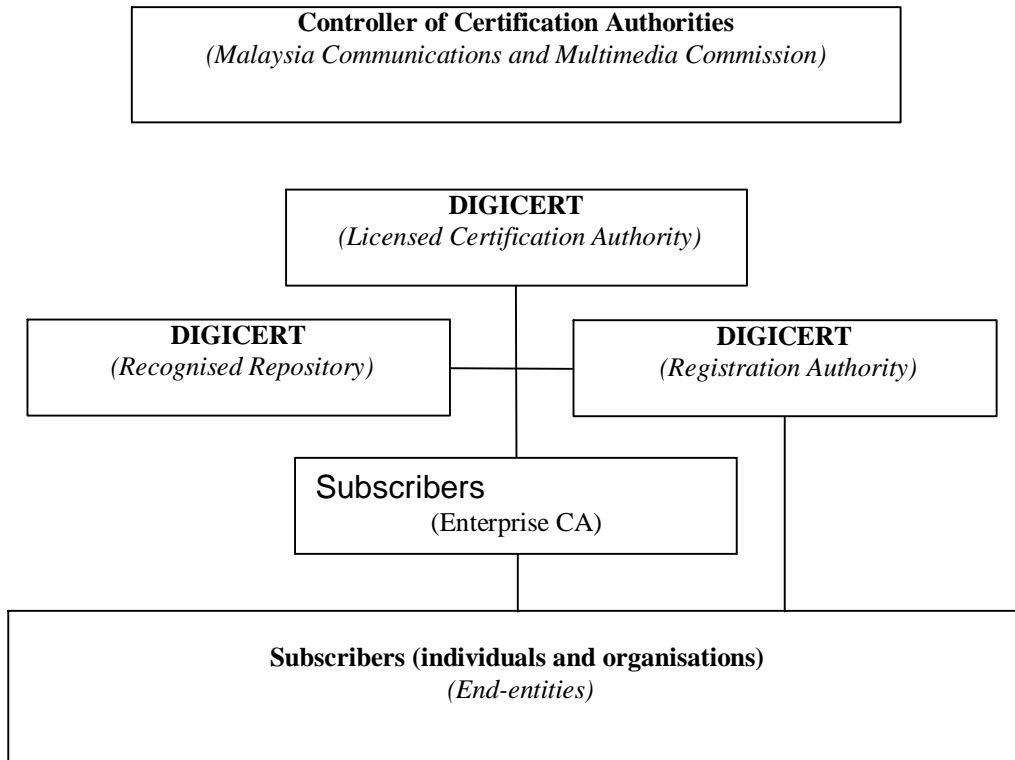


Figure 1 DIGICERT PKI TRUST MODEL

Controller of CA

The function of the Controller of CA ('the Controller') is conceived under the DSA. The Controller is designated by the Minister to monitor, regulate and ensure the legitimacy of CA operations in Malaysia.

The Office of the Controller is the regulatory agency established under the jurisdiction of the Ministry of Communications and Multimedia Commissions. It is fully empowered to issue licences to CAs and certificates of recognition to Repository and Date/Time stamp service providers and Foreign CA. The Office of the Controller is not an entity in DIGICERT's PKI hierarchy.

DIGICERT Sdn Bhd (Licensed CA)

DIGICERT is a licensed CA operating in compliance with the requirements of the DSA and the DSR. In electronic commerce, trust involves the combination of secure technology with reliable, visible processes for the identification and authentication of all parties. DIGICERT uses a trustworthy certificate management system (see **CPS Part 4**) to provide public key certification services to its subscribers.

The policies and practices adopted by DIGICERT are as important as the security attributes of the certificate management system. DIGICERT ensures that the policies and practices conform to industry standard DIGICERT's public key certification services have been designed to address the requirements of a diverse group of users as well as to comply with the DSA and DSR. This CPS sets out DIGICERT's practices to ensure the uniformity of its services and standards. DIGICERT's RAs will operate in accordance with the requirements of this CPS.

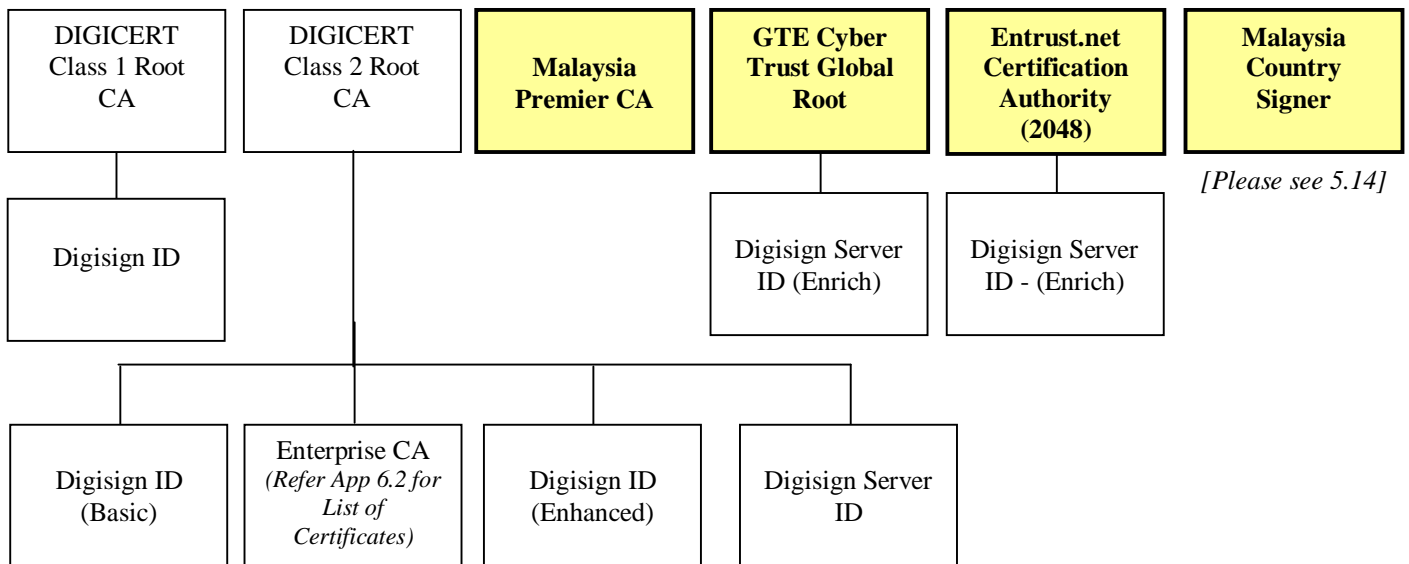


Figure 2 DIGICERT PKI HIERARCHY

DIGICERT Root CA is owned and operated by DIGICERT. It is used to issue certificates to Primary CA.

DIGICERT Root CA and other issuing CA are also owned and operated by DIGICERT. The key length is 2048 bits and it is created in a trustworthy environment. The Root CAs are categorised according to the certificate policies. Therefore, there can be a chain of certificates in support of each digital signature.

DIGICERT acts as the main naming authority in the PKI structure. The naming convention for all subjects of certificates registered through RAs will be determined by DIGICERT. The naming convention for Enterprise CA will be determined by DIGICERT on request from the respective Enterprise CA.

If the recipient does not know the CA of the signer of a given message, the recipient can search for the CA's certificate from the recognised repositories. Recipients are also advised to refer to the Controller's web site to view the CA's licence and disclosure record.

Registration Authorities (RAs)

RAs are trusted entities appointed by DIGICERT to assist subscribers in applying for certificates, to approve certificate requests and/or to help DIGICERT in revoking certificates. The functions that the RAs shall carry out vary from case to case but shall also include personal authentication, token distribution, revocation reporting, name assignment and subscriber's key generation.

The organisations that are appointed as Registration Authority (RA) for DIGICERT Sdn. Bhd. shall be officially published on DIGICERT's website and other printed materials

deemed necessary and copyrighted by DIGICERT. The list of DIGICERT's Registration Authorities is available at <http://www.digicert.com.my/ra.htm>

Recognised Repository

The repository service is fundamental and critical to the operation of an open PKI. DIGICERT will operate as a recognised repository that complies with the requirement of the DSA and the DSR. The repository is a publicly accessible collection of databases containing the certificates of its subscribers, the most recent Certification Revocation List ('CRL') and DIGICERT's Root certificate. DIGICERT's disclosure records are maintained by the Controller.

DIGICERT will promptly publish the certificates, CRL and other information consistent with this CPS, the DSA and the DSR.

Enterprise CA

In a distributed PKI model, organisations may wish to become the issuer of end-entity certificates. An Enterprise CA shall be the party who accepts applications, verifies, issues and revoke end-entity client certificates, subject to the agreement between Digicert and the party being the Enterprise CA.

Enterprise CA has the authority to act as its own RA.

End-Entities

End-entities are subscribers or relying parties of CA services. They could be individuals or organisations who hold and/or rely on digital certificates in electronic transactions. End-entity need not necessarily be a natural person; it could also be a certificate using system such as a secure web server or any organization. Each end-entity could own as many certificates as it needs and may use them for different purposes.

2.2 Certificate Classes

2.2.1 Class 1 Certificates (Digisign ID)

Attribute	Details
Level of trust	Low
Assurance	The subscriber's name is a unique and unambiguous entry in DIGICERT's repository. Class 1 certificates do not provide assurance on the identity of the subscriber.
Issued to	Malaysian and foreign individuals.
Validation	Simple email validation is performed to establish the validity of the email address supplied in the application form of the subscriber.
Possible usage	Class 1 certificates are used for rudimentary security requirements during web browsing and email exchange. They provide assurance that replies to emails are from the same source. They also provide assurance that the email address of the named subscriber is valid. This helps eliminate resource wastage as persons who provide feedback in the form of emails can filter out non-existent addresses.

2.2.2 Class 2 Certificates (Individuals)

Attribute	Details
Level of trust	Intermediate / High (depending on the media user)
Assurance	The subscriber is not a falsely created person insofar as the records of the subscriber's identity are maintained by reliable and independent third parties. RAs and enterprise CA provide that the subscriber is as portrayed by the information provided by government agencies (i.e. National Registration Department, Immigration Department etc). Trust is based on confirmation of the subscriber's identity. This is done through the physical presentation of the identification documents or confirmed against reliable third party database. For example, the RA could request for the original identification document (see CPS Part 3.1.2). All material representations made by the subscriber to DIGICERT, including all information known to the subscriber and represented in the certificate, shall be accurate and complete to the best of the subscriber's knowledge.

Issued to	Malaysian and foreign individuals (aged 18 years and above).
Validation	Strict verification and authentication by the CA, RA or its appointed agents or reliable database is required for software certificates and certificate issued in smart card, virtual smart card (floppy disk) or any other applicable tokens. Confirmation is based upon the official identification document issued by government agencies. The reliability of the information is determined at the sole discretion of the CA, RAs or Enterprise CA or database owner.
Possible usage	Class 2 individual certificates are used for communications requiring various levels of security. Some possible applications include on-line registration via the web, validation of user-identity for downloading of software or software upgrades and communication of user-ID creation within an organisation.

2.2.3 Class 2 Certificates (Organisation)

Attribute	Details
Level of trust	High.
Assurance	The subscriber is indeed the organisation that owns the secure server and the server has a valid URL as portrayed by the information contained in the certificate. However, the assurance provided is only correct at the time of the application for the certificate. Any subsequent changes to this information will only be known when it is communicated to DIGICERT.
Issued to	Malaysian and foreign legal entities.
Validation	Strict verification and authentication by the CA, RA or its appointed agents is required. The subscriber must appear before the Registration Officer at DIGICERT along with supporting documentation to prove ownership of the specified domain name of the web service (see CPS Part 3.1.2). The Registration Officer must be convinced of the validity and legitimacy of the legal entity as claimed by the documentation produced.
Possible usage	Class 2 certificates (organisation) are used for high-level security requirements. Examples of applications include the authentication of servers that contain private or confidential data, <u>electronic commerce</u> including <u>Electronic Data Interchange</u> (EDI) and electronic banking.

2.3 Certificate Profile

This section describes the profile of certificates issued by DIGICERT. Some of the important elements of this profile will be highlighted. This enables users of this CPS to understand the structure of a certificate and identify possible applications to take advantage of this structure.

Certificate format version	Version 3		
Certificate serial number	12345678		
Digital signature algorithm identifier for CA	RSA with MD5/SHA-1		
CA distinguished name	c=MY, o=DIGICERT Sdn Bhd		
Validity period	As per business contract terms requires but not exceeding three years as sanctioned by DSA 1997 Section 59. Most common validity period applies is either 1 year or 2 years or 3 years. e.g. 2 years validity: start = 01/01/2006 end = 01/11/2008		
Subject distinguished name	c=MY, o=DIGICERT Sdn Bhd, cn=Ali (with enhance option)		
Subject public key information	RSA		
CA unique identifier	OPTIONAL		
Subject unique identifier	1.NRIC Number; or 2. Passport Number; or 3.Any Other Acceptable Unique Identifier.		
Type	Criticality	Value	Standard extensions
Type	Criticality	Value	Standard extensions
CA signature	MD5/ SHA-1		

Figure 3 X.509 v3 Certificate format

All the fields of the X.509 version 3 certificate formats will be used except for following:

- issuer unique identifier.

2.3.1 Version Number

DIGICERT's certificates adopt the X.509 version 3 standard.

2.3.2 Certificate Extensions

DIGICERT issues certificates that comply with the X.509 (Amendment 1 to ISO / IEC 9594-8:1995) certificate format (see **Figure 3**). This standard provides DIGICERT with management and administrative controls to ensure that the application of the certificates is consistent with its policies. Such control can be achieved by defining the policies in the certificate extensions. A standard Object Identifier indicates the function of each extension.

Each ISO / IEC 9594-8:1995(E) extension comprises two fields:

- Criticality; and
- Value.

The 'Criticality' field is a single-bit toggle flag. When set to true, this indicates that the corresponding 'Value' field contains data that cannot be ignored by an application. For humans, this translates into understanding the data within the 'Value' field and having the knowledge of handling these data. For example, it could contain a disclaimer on the use of the certificate or a URL that points to a location where this information is available. When set to false, it indicates that the data within the 'Value' field can be ignored.

The 'Value' field holds any necessary data that is appended to the certificate.

As described previously, the X.509 "Amendment 1 to ISO / IEC 9594-8:1995" defines a number of extensions. These extensions can be categorised into the following four groups:

- Key Information Extensions

These extensions define the usage of a public key pair and certificate.

■ Policy Information Extensions

These extensions define a means for the CA to specify the method of interpretation and the use of the certificate. There are 2 extensions in this group:

- Certificate policy extension (see **CPS Part 2.3.6**).
- Policy mapping extension serves a similar purpose to the certificate policies extension. However, it applies only to cross certificates. This field allows an application to search and establish a set of consistent policies across multiple CAs.

■ User and CA Attribute Extensions

These extensions provide a means of specifying additional information regarding the subscriber and the CA that issued the certificate.

■ Certification Path Extensions

These extensions are used in cross-certified environments e.g. where two CAs cross-certify each other. They allow CAs to limit third-party trust in such an environment. This group can be subdivided into:

- Basic constraint extension specifies whether the subject of the certificate shall act as a subscriber only or as both a subscriber and a CA.
- Name constraints extension
- Policy constraints extension

A number of X.509 version 3 certificate extensions are included in certificates issued by DIGICERT. These are outlined in **CPS Part 2.3.2.1**. The X.509 version 3 certificate extensions, which are never present in certificates issued by DIGICERT, are outlined in **CPS Part 2.3.2.2**.

2.3.2.1 Supported Extensions

The following certificate extensions are used in DIGICERT PKI:

Extension	Criticality	Optional	Notes
AuthorityKeyIdentifier	No	No	<ul style="list-style-type: none"> • contains a 20 byte hash of the subjectPublicKeyInfo

			in the CA certificate
			<ul style="list-style-type: none"> only element [0] AuthorityKeyIdentifier is filled.
SubjectKeyIdentifier	Yes	No	<ul style="list-style-type: none"> contains a 20 byte hash of the subjectPublicKeyInfo in the CA certificate
KeyUsage	Yes	No	<ul style="list-style-type: none"> elements [5] keyCertSign and [6] cRLSign are set for CA certificate
PrivateKeyUsagePeriod	No	No	<ul style="list-style-type: none"> notafter is always used notbefore is always used
SubjectAltName	No	Yes	<ul style="list-style-type: none"> GeneralName – choices [0], [3] and [5] are not implemented.
BasicConstraints	Yes	No	<ul style="list-style-type: none"> only the CA Boolean is used
CertificatePolicies	Yes	No	<ul style="list-style-type: none"> only policyIdentifier element is supported with up to 10 OIDs <u>policyQualifiers</u> contains URL indicating the location of DIGICERT CPS
CRLDistributionPoints	No	No	<ul style="list-style-type: none"> only 1 distribution point name is included in each certificate only element [0] (distribution point) is used and includes the full DN

2.3.2.2 Unsupported Extensions

The following X.509 version 3 certificate extensions are optionally used whenever applicable in this PKI:

- extended key usage;

- policy mappings;
- name constraints;
- policy constraints;
- issuer alternative name; and
- subject directory attributes.

2.3.3 Algorithm Object Identifiers

Algorithm	Object Identifier
RSA-with-SHA1	1 2 840 113549 1 1 5
RSA-with-MD5	1 2 840 113549 1 1 4

2.3.4 Name Forms

The Distinguished Name ('DN') and subject DN fields contain the full X.500 DN of the certificate issuer or certificate subject. If the SubjectAltName extension is present in a certificate, it contains the certificate subject's rfc822Name with an optional email address are used.

2.3.5 Processing Semantics for the Critical Certificate Policy Extension

The only certificate extension, which shall be identified as critical in certificates issued by this CA, is the CRLDistributionPoints extension. The CRL or ARL will be retrieved from the CRL distribution point directory entry indicated in the certificate.

2.4 CRL Profile

The following fields of the X.509 version 2 CRL format are used in this PKI:

- version: set to v2;

- signature: identifier of the algorithm used to sign the CRL;
- issuer: Distinguished Name of the CA issuing the CRL;
- this update: time of CRL issue;
- next update: time of next expected CRL update; and
- revoked certificates: list of revoked certificate information.

2.4.1 Version Number(s)

CRLs issued by DIGICERT are X.509 version 2 CRL.

2.4.2 CRL and CRL Entry Extensions

A number of X.509 version 2 CRL and CRL entry extensions are used in this PKI. These are outlined in **CPS Part 2.4.2.1**. The X.509 version 2 CRL and CRL entry extensions which are never present in CRLs issued by DIGICERT are outlined in **CPS Part 2.4.2.2**.

2.4.2.1 Supported Extensions

The following CRL and CRL entry extensions are used in this PKI:

X.509 v2 CRL Extension	Criticality	Optional	Notes
AuthorityKeyIdentifier	No	No	<ul style="list-style-type: none"> ▪ . only element [0] (AuthorityKeyIdentifier) is filled in ▪ . contains a 20 byte hash of the subjectPublicKeyInfo in the CA certificate
CRLNumber	No	No	<ul style="list-style-type: none"> ▪ . Incremented each time a particular CRL is changed
ReasonCode	No	No	<ul style="list-style-type: none"> ▪ . CRL entry extension – only reason codes [0], [1], [3], [4] and [5] supported [6],[2]
IssuingDistributionPoint	No	No	<ul style="list-style-type: none"> ▪ . Element [0] (distributionPoint) includes the full DN of the

distribution point

- Element [1] (onlyContainsUserCerts) is included for CRLs
- Element [2] (onlyContainsCACerts) is included for s
- Element [1] and [2] are never present together in the same revocation list
- Elements [3] and [4] are not used.

2.4.2.2 Unsupported Extensions

The following X.509 version 2 CRL extensions are not used in this PKI:

- issuer alternative name;
- invalidity date;
- certificate issuer; and
- delta CRL indicator.

3.0 DIGICERT Operational Requirements

3.1 Certificate Application

3.1.1 Key Generation and Protection

Subscribers are given the option to either generate their own key pairs or request DIGICERT to generate the key pairs. Subscribers who choose to generate their own key pairs should be responsible for ensuring that the key pairs are generated in a trustworthy manner. When DIGICERT creates subscriber key pairs, DIGICERT warrants that it will not keep or escrow a copy of the subscriber’s private key unless with consent by subscriber. The following key generation options are available:

Certificate class	Options available
Class 1 (Digisign ID)	CA generates key.
Class 2 (Digisign ID Basic)	CA or Subscriber generates key.
Class 2 (Digisign ID Enhanced)	CA or Subscriber generates key.
Class 2 (Digisign Server ID)	CA or Subscriber generates server key pair.
Class 2 (Digisign Server ID (Enrich))	CA or Subscriber generates server key pair.
Class 2 (Enterprise CA)	CA or Enterprise CA generates key pair

3.1.2 Certificate Application

The following section will outline the procedures in applying for and reviewing of a certificate application. The table below specifies the requirements for obtaining certificates. The table briefly describes the certificate application process based on the certificate policies. Mandatory requirements will be highlighted where necessary.

Certificate	Mode of application
Class 1 (Digisign ID)	Email to customer@digicert.com.my to request for Digisign ID purchase. Alternatively, customers may choose to have a walk in registration. Available to all Malaysian and foreign individuals.

<p>Class 2 (Digisign ID Basic/Enhanced)</p>	<p>Walk-in registration at DIGICERT or its RA. The source of identification documents required to accompany the application is either:</p> <p>One (1) of the following: NRIC / Passport; OR</p> <p>Two (2) of the following: Birth Certificate / Valid Driving Licence / credit card bill / bank statement / Letter of Employment / Certificate of Adoption / any documentation deemed fit by the CA.</p> <p>For Enterprise CA, requests shall have to come from the organisation assuming the role of Enterprise CA itself, subject to prior arrangement between DIGICERT and the Enterprise CA.</p> <p>Online registration at web service provider, the identification documents and information required are set forth by the web service provider and CA.</p> <p>Available to all Malaysian and foreign individuals who are 18 years and above.</p>
<p>Class 2 (Digisign Server ID/Enrich)</p>	<p>Walk-in registration at DIGICERT or any of its appointed RAs. At least two sources of identification documents (Certificate of Incorporation AND/OR Certificate of Registration OR either any two of the following: Memorandum of Association / Articles of Association / Societies Bylaws booklet / Cooperative Bylaws booklet / latest audited financial statement / latest income tax return) should accompany the application. In addition, the server public key and an authorisation letter from the management are required to allow a representative of the organisation to submit this application.</p> <p>Available to all Malaysian and foreign legal entities (except individuals).</p>

The RP of DIGICERT or its RA or the appointed Authorised Personnel of an Enterprise CA is principally responsible for ensuring that the required information is obtained from the subscriber prior to approving the application for a certificate. The application must be

rejected should the information be incomplete or is discovered to be inaccurate upon investigation. The information requirement of each class of certificate is outlined below:

Class 1 (Digisign ID)

- i) name (as indicated on the applicant's NRIC or Passport);
- ii) email address;
- iii) the telephone number;
- iv) postal address (this should be the place where the applicant will reside for more than one year in the immediate future, if no such place is available, the current place of residence will suffice);
- v) the new NRIC / Passport number;
- vi) date of birth;
- vii) a valid credit card number and its expiration date (if applicable)

Class 2 (Digisign ID Basic/Enhanced)

- i) name (as indicated on the applicant's NRIC or Passport);
- ii) email address(optional);
- iii) the telephone number;
- iv) postal address (this should be the place where the applicant will reside for more than one year in the immediate future, if no such place is available, the current place of residence will suffice);
- v) the new NRIC / Passport number;
- vi) date of birth;
- vii) challenge pass phrase (if applicable)

Class 2 (Digisign Server ID / Enrich)

- i) domain name of the server;
- ii) name of the organisation that operates the server;
- iii) name of the organisation unit within the organisation (specified in (ii) above) that operates the server; (optional)
- iv) mailing address of the organisation (as specified in (ii) above);
- v) the proposed distinguished name of the server;
- vi) the telephone number and facsimile number of the organisation;
- vii) email address through which the organisation may be contacted; and

vii) the name of the contact person in the organisation who is responsible of the server.

Class 2 (Enterprise CA) Similar to Individual Class 2 certificates mentioned above. Any changes in the requirements shall be reflected in the agreement between DigiCert and Enterprise CA.

3.1.3 Validation of Certificate Applications

The validation requirements of applicants for certificates differ between the classes of certificates. The level of validation detail is commensurate with the level of trust guaranteed by the certificate. Should the validation of the application fail at any stage due to reasons outside of the RA’s control, the application should be rejected (see **CPS Part 3.2.2**).

Upon receipt of the application details from an applicant, the RP at DIGICERT or its RA will perform the following validation requirements to identify the applicant:

Certificate class	Validation requirements
Class 1 (Digisign ID)	The email address of the user must be from the domain of a valid Internet Service Provider (ISP). Web-based email accounts will be rejected. The validity of the email address is confirmed by the email reply from the subscriber.
Class 2 (Digisign ID Basic/Enhanced)	The identity of the applicant is verified through the presentation of the identification documents as described in CPS Part 3.1.2 . The data of the applicant for online enrolment is verified against reliable database. Automated online system will compares the applicant Identification Card/ Passport Number and other personal information against the database.
Class 2 (Enterprise CA)	The identity of the applicant is verified by the Enterprise CA as described by CPS Part 3.1.2 and agreement between DIGICERT and the Enterprise CA.
Class 2 (Digisign Server ID/Enrich)	The scope of verification for Class 2 Server applicants is limited to the organisation that operates the server. The identity of the applicant is verified through the presentation of two identification documents as described in CPS Part 3.1.2 .

If the application is approved, the following table summarises the nature of communication for the different classes of certificates:

Certificate class	Nature of communication
Class 1 (Digisign ID)	The subscriber shall receive the digital certificate and PIN number to access the private key via separate e-mail.
Class 2 (Digisign ID Basic)	The subscriber shall receive the certificate and the related private key in softcert, smart card, USB token, floppy disk or any other applicable tokens. A PIN number to access the private key will be sent later to the subscriber via regular mail.
Class 2 (Digisign ID Enhanced)	The subscriber shall receive the certificate and the related private key in a smart card or any other applicable tokens. A PIN number to access the private key will be sent later to the subscriber via regular mail.
Class 2 (Digisign Server ID/Enrich)	The subscriber shall receive the certificate in a floppy disk or smart card.
Class 2 (Enterprise CA)	The subscriber shall receive the certificate and the related private key in a media agreed upon by the Enterprise CA and DIGICERT.

3.2 Certificate Issuance

3.2.1 Certificate Acceptance

Certificates are issued to the subscribers upon successful processing of the application and the acceptance of the certificates by the subscribers (see **CPS Part 3.3**).

Subscribers demonstrate their acceptance of the certificate by adhering to the following procedures:

Certificate class	Nature of communication
Class 1 (Digisign ID)	For Digisign ID, subscriber indicates acceptance by using the certificate after receiving the necessary PIN.
Class 2 (Digisign ID Basic/Enhanced)	Subscriber indicates acceptance by receiving/downloading the certificate from DIGICERT or its RAs and/or usage of the digital certificate whichever come first.
Class 2 (Enterprise CA)	Similar to Class 2 (Basic / Enhanced) unless indicated in the agreement between DIGICERT and the Enterprise CA
Class 2 (Digisign Server ID/Enrich)	Subscriber indicates acceptance by physically obtaining the floppy disk/ smart card containing the digital certificate from DIGICERT or its RAs.

The subscriber is advised to verify all details contained within the certificate. Errors or omissions must be communicated immediately to DIGICERT. It is imperative that the subscriber is aware of this requirement. DIGICERT's scope of responsibility extends only to ensure that the information contained within the certificate accurately reflects the information that was provided to DIGICERT by the subscriber during the application stage.

3.2.2 Refusal to Issue a Certificate

DIGICERT shall refuse to issue a certificate if the subscriber provides incomplete, falsified or fraudulent information and, if the identity of the subscriber cannot be verified.

3.2.3 Time of Certificate Issuance

DIGICERT will make reasonable efforts to adhere to the following time-schedule in issuing certificates. However, no guarantees can be provided as circumstances beyond the control of

DIGICERT may inhibit such adherence. In particular, the timeliness of the following schedule will depend on the amount of co-operation received from the subscriber, including but not limited to payment, and the provision of accurate and complete information. Incomplete application forms will invariably cause the application to be delayed or rejected.

All time frames quoted depend upon the receipt of the confirmation to proceed with the application from the applicant. The following sets out the time-schedule for the issuance of certificates:

Class 1 certificate	Class 2 certificate	Class 2 certificate (Server)
<p>The issuance is immediate upon receiving payment and the PIN number will be sent within 3 business days via regular mail.</p>	<p>For the virtual smart card (floppy disk) (Basic only), the issuance is immediate, and the PIN number will be sent within 3 business days via regular mail. For online application, issuance is immediate where the PIN is set by the subscriber.</p> <p>For the smart card (Basic/Enhanced), the issuance requires 7 business days, and the PIN Mailer will be sent within 5 business days via regular mail.</p> <p>For Enterprise CA, the issuance is as per agreement with the Enterprise CA itself.</p>	<p>For the application by organisation for server certificate, the issuance is immediate after the subscriber fulfil all the requirements including providing the supporting documents, key request from the server and the payment.</p> <p>PIN Number for Server ID in smart card will sent within 5 business days via regular mail.</p>

3.2.4 Certificate Validity and Operational Periods

Certificates issued by DIGICERT must be renewed periodically. Renewal procedures can be found in **CPS Part 3.5.3**. All certificates issued by DIGICERT have a validity period of one (1) to three (3) years (whichever applicable).

3.2.5 Representation upon Issuance of Certificates

By issuing certificates DIGICERT makes certain representations to the subscriber and to the subsequent parties relying on the certificates.

DIGICERT makes no representations or guarantees, which includes but is not limited to, the accuracy, integrity, reliability, completeness, fitness for a particular purpose or the authenticity of the information contained within the digital certificate. DIGICERT shall not be liable to any person for any liabilities, damages or claims whatsoever in respect of any loss suffered, economic or otherwise, whether consequential, direct or indirect, resulting from the person's reliance on such information.

DIGICERT makes no further representations and provides no further guarantees of any kind whatsoever to any person regarding the identity of the subscriber to whom DIGICERT has issued a certificate to the extent that such identity has been verified in the manner set out within this CPS.

In addition, subscribers must maintain full responsibility to ensure that their private key is not compromised, stolen, modified or used in an unauthorised manner. The subscribers assume this responsibility upon transmission of the key from DIGICERT (if the subscriber did not generate the key).

In this respect, DIGICERT will not guarantee that the receiving party is the subscriber in person. DIGICERT will only guarantee that the private key was transmitted to an address, whether electronic or otherwise, or to a natural person, designated by the subscriber as being the address or the natural person through which he will receive the private key. DIGICERT will not be liable in any way for damages suffered, whether directly or indirectly, as a result of a person's reliance that the private key was transmitted to the actual intended party.

The subscribers may delegate to another person the responsibilities to prevent compromise, theft, modification, or unauthorised use of the private key. However, this does not negate the delegator of his responsibilities as outlined in the above paragraphs.

By accepting a certificate issued by DIGICERT, the subscriber acknowledges and represents the following to DIGICERT and to persons relying on the information contained within the certificate throughout the validity period of the certificate (until such time that the certificate is revoked, suspended or expired):

- all information contained in the certificate is true to the best of the subscriber's knowledge to the extent that any changes to the information is not made known to DIGICERT or has been made known to DIGICERT but has not been amended by DIGICERT due to an unreasonable time frame or reasons beyond the control of DIGICERT;
- the subscriber promises to notify DIGICERT as soon as practicable of changes to the information contained in the certificate;
- the private key of the subscriber has not been compromised, stolen, modified, or used in an unauthorised manner and the subscriber has taken necessary steps to prevent these from happening;
- the private key of the subscriber is not to be used in any manner other than its intended use as described in **CPS Part 3.3**;
- digital signatures created by the subscriber are used for legal purposes (within the context of applicable local laws) and subject to the terms and conditions within this CPS; and
- digital signatures created by the subscriber are signed with the private key that corresponds to the public key listed in the certificate.

Upon acceptance of the certificate by the subscriber, a copy of the certificate will be published in DIGICERT's repository. This copy will be maintained until such time that the certificate is expired, revoked or suspended.

3.3 Usage of Certificates

The certificates containing public key that is intended for verifying digital signature created using the corresponding private key, should only be used for its intended usage.

Certificates shall not be used in an illegal or discriminatory manner including, but not limited to, trafficking of illegal material, engaging in activities that compromise national security and utilising the certificate for accessing illegal material.

If certificates are used in an illegal manner, DIGICERT will not hesitate to revoke the certificate without prior notice to the subscriber. In addition, future applications made by the subscriber shall be prejudiced against this.

3.4 Certificate Revocation and Suspension

Suspension or Revocation of certificates can occur due to the reasons specified in **CPS Part 3.4.1** and **CPS Part 3.4.2**.

In the event that DIGICERT believes or has reason to believe, due to reliable evidence or while acting in good faith, that a certificate should be suspended or revoked, DIGICERT will take all necessary to do so even if this is without the consent of the subscriber. In most instances, the suspension or revocation occurs when there is a security breach of the private key or the certificate will materially affect the truth of the information reflected in the certificate and thus possibly mislead a person relying on that information.

In the event that the subscriber requested for a revocation or suspension, DIGICERT will take all necessary precautions to verify the identity of the subscriber. Suspension and Revocation will not proceed without the verification that the purported party is indeed the subscriber.

Upon revocation of the certificate, DIGICERT shall within 24 hours indicate that it is revoked by updating the CRL. The CRL will be published in at least one recognised Repository at an interval specified in **CPS Part 3.4.3**. Subscribers with revoked certificates are allowed to reapply for a new certificate at the discretion of DIGICERT. Under no circumstances can the revoked certificate be reinstated to its original state after revocation.

3.4.1 Revocation by DIGICERT

In general, a revocation could be initiated by DIGICERT when one or a combination of the following conditions has occurred:

- upon such instruction from the Controller or upon the requirements of an applicable law.

- the certificate was not issued in accordance with the requirements of Section 29 and 30 of DSA;
- certificates become unreliable due to the following :
 - breach of the private key's security including unauthorised use;
 - the information contained within the certificate as supplied by the applicant has changed in such a manner that it will be grossly inaccurate to allow the certificate to continue to be operative without it being withdrawn and updated;
 - the applicable obligations, terms and conditions under this CPS have been materially breached by the certificate holder; or
 - a material fact contained in the certificate is misstated or known to be misstated.

The above list is not meant to be exhaustive but merely to highlight the more common cases of suspension or revocation. Should the revocation be carried out, a notice of revocation will be sent to the subscriber. This notice will contain:

- a notice that the subscriber's certificate has been revoked;

DIGICERT shall notify the subscriber by email. The contact information of the subscriber that was submitted during the application stage or that was subsequently updated in the digital certificate will be used as the destination for the transmission of this notice.

3.4.2 Revocation by Subscriber

Revocation by a subscriber can be initiated due to the following reasons:

- breach of the private key's security including unauthorised use;
- the media / token containing the private is loss or damaged;

The above list is not meant to be exhaustive but merely to highlight the more common cases of suspension or revocation.

There are currently two options available for the subscriber to initiate a request for revocation:

- walk in to DIGICERT or any of DIGICERT appointed RA's premises and filling in the Revocation of Certificate form; or
- fax in the revocation form to DIGICERT or any of DIGICERT appointed RA's.

The informational content of the message channelled to DIGICERT to initiate revocation will depend on the mode of communication chosen. The following table will summarise this point and include verification procedures to prevent malicious acts of sabotage where a certificate is revoked without the subscriber’s knowledge:

Certificate Class	Verification procedures
Class 1 Digisign ID	<p><u>Revocation</u></p> <p>Required information includes the email address. The system shall email back to confirm request. Upon the request confirmation via email, the certificate shall be immediately revoked.</p>
Class 2 (Digisign ID Basic/Enhanced)	<p><u>Walk-in to DIGICERT or its RA</u></p> <p>Subscriber shall fill in Revocation Request Form or Online Form (if applicable) upon the request for revocation with following details:</p> <ul style="list-style-type: none"> • NRIC/Passport • Reason for revocation is required • Challenge Pass Phrase or any submitted enrolment information (if applicable)
Enterprise CA	<p>Subscribers shall provide the information as above to the Enterprise CA or Digicert upon request for revocation. Unless stated otherwise, Digicert shall assume all requests from Enterprise CA on behalf of subscribers as legitimate.</p>
Class 2 (Digisign Server ID/Enrich)	<p><u>Walk-in to DIGICERT or its RA</u></p> <p>Subscriber shall fill in the Revocation Request Form and provide the following information to DIGICERT or its RA:</p> <ul style="list-style-type: none"> • Company name • Company incorporation number • Certificate number • Reason for revocation <p>An authorisation letter is required if an agent is appointed to for request revocation.</p>

DIGICERT’s decision on whether to revoke the certificate will be final. If the revocation is instructed by the Controller, notice will be sent to the subscriber before the revocation is made. Sufficient time will be given to the subscriber to be heard. The subscriber will be notified via email or regular mail when the certificate is revoked. Upon the successful

revocation of the certificate, the Certificate Revocation List will be updated to reflect this fact within one business day after receiving the request of the revocation.

3.4.3 CRL Issuance Frequency

All revocation will be updated in the CRL automatically after the revocation at the system and DIGICERT shall publish the CRL in its repository and other recognised repository (if available) 24 hours after the certificate being revoked.

3.4.4 Revocation Status

Status of revocation will be made available in a publicly accessible Certificate Revocation List. DIGICERT shall publish the revocation status in the website, which DIGICERT deems appropriate.

3.5 Certificate Expiration

The following section serves to provide the necessary procedures to be carried out by the parties involved. Certificates will expire after it exceeds its deemed operational period as described in **CPS Part 3.2.4**.

3.5.1 Notice of Expiration

DIGICERT will provide notice to the subscriber on the expiry date as follows:

Notice	Class 1 Certificate (Digisign ID)	Class 2 Certificate (Digisign ID Basic/ Enhanced)	Class 2 Certificate (Digisign Server ID/Enrich)
First	Two months	Two months	Two months
Second	One month	One month	One month
Third	One week	One week	One week

The time frames specified above are relative to the expiry date of the certificate. For example, Class 2 (Digisign ID Basic/ Enhanced) certificate users will be notified initially one month prior to the expiry date; the notification will be sent again one week prior to the expiry date.

The expiry notice time frames for certificate issued by RA and Enterprise CA are similar to Class 2 (Basic / Enhanced) unless indicated in the agreement between DIGICERT and the RA/Enterprise CA

DIGICERT shall notify the subscriber by email. The contact information of the subscriber that was submitted during the application stage or that was subsequently updated in the digital certificate will be used as the destination for the transmission of this reminder.

3.5.2 Effect of Certificate Expiration

Expired certificates will not be revoked or removed. Upon expiration of the certificate, subscribers can either:

- cease to be a subscriber; or
- renew the expired certificate.

3.5.3 Renewal of Certificate

The certificate renewal process is similar to an application for a new certificate unless agreed upon the relying parties between the Certification Authority and the Enterprise CA subscriber. However, for all classes of certificates with the exception of Class 1, the subscriber only needs to provide information that has changed since the expiration date of the certificate. Class 1 certificates can only be renewed by re-applying for a new certificate using the same procedure as described in **CPS Part 3.1**.

Subscribers shall be solely responsible to update DIGICERT in regards to any information changes during this renewal process.

3.6 Security Audit Procedures

3.6.1 Types of Event Recorded

All significant security events on DIGICERT CA software are automatically time stamped and recorded in audit trail files. These include but are not limited to the following events:

- successful and failed attempts to create, remove, login as, set reset and change passwords of and revoke privileges of DIGICERT's operative personnel and its Registration Officer;

- failed interactions with the directory including failed connection attempts, read and write operations by DIGICERT CA software; and
- all events related to certificate revocation, security policy modification and validation, DIGICERT CA software start-up and stop, database backup, cross-certification, attribute certificate management, DN change, database and audit trail management, certificate life-cycle management and other miscellaneous events.

3.6.2 Frequency of Processing Log

Critical system events, access attempts and CA software operation events are logged on a daily basis. The audit trail is reviewed at least once per week.

3.6.3 Retention Period for Audit Log

The yearly backup of the audit trails files is retained for ten (10) years under normal operations.

3.6.4 Protection of Audit Log

The audit trail is stored in regular operating system flat files. Audit trail for CA software operation events is digitally signed to ensure integrity. Each log record contains the timestamp, the type of log entry and the identity of log event. A new audit trail file is created when the current audit trail file reaches a preset size. Only the authorised Manager or the Security Officer is authorised to view and process audit trail files.

3.6.5 Audit Log Backup Procedures

Audit trail files are backed up by the System Administrator on a daily, weekly and monthly basis. All files including the latest audit trail file are stored either in a LTO 4 Cartridge media or DAT tape and kept in a secure archive facility.

3.6.6 Audit Collection System

The audit trail accumulation system is part of the CA software system. The log can be viewed using a standard CA Software Administrative Module.

3.7 Records Archival

3.7.1 Retention Period for Archive

The archive of the DIGICERT CA database and audit trail files will be retained for at least ten (10) years.

3.7.2 Protection of Archive

The DIGICERT CA archive media is kept in a fireproof safe and retained in a restricted access facility to which only authorised personnel have access. Protection of the audit trail is as described in **CPS Part 3.6.4**.

3.7.3 Archive Backup Procedures

The archive files are backed up as they are created. Originals are stored on-site and housed with the DIGICERT CA system. Backup of the archive files is stored at a secure and separate geographic location.

3.7.4 Archive Collection System (Internal or External)

The archive collection system (backup facility) for the DIGICERT CA database is internal to the DIGICERT CA system. The archive collection system (backup facility) for the audit trail files is described in **CPS Part 3.6.6**.

3.7.5 Procedures to Obtain and Verify Archive Information

Once a year the archive tapes are retrieved by a Security Officer and verified to ensure that no damage or loss of data has occurred. If any loss has occurred, the backup archive is retrieved to become the new master archive and a new backup is produced.

Once every five-(5) years a new backup of each archive is produced, even if there is no evidence of damage or loss of data on the master or backup archive. For each tape, the new backup becomes the master archive, the previous master archive becomes the backup archive and the previous backup archive tape is securely deleted.

3.8 Compromise and Disaster Recovery

DIGICERT has a comprehensive *disaster recovery* plan to enable complete recovery of all CA systems in the event of a disaster.

4.0 Security Controls

4.1 Physical Controls

The DIGICERT CA system is located in a locked room to which only trusted authorised operative personnel has physical access.

4.2 Procedural Controls

4.2.1 Trusted Roles

The roles and responsibilities of operative personnel employed by DIGICERT are segregated according to their CA function. The System Administrator and PKI Engineer have access to the computer that hosts DIGICERT CA software to maintain the DIGICERT PKI.

4.2.2 Number of Persons Required per Task

Critical CA operations need authorisation from at least one Security Officer. However, the following operations need authorisation from two Security Officers:

- adding and deleting Security Officer;
- creating CA keys;
- issuing cross-certificates;
- creating Key Encryption Card (used to encrypt and decrypt CA keys);
- activating a CA private key for signing activities.

4.2.3 Identification and Authentication for Each Role

The individuals fulfilling any of the trusted roles in DIGICERT possess a smart card for initiating core CA processes. The smart card (which is protected by PIN) is stored in the DIGICERT corporate safe under a dual access control mechanism.

4.3 Personnel Controls

4.3.1 Personnel Management

All DIGICERT operative personnel are competent in their performance and shall provide reasonable assurance of their trustworthiness while serving in a trusted position in the trusted organisation.

4.3.2 Background Check Procedures

All operative personnel in DIGICERT are required to go through a stringent background check.

4.4 Key Management Controls

4.4.1 Key Pair Generation and Installation

4.4.1.1 Key Pair Generation

The DIGICERT CA and Enterprise CA signing key pairs are generated, as and when necessary through proper documented procedures, on hardware and are protected by the master encryption key stored in an ISO 7816 smart card. The digital signature key pair for the subscribers can either be generated by the CA software or, in some cases, by hardware token.

4.4.1.2 Private Key Delivery to Entity

If DIGICERT is requested to generate the key pair, the private key will be stored in a smart card, USB token, virtual smart card (floppy disk) or any other forms of token and shall be delivered securely to subscribers. For the key pair generated by the subscriber using standard browsers, no delivery of the private key is required.

4.4.1.3 Public Key Delivery to Certificate Issuer

If DIGICERT is requested to generate the key pair, the public key will be stored in a smart card, virtual smart card (floppy disk) or any other forms of token and delivered securely to subscribers.

4.4.1.4 CA Public Key Delivery to Users

The CA verification public key (CA certificate) will be made available to subscribers in a recognised repository.

4.4.1.5 Key Sizes

DIGICERT Root CA signing key pair is 2048 bits and the signing key pair of other CA at the lower level of the PKI hierarchy is 1024 bits.

4.4.1.6 Public Key Parameters Generation

DIGICERT employs and recommends its subscribers to use digital signature schemes approved by the DSA and the DSR.

4.4.1.7 Hardware/Software Key Generation

The keys generated by DIGICERT are generated by either hardware for CA Keys and subscribers keys or software for subscriber's keys. However, hardware tokens, for example crypto smart cards can be used to generate key pair.

4.4.1.8 Key Usage Purposes (as per X.509 v3 key usage field)

Certificates issued by DIGICERT contain the **KeyUsage** certificate extension restricting the purposes to which the certificate can be applied.

The signing key pair is used to provide authentication, integrity and support for non-repudiation services. The DIGICERT CA and Enterprise CA signing key is used to sign certificates; CRLs issued by DIGICERT.

The encryption key pair is used to protect a symmetric key used to encrypt data, and provides confidentiality services.

4.4.1.9 Public Key Archival

The CA signing key pair and verification public key certificates are backed up in the DIGICERT CA database. The DIGICERT database is archived according to the procedures described in **CPS Part 3.7.4**.

4.4.1.10 Usage Periods for the Public and Private Keys

The validity period of the CA key pairs is five years unless agreed by the subscriber of Enterprise CA and Digicert. For Root CA, the validity is 20 years.

4.4.2 Private Key Protection

4.4.2.1 Standards for Cryptographic Module

The cryptographic module used by DIGICERT CA hardware and software to generate keys is designed to comply with international standards.

4.4.2.2 Private Key Multi-Person Control

Actions that require the authorisation from two persons include:

- assigning/removing Registration Officer privileges to/from Security Officer;
- creation of new certificate policies;
- activating a given CA's private key to initiate certificate generation;
- generation of CA key pair; and
- cross-certifying with other CAs.

Other actions require the authorisation from a single person.

4.4.2.3 Private Key Escrow, Backup and Archival

Escrow of private keys by an external third party is not performed.

The DIGICERT CA private keys are backed up in the CA database in an encrypted format. The subscriber's private signing key is never backed up, to provide support for non-repudiation services. However, subscribers are advised to make a copy of their signing keys. The DIGICERT signing key is encrypted and its integrity is protected by the CA master keys stored in the smart card.

The CA database is backed up at a minimum on a daily basis.

Recovery of information from the CA database can only be done by the Security Officer and PKI Engineer.

4.4.2.4 Private Key Activation and Entry into Cryptographic Module

The CA signing private keys are generated by the hardware, within the cryptographic module. Private keys are stored encrypted in the cryptographic module. For both the software and hardware token cases, they are decrypted only when they are actually being used.

4.4.2.5 Method of Deactivating Private Key

The CA signing private keys remain active for the period that an authorised person logs into the DIGICERT CA system. The login period ends when the CA system is shut down.

4.4.2.6 Method of Destroying Private Key

All sensitive keys in the memory of the CA system are overwritten with zeros when they are no longer in used. Permanent destruction of private keys is achieved with secure delete operations.

4.5 Logical Access Controls

Smart cards are required by all entities logging onto DIGICERT CA software. The smart cards contain a valid certificate issued by DIGICERT. The administrator and operator must authenticate themselves to the CA system by entering the correct PIN of the smart cards.

Extra steps are taken to protect the PIN. The smart card will be invalidated if the PIN is incorrectly for 3 times consecutively.

Remote access to the main CA system via the client interface is secured using the security features of the SSL protocol, and other remote access services are disabled.

4.6 Information Security Controls

4.6.1 Computer Security Requirements

The CA workstation is physically secured as described in **CPS Part 4.1**. Access to the certificate database and audit trails is restricted as described in **CPS Part 3.7.3** and **3.7.5**.

All computers installed with the CA software are configured to perform CA operations only. All irrelevant services of the operating system are disabled. The operating system enforces identification and authentication of all users.

4.6.2 Computer Security Rating

All computers that host the CA software comply with C2 level security requirements.

4.7 Cryptographic Module Engineering Controls

DIGICERT CA hardware cryptographic module is designed to comply with international standards. (FIPS 1 – 140 Level 2)

5.0 General Provisions

5.1 Obligations

5.1.1 CA Obligations

This section describes various terms, conditions, obligations, liabilities, representations, guarantees, warranties and other provisions of all relevant parties whether covered by this CPS or otherwise. Some of the provisions included in this section can be found in the preceding sections but have been reproduced here as a convenient consolidation and a reference point for readers of this CPS.

In relation to this CPS, DIGICERT warrants and promises to:

- engage the services of a RA or enterprise CA to perform validation, and registration of subscribers to the certification services;
- generate public and private key pairs in relation to a particular subscriber;
- provide a publicly accessible repository to store certificates of subscribers;
- publish accepted certificates of subscribers and make certain representations and assurances to parties seeking to rely on the information contained within the certificate;
- revoke or suspend certificates where appropriate;
- publish a certification revocation list on a regular basis;
- provide for the renewal or expiration of certificates where appropriate;
- comply with any other provisions and requirements set forth in CPS Part 3;
- ensures that CA signing private keys are not compromised unless notice otherwise is provided; and
- provide CA services in accordance with the policies and processes described in this CPS and in compliance with the requirements of the DSA and the DSR on business days.

DIGICERT makes no further warranties or promises and have no further obligations under this CPS.

Successor CAs will be subrogated all the rights and obligations of the terminating CA (DIGICERT) except where expressly agreed to prior to the subrogation.

DIGICERT hereby disclaims all further warranties and obligations including merchantability, fitness for a particular purpose, and the accuracy of information provided; and liabilities for negligence and lack of reasonable care, except as expressly provided for in this CPS.

5.1.2 Subscriber Obligations

It is the responsibility of the subscriber to ensure that all the information that has been provided to a RA for the purpose of obtaining a certificate is accurate and kept up-to-date as soon as practicable.

Subscribers are to maintain the integrity of the private key of the corresponding public key pair that is kept in DIGICERT's repository. DIGICERT will not be held liable, be in breach of this CPS, negligent, or be subject to any form of liability as a result of a breach in the integrity of the private key. Subscribers must inform DIGICERT or its RAs within 48 hours of a change to any information included in their certificate or certificate application request. Subscribers must also inform DIGICERT or its RAs within 8 hours of a suspected compromise of one/both of their private keys.

Subscribers are not to submit to DIGICERT or its RAs any material that is offensive, racially discriminatory or prejudiced in any other manner, obscene, pornographic, illegal, hateful within the context of Malaysian laws or the subscriber's local applicable law (where there is discrepancy between the laws, Malaysian law will take precedence), or stolen. The list provided is not meant to be exhaustive. In a more general term, the material submitted must not be of such a manner that it will

- violate any law whether Malaysian or otherwise; and/or
- causes the DIGICERT or its RAs be liable for breach of a law whether Malaysian or otherwise.

5.1.3 Relying Party Obligations

The relying parties are obliged to:

- restrict reliance on the certificates issued by DIGICERT to the appropriate usage for those certificates in accordance with this CPS and with the certificate policy under which the certificate was issued;
- verify certificates before verifying a digital signature, including the use of CRLs and , in accordance with the certification path validation procedure specified in ITU-T Rec. X.509:19971 ISO/IEC 9594-8 (1997), taking into account any critical extensions; and
- trust and make use of certificates only if a valid certificate chain is established between the relying party and the certificate owner.

5.2 Liability

5.2.1 CA Liability

Additional terms, conditions or other representations whether oral or in written form by DIGICERT or its employees, agents or persons claiming to be its employees or agents will not increase the scope DIGICERT’s liability contained within this CPS except where DIGICERT expressly provides for it.

DIGICERT shall only be liable for the issued certificates to an amount not exceeding the following:

Class of certificate	<u>Reliance limit/ Liability Cap</u>
Class 1	RM500.00
Class 2	RM2,000.00 (Basic)
Class 2	RM25,000.00 (Enhanced)
	RM50,000.00 (Server)
	Up to RM25,000 (Enterprise CA)

The reliance limit on each certificate shall be the same regardless of the number of digital signatures, transactions, or claims related to such certificate. In the event the liability cap is exceeded, the available liability cap shall apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall Digicert Sdn Bhd be obligated to pay more than the aggregate liability cap for each certificate, regardless of the method of apportionment among claimants to the amount of liability cap.

DIGICERT will not be liable to any party whatsoever for any damages suffered whether directly or indirectly as a result of terminating its services.

Subscribers are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been verified by DIGICERT. Verification does not provide a one hundred percent guarantee of accuracy. This is due to the reason that facts may change over time or could have been fraudulently created and only through a detailed investigation (which shall be beyond the scope of the CA/ RA due to time and cost constraints) shall the deception be detected.

DIGICERT shall not be liable to any person for any liability, damages or claims whatsoever in respect of any loss whether consequential, direct or indirect, resulting from this person's direct, indirect or implied reliance on the identity of the person, who signed an electronic message and purports to be the subscriber, that has been verified by the CA/ RA as dictated by the requirements of this CPS.

Subscribers, relying parties, RAs and cross-certified CAs are not eligible for compensation claims for losses resulting from inappropriate or fraudulent use of this PKI.

5.3 Financial Responsibility

5.3.1 Fiduciary Relationships

DIGICERT shall not act as an agent, fiduciary, trustee or other representative of the subscriber at any time. Subscribers must in no way attempt to enforce a fiduciary relationship between DIGICERT and the subscriber. This includes the formation and consequential enforcement of any contract under the guise of a principal-agent relationship with the intention of binding DIGICERT.

5.4 Interpretation and Enforcement

5.4.1 Governing Law

This CPS complies with the Malaysian Law, namely, the Digital Signature Act 1997 (Act 562) and Digital Signature Regulations 1998.

5.4.2 Severability, Survival, Merger, Notice

Severance or merger may result in changes to the scope, management and/or operations of DIGICERT. In such an event, this CPS shall require modifications as well. Changes to the operations will occur consistent with the administrative requirements stipulated in **CPS Part 1.5**. In either event, the DNs of all DIGICERT's subscribers within the current scope of DIGICERT's PKI will likely change, resulting in the need to update keys for those subscribers.

5.4.3 Dispute Resolution Procedures

Within the DIGICERT domain, disputes between subscribers, one of which acts in the role of a subscriber and the other which acts in the role of a relying party, or between subscribers and DIGICERT, will initially be reported to DIGICERT for dispute resolution.

5.5 Fees

5.5.1 Certificate Issuance or Renewal Fees

Certificate fees shall be officially published on DIGICERT's website and/or other printed materials deemed necessary and copyrighted by DIGICERT. Further information on DIGICERT certificate fees can be obtained from the Sales Department of DIGICERT.

5.6 Publication and Repository

5.6.1 Publication of CA Information

DIGICERT shall publish all information regarding its services and business practices in its publicly accessible repository at <http://www.digicert.com.my>. DIGICERT is obliged to publish this information to inform or educate its subscribers on the subject related to PKI and digital signatures. Notice of revocation shall be published in the form of CRL and ARL.

5.6.2 Frequency of Publication

DIGICERT may consider sending bulletin or newsletter in the form of an email to inform subscribers of its new services or updates and changes in its services or practices as and when necessary. Frequency of publication of CRL is specified in **CPS Part 3.4.3**.

5.6.3 Repositories

DIGICERT shall operate as a recognised repository that fully complies with the requirements of the DSA and the DSR. The repository contains certificates of subscribers and DIGICERT CA root certificates.

5.7 Compliance Audit

5.7.1 Frequency of Entity Compliance Audit

A comprehensive compliance audit on DIGICERT CA operations is performed annually as required by Section 20 of the DSA.

5.7.2 Identity/Qualifications of Auditor

Annual performance audit will be performed by qualified auditors registered with the Office of the Controller. Please refer to <http://www.skmm.gov.my>

5.7.3 Audit Coverage

The annual compliance audit investigates the operations of DIGICERT CA and its RA functions to ensure their compliance with the DSA and the DSR.

5.7.5 Actions Taken as a Result of Deficiency

Based on the information gathered in the audit, the qualified auditor shall categorise DIGICERT's compliance as one of the following:

- a) full compliance, if DIGICERT appears to comply with all the requirements of the DSA and the DSR;

- b) substantial compliance, if DIGICERT appears generally to comply with the requirements of the DSA and the DSR but one or more instances of non-compliance or of inability to demonstrate compliance is found in the audited sample, that is likely to be inconsequential;
- c) partial compliance, if DIGICERT appears to comply with some of the requirements of the DSA and the DSR but was found not to have complied with or not to be able to demonstrate compliance with one or more important safeguards; or
- d) non-compliance, if DIGICERT :
 - complies with a few or none of the requirements of the DSA or the DSR;
 - fails to keep adequate records to demonstrate compliance with more than a few requirements; or
 - refuses to submit to an audit.

There are three possible actions to be taken as a result of identification of a deficiency:

- continue to operate as usual;
- continue to operate but at a lower assurance level; and
- cease operation.

5.7.6 Communication of Results

The qualified auditor shall, within fourteen (14) days from the completion of a compliance audit under Regulation 42, submit a written report to the Controller.

All information, which is not considered by DIGICERT to be public domain information, is to be kept confidential. Some specifics are addressed in **CPS Part 5.8**.

5.8 Confidentiality

5.8.1 Types of Information to be Kept Confidential

The private signing key belonging to DIGICERT's subscriber is confidential to that subscriber. DIGICERT will provide any access to those keys. Information held in audit trails is considered confidential to DIGICERT and shall not be released outside of DIGICERT, unless required by law (see **CPS Part 5.8.4**). Personal and corporate information held by the DIGICERT, other than that which is explicitly published as part of a certificate, CRL, ARL,

certificate policy or this CPS is considered confidential and shall not be released unless required by law (see **CPS Part 5.8.4**). Generally, the results of annual audits are kept confidential, with exceptions as outlined in **CPS Part 5.7**.

5.8.2 Types of Information Not Considered Confidential

Information included in certificates, CRLs and issued by DIGICERT and DIGICERT's certificate policies are not considered confidential.

Information in this CPS itself is not considered confidential. However DIGICERT policy requires that it only be made available to subscribers of its certification services, including those in cross certified CA domains.

Confidentiality of information in the DIGICERT repository is dependent on the particular data items and applications. Confidentiality of relevant information in the repository is achieved through the use of access controls.

5.8.3 Disclosure of Certificate Revocation/Suspension Information

When DIGICERT revoke/suspend a certificate, its RAs or the Controller, the list of revocation can be found in the CRL. A revocation reason is included in the CRL entry for the revoked/suspended certificate. This revocation reason code is not considered confidential and can be shared with all other users and relying parties. However, no other details concerning the revocation/suspension are disclosed.

5.8.4 Release to Law Enforcement Officials

DIGICERT is obliged under the DSA to disclose or release production of records and identification document, accounts, computerised data and other relevant documents to the enforcement officials.

5.9 Intellectual Property Rights

Subscribers, users of this CPS, and parties covered in **CPS Part 3** are not to reverse engineer, decompile or attempt to reverse engineer or decompile the technologies including encryption algorithms employed by DIGICERT in providing the CA services to subscribers.

Unless otherwise stated, the following property-ownership relationships are assumed to be in force:

- public key - public keys are the personal property of the holders of the corresponding private key. Public keys may be distributed freely due to the nature of its usage;
- private key - private keys are the personal property of the subscribers. Subscribers are individually responsible for the security of the private key;
- certificates - certificates are the private property of DIGICERT. Certificates shall only be reproduced in a publicly accessible repository with the prior permission of DIGICERT. Should the certificate be reproduced in a non-publicly accessible repository, no part of the certificate must be omitted; and
- CPS - this CPS remains as the sole private property of DIGICERT. Reproduction of this CPS requires the prior permission of DIGICERT. Proper citation should be included in **CPS Part 1.2**.

5.10 Limitations on Usage of Services

DIGICERT's services are not intended to be used in situations which require fail-safe guarantees where failure could lead to severe cases of undesirable outcomes including, but not limited to, physical injury, insanity, death, severe environmental damage, or war.

5.11 Conflict of Provisions

In the event that sections of this CPS is in conflict with other provisions, rules, requirements or regulations, the requirements of this CPS will take precedence except where the conflicting provision:

- (i) pre-dates this CPS;
- (ii) expressly states that it supersedes this CPS;
- (iii) is allowed for by this CPS;
- (iv) is a requirement of law; or
- (v) is a requirement put in place by the Controller or the Minister (within the meaning of the DSA).

Except for item (iv) and (v) above or any combination of the above including item (iv) and (v), the final decision on compliance will be at the sole discretion of DIGICERT.

5.12 Interpretation and Validity of this CPS

The DSA and the DSR will govern the enforceability, construction, interpretation and validity of this CPS. Interpretation of this CPS is also governed by what is considered to be business norms and be based upon its intended meaning, scope of application and observance of good faith.

5.13 Force Majeure

DIGICERT is not responsible for any breach of warranty, delay, failure to perform, negligence, or any of the liabilities that will necessarily be incurred as a result of a breach of this CPS or applicable laws, including Malaysian law, due to acts of God, war or national emergency, epidemic, fire, flood, earthquake, strikes, riots, and other natural disasters as well as circumstances and occurrences that are beyond the control of DIGICERT.

5.14 Exceptions

With regards to certification issued to Jabatan Imigresen Malaysia (JIM) under the Root CA of Malaysia Country Signer and prescribed to ICAO 9303 document (Part 1 Vol 2), some exceptions are given as below:

5.14.1 Key length is at 3072 bits.

5.14.2 The Malaysia Country Signer key pairs are generated as and when necessary through proper documented procedures on Hardware Security Module (HSM).

5.14.3 The requirement for the Document Signer Certificates issuance is bound by the agreed procedure between DIGICERT and Jabatan Imigresen Malaysia (*please see Appendices 6.3*).

5.14.4 Algorithm used for subscriber (Document Signer Certificate) is SHA256 with the corresponding identifier.

6.0 Appendices

6.1 Glossary of Terms

This document makes use of the following defined terms:

Term	Definition
Authentication	A process used to confirm the identity of a person or to prove the integrity of specific information.
Asymmetric cryptosystem	An algorithm or series of algorithms that provide a secure key pair.
Certificate	<p>a computer-based record which-</p> <ul style="list-style-type: none"> • identifies the certification authority issuing it; • names or identifies its subscriber; • contains the subscriber's public key; and <ul style="list-style-type: none"> • is digitally signed by the certification authority issuing it.
Certificate policy	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.
Certification Authority (CA)	A person who issues a certificate.
Certification Authority disclosure record	An on-line and publicly accessible record which concerns a licensed certification authority which is kept by the Controller.
Certification path	An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.
Certification Practice Statement	A declaration of the practices which a certification authority employs in issuing certificates generally, or employed in issuing a particular certificate.

Certification Revocation List (CRL)	A list of suspended or revoked certificates.
Controller	The Controller of Certification Authorities appointed under Section 3 of the DSA.
Date/time stamp service	A date/time stamp service recognised by the Controller under the DSA.
Digital signature	<ul style="list-style-type: none"> • a transformation of a message using an asymmetric cryptosystem so 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 message has been altered since the transformation was made.
Electronic Data Interchange (EDI)	Technology involving computer-to-computer exchange of structured data between two or more companies sent in a form that allows automatic processing, with no manual intervention. It is relevant to any business that regularly exchanges information, for example, client or company records, but is especially relevant if you send and receive orders, invoices, statements and payments.
Entrust.net Certification Authority (2048)	Cross-certifying root between Entrust and Digicert Sdn. Bhd.
GTE Cyber Trust Class 2 Global Root	Cross-certifying root between Cyber Trust and Digicert Sdn. Bhd.
ICAO	International Civil Aviation Organization.
Issue a certificate	The act of a certification authority in creating a certificate and notifying the subscriber listed in the certificate of the contents of the certificate.
Key pair	A private key and its corresponding public key in an asymmetric cryptosystem, where the public key can verify a digital signature that the private key creates.
Licensed certification authority	A certification authority to whom a licence has been issued by the Controller and whose licence is in effect.
Message	A digital representation of information.

Malaysia Premier CA	Self issuing CA for the subscribers who participate in the e-Government projects
Notify	To communicate a fact to another person in a manner reasonably likely under the circumstances to impart knowledge of the information to the other person.
Object Identifier (OID)	A value comprised of a sequence of integer components, which can be assigned to a registered object and which has the property of being unique among all object identifiers.
Person	A natural person or a body of persons, corporate or unincorporated, capable of signing a document, either legally or as a matter of fact.
Policy qualifier	Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.
Private key	The key of a key pair used to create a digital signature.
Public key	The key of a key pair used to verify a digital signature.
Publish	To record or file in a repository.
Provisions	A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS employing the approach described in this framework.
Recipient	A person who receives or has a digital signature and is in a position to rely on it (see Relying Party).
Recognised repository	A repository recognised by the Controller under Section 68 of the DSA.
Reliance limit	The monetary amount recommended for reliance on a certificate under Section 60 of the DSA.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (e.g., a RA is delegated certain tasks on behalf of a CA).
Relying party	A recipient of a certificate who acts in reliance on that certificate and/or digital signature verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.
Repository	A system for storing and retrieving certificates and other information relevant to digital signatures.

Revoke certificate	To make a certificate ineffective permanently from a specified time forward.
RSA	<p>The first significant asymmetric cryptographic algorithm; the initials stand for Rivest, Shamir and Adleman, its inventors.</p> <p>Note that RSA can also refer to a particular commercial entity; see RSA DSI. RSA is protected by US patents held by RSA DSI. It is not protected outside the US.</p>
Subscriber	<p>a person who-</p> <ul style="list-style-type: none"> • is the subject listed in a certificate; • accepts the certificate; and • holds a private key which corresponds to a public key listed in that certificate
Suspend a certificate	To make a certificate ineffective temporarily for a specified time forward.
Trustworthy system	<p>computer hardware and software which-</p> <ul style="list-style-type: none"> • are reasonably secure from intrusion and misuse; • provide a reasonable level of availability, reliability and correct operation; and • are reasonably suited to performing their intended functions.
Uniform Resource Locator (URL)	a standardised addressing scheme which identifies a particular Internet resource, such as a Web page, a gopher server, a library catalogue, an image, or a text file.
Valid certificate	<p>a certificate which-</p> <ul style="list-style-type: none"> • a licensed certification authority has issued; • has been accepted by the subscriber listed in it; • has not been revoked or suspended; and

	<ul style="list-style-type: none"> • has not expired: <p>Provided that a transactional certificate is a valid certificate only in relation to the digital signature incorporated in it by reference.</p>
Verify a digital signature	<p>in relation to a given digital signature, message and public key, to determine accurately that-</p> <ul style="list-style-type: none"> • the digital signature was created by the private key corresponding to the public key; and • the message has not been altered since its digital signature was created.
Writing / written	<p>Includes any handwriting, typewriting, printing, electronic storage or transmission, or any other method of recording information or fixing information in a form capable of being preserved.</p>

6.2 List of Certificates for Enterprise CA

1. Digisign iVest CA
2. Digisign iVest CA Enhanced
3. MyKad Online
4. CIMB Investment Bank Bhd Enterprise CA
5. Bumiputra Commerce Bank Bhd Enterprise CA
6. Bank Negara Malaysia Sub CA
7. Alliance Bank Sub CA

6.3 Document Signer Certificates Issuance - Process Flow

