CERTIFICATION PRACTICE STATEMENT (CPS)

Published by
Radiant InfoTech Nepal Pvt. Ltd.
GPO Box: 1212, Mahamati Complex,
Gairidhara, Kathmandu, Nepal
Phone: +977 1 4445765, 4424311, 4441770
Email: info@radiantnepal.com | Website: www.radiantnepal.com

Approved by
Office of Controller of Certification
Ministry of Information, Communication & Technology
Government of Nepal

Type	Date of Publication	Version No	Document No
PUBLIC	25-11-2015	0.1	RADIANTCA/DOC/CPS/0.1

© Copyright 2015, Radiant InfoTech Nepal Pvt. Ltd. All rights reserved.

This document namely the Certification Practice Statement has been drafted based on the RFC-2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework and the guidelines for submission of application for license to operate as a Certifying Authority under the Electronic Transaction Act, 2006, Annexure –1.

Wherever the phrase “Radiant InfoTech Nepal Pvt. Limited” or the abbreviation “RIN” appears in this document, including within the abbreviation “RADIANTCA”, it shall be taken to mean “Radiant InfoTech Nepal Pvt. Ltd”.

Notice

Save as otherwise provided as per the laws of Nepal, the services provided by RIN shall, at any time, be in accordance with the applicable laws in Nepal and shall be subject to the jurisdiction of various courts, tribunals and authorities in Nepal, including but not limited to the Electronic Transaction Act, 2006, its rules and regulations and any amendment thereto.

Any person who uses the digital signature certificate in an improper manner or violate the provisions detailed under this RadiantCA Certification Practice Statement shall render himself/herself liable for civil/criminal action and be proceeded against as per the provisions of applicable civil/criminal laws and Electronic Transaction Act or any other act/acts that are relevant and in force from time to time. Attention is also drawn to the Electronic Transaction Act Chapter VI wherein the duties of subscribers are specified.

Definitions

The following definitions are to be used while reading the RADIANTCA CPS. The following terms shall bear the meanings assigned to them hereunder and such definitions shall be applicable to both the singular and plural forms of such terms:

- "**Radiant CA**" is a brand name, refers to the Certifying Authority, owned by Radiant InforTech Nepal (P) Limited, which is licensed by Office of Controller of Certification (OCC), Govt. of Nepal under Electronic Transaction Act 2006, and includes the associated infrastructure as mentioned in this CPS for providing Certification & Trust services.
- "**Radiant InfoTech Nepal (P) Ltd.**" refers to a company incorporated under the Nepalese Companies Act, 2006.
- Unless otherwise specified the word '**Act**' in this CPS refers to Electronic Transaction Act 2006 and amendments there to
- "**Access**" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network
- "**Affixing Digital Signature**" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Digital Signature
- "**Applicant**" or "**User**" means a person, entity or organization that has requested for a digital signature certificate to be issued by RADIANTCA.
- "**Auditor**" means any Audit organizations appointed by RADIANTCA and empanelled by Office of Controller of Certification (OCC) for auditing of Licensed CA.
- "**CA**" refers to RADIANTCA, as licensed by OCC to issue digital signature certificate.
- "**Compromise**" means a violation (or suspected violation) of a security policy, in which an unauthorized disclosure of or loss of control over sensitive information may have occurred
- "**Computer**" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network
- "**Controller**" means the Office of Controller of Certification appointed as per Section 13 subsection (1) of the Act.
- Unless otherwise specified, the word "**CPS**" used throughout this document refers to Certification Practice Statement of RADIANTCA

- "**Digital signature**" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of the Electronic Transaction Act;
- "**Digital signature certificate**" or the "**certificate**" means a digital signature certificate issued by RADIANTCA to the Applicant. It also means a Digital Signature Certificate issued under sub-section (4) of Section 35 of Electronic Transaction Act.
- "**End Entity**" or "Entity" refers to either applicant or subscriber of Digital Certificate issued by RADIANTCA.
- "**Private Key**" means that part of cryptographic key pair generated for creating Digital Signature and is held privately by the subscriber.
- "**Registration Authority**" or "**RA**" means an entity or organization trusted under RADIANTCA hierarchy and has right to verify the credentials of the applicant/subscriber before forwarding to RADIANTCA for issuance and revocation of certificate etc.
- "**Subscriber**" means a person, entity or organization in whose name the Digital Signature Certificate is issued by RADIANTCA.

Note: The contextual meaning of the terms may be considered for such terms that are used in this CPS but not defined above.

Executive Summary of RADIANTCA CPS

1. RADIANTCA Certification and Trust Services Radiant InfoTech Nepal (P) Ltd.'s (Radiant) core business goals are:

- To change the rule of the game of consumer servicing by providing either totally unique services or existing services with material difference to the consumer;
- To enable consumers to manage their financial and statutory obligations and need through technology enabled process and by changing the way they have been transacting;
- To enable and empower consumer by aiding with secured technology that will help them achieving their financial goals.

As the Nepalese consumer base is exponentially growing, to manage the volume, RADIANTCA has built appropriate technology engines which will provide for a non-linear model to deliver the services needs of consumers. Radiant provides digital signature certificates to consumers so that they can transact over the internet in a secured way.

This Certification Practice Statement (CPS) describes the practices followed with regard to the management of the lifecycle of the certificates issued by RADIANTCA

2. Rights and Obligations

Except for notice by the applicant to the contrary, an applicant, applying for a Certificate through RADIANTCA, understand and agree that, at all times during the acceptance and the validity of the certificate, he shall be bound by this CPS and for any person who relies on the information provided in the Certificate, for the following:

- The information submitted by the certificate applicant to Radiant and included in the certificate is considered to be true and accurate as submitted by the applicant.
- No other person has ever had access to subscriber's private key.

The subscriber undertakes that, by accepting the certificate issued by the RADIANTCA, shall use it in a trustworthy system and he shall be solely responsible for his possession and use of private key and shall take such measures necessary to prevent any unauthorized use, access, tampering or loss of the private key. The user shall request for revocation at all times where there has been evidence of theft, tampering, loss and compromise of the user's private key.

3. Liability

Without limiting subscriber's obligations stated in this CPS, subscribers are liable for any misrepresentation they make in the digital signature certificates and on which third parties reasonably rely believing the same to be true.

For more information visit www.RadiantCa.com.np or contact info@RadiantCa.com.np

List of Acronyms & Abbreviations

Acronym	Term
ARL	Authority Revocation List
ASN.1	Abstract Syntax Notation.1
CA	Certifying Authority
OCC	Office of Controller of Certification
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol With SSL
IETF	Internet Engineering Task Force
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Directory Interchange Format
NRDC	National Repository Of Digital Signature Certificates
OID	Object Identifier
PAC	Policy Approval Committee
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
PUK	PIN Unlock Key
RA	Registration Authority
RCAN	Root Certifying Authority Of Nepalese
RFC	Request For Comment
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
SUB-CA	Subordinate Certifying Authority
URI	Uniform Resource Indicator
URL	Uniform Resource Locator

Table of Contents

1. Introduction

This Certification Practice Statement details the practices that RADIANTCA adopts to provide Digital Signature Certificates and related services. The CPS is the principal practice statement governing the services provided by RADIANTCA and establishes conformance to the requirements of the Electronic Transaction Act, 2006 (ET Act). All transactions facilitated by electronic means viz., electronic data interchange and electronic means of communication, falling under the umbrella of "Electronic commerce", are granted legal recognition under the Electronic Transaction Act.

1.1. Services Offered

RADIANTCA operates a PKI hierarchy to offer a range of 'Trust' services. The following services are being offered by RADIANTCA:

1.1.1. Retail Trust Services

RADIANTCA issues various classes of Certificates. These would be issued to Individuals or individual representing organizations or specific devices (web servers) based on the validation requirements specified by RADIANTCA. The certificates issued under this service can be used for file signing, digital signatures, encryption, web server authentication, code signing, web form signing, online transaction and e-commerce. The process of encryption certificate issuance is mentioned in Section 1.8.2.2 of this CPS.

1.1.2. Managed PKI Services

As business on the net has grown and communication in the electronic form plays a critical role in day-to-day business of any organization, it is necessary for organizations to setup a secure communication environment using PKI-based technologies. RADIANTCA shall provide a Managed PKI solution which would enable organizations to manage certificate issuance to their employees / partners / affiliates / customers with minimal investment.

RADIANTCA Managed PKI solution would provide enterprises with a cost-efficient solution to a PKI system that can be adapted to the enterprises requirements without having to operate a Certification Authority set-up. The enterprises can outsource to RADIANTCA the issuance of digital signature certificates and other administrative tasks such as digital signature certificate generation, validation, renewal and revocation of certificates issued to their customers, employees and partners.

1.1.3. OCSP (Online Certificate Status Protocol) Validation Services

RADIANTCA offers OCSP validation services to relying parties for certificate status verification in real time.

1.2. Certifying Authority

The term "Certifying Authority" or CA as used in this CPS, represents RADIANTCA as the entity, licensed by the Office of Controller of Certification (OCC), Govt. of Nepal

RADIANTCA may issue several "classes" of certificates depending on the level of 'trust' requirements. It is to be noted that:

- RADIANTCA certificate will be signed by OCC. RADIANTCA in turn will create and sign the public keys of various class level sub-CAs representing each class of digital signature certificate. RADIANTCA may also create and sign end user subscriber certificates for specific classes of certificate.
- The responsibilities related to the certificate issued under any class of RADIANTCA hierarchy rests with RADIANTCA.

In carrying out this responsibility RADIANTCA may enter in to contractual agreements with external parties like RAs, Managed PKI customers, partners etc.

1.3. Registration Authority

Registration Authorities (RAs) are entities appointed by RADIANTCA to evaluate and either approve or reject digital signature certificate applications in accordance with this CPS. The Registration Authorities may in turn have personnel to process and evaluate the application requests, but the requests shall be forwarded to the RADIANTCA only through the designated RA.

1.4. Components of RADIANTCA Public Hierarchy

RADIANTCA public hierarchy consists of RADIANTCA (the CA certificate signed by OCC). RADIANTCA in turn signs the following sub-CAs representing various classes of certificates. The list of Sub-CAs are provided in www.RadiantCa.com.np/repository

The subscriber can choose any one of the classes based on his requirements. For Managed PKI services or for any future purposes, if need be, RADIANTCA would offer an arrangement whereby some more specific Sub-CAs are created for representing various class of certificates.

Notes:

1. RADIANTCA may choose to have only a subset of the hierarchy and services mentioned based on commercial and operational considerations. The service and offerings mentioned above could be changed in the subsequent versions of the CPS.
2. RADIANTCA reserves the sole right to accept applications for its certificates and issue digital signature certificates. The validation and verification procedures for each class of certificates will be as mentioned in this CPS and in accordance with the Electronic Transaction Act.

1.5. Role of CPS and Other Documents

This CPS explains specific practices of RADIANTCA with respect to issuance and management of the certificates. It covers the following areas:

- Appropriate application for various classes of certificates.
- Assurance level associated with each class.
- Obligation of RADIANTCA, Registration Authority (RA), Subscriber and Relying parties.
- Legal matters that are covered in subscriber agreements and relying party agreements.
- Audit and related security and practices reviews undertaken by company.
- Methods used for identification and verification of subscriber for various certificates.
- Operational procedures for certificate applications, issuance, acceptance, revocation, and renewal.
- Physical, personnel, cryptographic private key and logical security.
- Operational security procedures for audit logging, records retention and disaster recovery.
- Certificate and certificate revocation list (CRL) content
- Administration of CPS, including methods of updating it.

Security and operational policy and procedure documents and manuals are some of the other documents that in addition to the CPS define the practices and processes of RADIANTCA operations.

- Technical Specifications of CA System: The principles which define RADIANTCA PKI security requirements and standards followed.
- IT Security Policy: Defines the guidelines covering the security implementation across various areas such as Physical, Key Operations, People etc. and also the audit requirements.
- Operating Procedure Manuals: Sets the operations guidelines governing the PKI operations.
- Key Ceremony Guide: Key Management Operations guidelines policy and manuals gives the detail procedure for carrying out various activities.
- Agreement documents including the Subscriber and the RA agreements are the legal agreements that bind the various participants such as users, RAs to RADIANTCA standards.

RADIANTCA may rely on the ancillary documents as may be required in addition to the CPS for referring to any specific detailed standards.

1.6. Relationship with Office of Controller of Certification

The Root Certifying Authority of Nepal (RCAN) of OCC digitally signs the public keys of licensed CAs are in Nepal. The OCC operates the Root Certifying Authority of Nepal (RCAN) under section 18(b) of the Electronic Transaction Act. RADIANTCA PKI, is by design, subordinate to the RCAN. As part of the CA licensing process defined in the Act, the OCC has issued a CA certificate to RADIANTCA. This CA Certificate signed by the RCAN, authenticates the Public Key of RADIANTCA and can be downloaded from the OCC's website [http://www.cca.gov.np/] as well as RADIANTCA's website (www.RadiantCa.com.np/repository).

1.7. Compliance with Electronic Transaction Act

RADIANTCA complies with Electronic Transaction Act , Rules and Regulations. RADIANTCA practices described in the CPS are designed to comply with the prevalent and applicable provisions under the Act. As required by Electronic Transaction Rules 2008, this CPS conforms the adherence to framework provided in ITU RFC 1422 (X.509 version 3 certificates) in order to make interoperation easier for person who is intending to use RADIANTCA services.

1.8. Policy Overview

In accordance to the guidelines of Electronic Transaction Act and the X.509 Certificate Policy for Nepal PKI published by Office of Controller of Certification, RADIANTCA issues 3 classes of Certificates, namely: Class 1, Class 2 and Class 3. Each class of digital signature certificate is associated with specific security features and corresponds to a specific level of trust.

1.8.1. Assurance Levels and Applicability

Class	Assurance Level	Applicability
Class 1	Class 1 certificates shall be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer database.	This provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance.
Class 2	These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial
Class 3	This certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities.	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

1.8.2. Types of Certificates

RADIANTCA can issue six types of certificates: Signature, Encryption, Device/System, SSL Server,

Code Signing and Document Signer Certificate

1.8.2.1. Signature Certificate

The signature certificate is corresponding to the signing private key. It will be used by individuals or organizations for signing purpose. The key pair will be generated by applicant/subscriber in a secure medium and is inherent to keep his private key in safe custody. The signature certificate is issued by RADIANTCA after the validation process mentioned in this CPS. The relying parties can make use of this certificate for signature verification.

1.8.2.2. Encryption Certificate

The encryption key pair is used by the subscriber for receiving encrypted messages which is encrypted using subscriber's public key. The subscriber fills in the application and submits to RADIANTCA or it's authorized RAs along with the identification and address proof. The RA verifies the application, id proof and address proof and approves the request. The Subscriber provides a password in the portal for protecting the encryption certificate. The server generates the encryption key, escrows and makes it available for the customer in the portal. The subscriber needs to login with the credentials sent to his digital id and download the encryption certificate from the portal.

1.8.2.3. Device/System Certificate

Device/System Certificates include the digital certificates issued to particular device, like Firewall, Router, Computer, etc. The issuance process will be as referred in Section 3.1.12.

1.8.2.4. SSL Server Certificate

SSL server certificates are digital identifications containing information about web server and the organization that is owned the server's web content. An SSL server certificate enables users to authenticate the server, check the validity of web content, and establish a secure connection. The issuance process will be as referred in Section 3.1.12.

1.8.2.5. Code Signing Certificate

Code signing certificate helps user to develop confidence in downloaded code. It allows users to identify the signer to determine if codes have been modified by someone other than the signer. Signed codes can be Java Applets, Java scripts, plug-in, ActiveX controls of any other kind of code. The issuance process will be as referred in Section 3.1.12.

1.8.2.6. Document Signer Certificate

The Document Signer Certificates are issued to organizational software applications for operating automatically to authenticate documents/information attributed to the organization by using Digital Signature applied on the document, documents/Information. The issuance process will be as referred in Section 3.1.12.

1.9. Identification

This CPS is called RADIANTCA Certification Practice Statement. RADIANTCA manages the life-cycle of digital signature certificates under RADIANTCA, and the contact details are mentioned in section 1.12.1 of this CPS.

1.10. Community and Applicability

The community governed by this CPS is RADIANTCA Public Key Infrastructure (PKI) that accommodates a large, public community of users with diverse needs for communication and information security.

The parties involved in RADIANTCA PKI are:

- RADIANTCA that issue certificates.
- Entities that function as RAs
- Entities that are certified as applicants or subscribers.
- Entities that rely on the certificates (relying party).

1.10.1. Certifying Authority and Hierarchy

The term Certifying Authority refers to all entities signing certificates in accordance with RADIANTCA PKI hierarchy pertaining for each class of certificates, as mentioned under section 1.4 of this CPS.

1.10.2. Registration Authorities

A Registration Authority ("RA") is a local office/Agents or partners appointed by RADIANTCA that receives the applications for the Certificate (as prescribed in the Electronic Transaction Act, 2006) from the applicant/subscriber and verifies the details contained in the application. If the verification is successful, then the application is additionally signed by RA and forwarded to the CA for further verification of Application and Supporting Documents, as may be applicable. If the verification by authorized CA personnel is successful, the request is then digitally signed (by CA) and forwarded to respective Sub-CA under RADIANTCA PKI recommending generation of a Digital certificate for the verified applicant/subscriber.

The Managed PKI Customers (enterprises) would act as Registration Authority for their affiliated entities.

1.10.3. End Entities

The end entities / end users of the Digital signature certificates in business and other communication applications are:

Applicants - An applicant is a person, entity, or organization that has applied for, but has not yet been issued a RADIANTCA Digital signature certificate.

Subscribers - A Subscriber is a person, entity, or organization that has been issued a RADIANTCA Digital Signature Certificate.

Relying parties – A Relying Party is a person, entity, or organization that relies on or uses RADIANTCA Digital signature certificates and/or any other information provided in RADIANTCA repository to verify the identity and public key of a subscriber and/or use such public key to send or receive encrypted communications to or from a subscriber.

1.11. Community and Applicability

The RADIANTCA PKI community includes, CAs, sub-CAs, RAs, Subscribers, and Relying Parties. This CPS is applicable to all the members of the RADIANTCA PKI community and it defines the practice statement for use of such digital signatures in order of hierarchy.

RADIANTCA digital signature certificates are intended to support the security needs as mentioned in this CPS. RADIANTCA shall not be responsible for any liabilities howsoever or whatsoever arising from the use of any Certificate unless RADIANTCA has expressly undertaken to assume such liabilities in this CPS.

1.11.1. Prohibited Applications

RADIANTCA certificates are not for use for any equipment operated in hazardous conditions or under fail proof conditions (eg. Nuclear facilities, aircraft navigation etc) where any failure could directly lead to grievous injury, death or severe environmental damage.

In addition specific categories or types of certificates are to be used only for the designated purposes such as RADIANTCA certificates are to be used only for CA function, end subscriber certificates cannot be used for CA function.

More generally, certificates shall be used only to the extent where use is consistent with all applicable laws, rules and regulations and in particular shall be used only to the extent permitted by applicable export or import laws.

Also, with respect to X.509 Version 3 Certificates, the key usage extension is intended to limit the technical purposes for which a private key corresponding to the public key in a certificate may be used.

1.12. Contact Details

1.12.1. Specification Administration Organization

This CPS is administered by RADIANTCA. The CPS shall be revised from time to time as and when needed by the CA, upon approval from the OCC, with sufficient notification to the end users.

RADIANTCA can be contacted at the following address.

Radiant InfoTech Nepal (P) Ltd.
Gairidhara, Kathmandu, Nepal
Phone: +977-1-4445765, Email: info@RadiantCa.com.np, Website: www.RadiantCa.com.np

1.12.2. Contact Person

RADIANTCAn be contacted at the address specified in section 1.12.1 of this CPS.

For more information, refer to RADIANTCA's website at www.RadiantCa.com.np or contact administrator at info@RadiantCa.com.np.

1.12.3. Person Determining CPS Suitability for the Policy

The CPS suitability is approved and decided by the Policy Approval Committee of RADIANTCA. However, the CPS can be adopted only after the approval by the office of Office of Controller of

Certifcation (OCC).

1.13 Time stamping

All critical servers used in RADIANT CA setup is synchronized with national time source directly or indirectly. Accordingly, RADIANT CA will offer time stamping services. Time stamping server shall be synchronized to NST through NTP.

2. GENERAL PROVISIONS

The responsibilities of various parties, participating in the RADIANTCA PKI as established by this CPS has been defined in this section. The obligations of various parties have been detailed.

2.1. Obligations

2.1.1. CA Obligations

The CPS specifies obligations for RADIANTCA throughout this document.

Broadly the RADIANTCA shall have the following obligations:

- Performing activities as per the policies, procedures and process as designed to secure the certificate management process. (including certificate issuance, suspension, activation, revocation, CRL publication and audit trails)
- To protect its private key from compromise.
- Issuing a Digital Signature Certificate to the applicants who has submitted an application, and verified & validated by the RADIANTCA appointed RA
- Revocation of the Digital Signature Certificate upon the request from the subscriber or RA as per the terms and conditions in RADIANTCA CPS.
- Publishing the CRL regularly as per the terms and conditions in this CPS document.
- To Maintain the OCC approved CPS with previous versions / revisions as and when changes are made.
- Creation & maintenance of Audit Trail of CA operations
- To ensure that all requirements, representations, warranties as mentioned in this CPS are adhered when performing the Certificate issuance, operations and CA services.
- RADIANTCA shall be responsible for all PKI related operations performed by RA.
- To submit certificate/CRL issued by RADIANTCA to the OCC for its National Repository of Digital certificates.

In addition RADIANTCA will make reasonable efforts to bind the subscriber and relying party through the Subscriber Agreements and the Relying Party Terms & Conditions. Subscriber (whether direct or Managed PKI) will not be enrolled or issued a certificate without consent/agreement to the Subscriber Agreement.

2.1.2. RA obligations

RAs assist CA by performing validation functions, approving or rejecting Certificate Applications, requesting revocation of Certificates, and approving renewal requests.

- Implement the practices described in this CPS.
- Verifying the applications and validating the supporting/relevant documents as provided by the applicant and if necessary entering of relevant details online to RADIANTCA.
- Before forwarding the signed approval for issuance of certificate by RADIANTCA, RA shall check for any known infringement by the applicant for Trademark, etc
- Authenticate requests from subscribers for revocation of certificates and send timely revocation requests to RADIANTCA.
- Request of Revocation from other subscriber is to be forwarded to RADIANTCA for timely revocation. RA to ensure the authenticity of such requests.
- Collect the relevant documents for the corresponding class of certificates from applicant, as applicable under the provisions of this CPS.
- Send the subscriber applications with all necessary supporting documents (and attestations) to RADIANTCA, as required and defined in the Electronic Transaction Act 2006 and subsequent amendments.

2.1.3. Subscriber Obligations

The Subscriber shall have the following obligations:

- To ensure that the information / data provided in the application for certificate request is true, accurate, current and without errors, omissions or misrepresentations
- To ensure the use of only those secure medium as specified in the RADIANTCA CPS to generate the key pair (except in case of Encryption Certificate)
- Use the certificate for authorized purposes consistent with this CPS.
- To protect his private key in a trustworthy secure medium.
- Confirm acceptance of the Digital signature Certificate generated by RADIANTCA when all information contained in the certificate, as provided by the applicant, is validated as true.
- Notify RADIANTCA immediately when the information included in the Subscriber's Digital Signature Certificate is inaccurate, false or incomplete.
- Notify RADIANTCA immediately upon any actual or suspected compromise of the Subscriber's private key.
- Comply with any other additional obligations as mentioned in the Subscriber agreement.
- To keep the private key safe and protect it from any disclosure or unintended use.
- Read and accept the policies and procedures as specified in this CPS.

2.1.4. Relying Party Obligations

Relying Party shall have the following obligations.

- Relying Parties must independently assess the appropriateness of the use of a Digital signature certificate for any given purpose.
- Relying Parties must not use certificates beyond the limitations and for applications which have been prohibited section 1.11.1 of this CPS.
- Relying parties must use appropriate utilities or tools to perform digital signature verification or other operations. The utilities/ tools should be able to identify the certificate chain and

verifying the digital signature on all certificates in the chain and only on successful verification should rely on the certificate.

- The relying parties have to determine the appropriateness of the use of a certificate.
- Relying parties are deemed to have read and understood the "Relying Party Terms and Conditions" published in www.RadiantCa.com.np/repository

2.1.5. Repository obligations

RADIANTCA is responsible for the repository functions for all RADIANTCA CAs in its PKI hierarchy. All certificates issued by RADIANTCA shall be published in its repository and updated on a regular basis. The updated CRLs shall be published in the RADIANTCA Repository once in every week on Friday, however if there is any revocation of DSC in between then it will be published immediately in the corresponding CRL. Thus the CRL will contain updates based on revocations done.

2.2. Liability

2.2.1. Certifying Authority Liability

RADIANTCA provides the service on best effort basis. The security and suitability of the service will not be guaranteed by RADIANTCA. RADIANTCA shall not be liable for delay or omission to issue/revoke/activate a digital certificate or any other consequences arising from events beyond the control of RADIANTCA. RADIANTCA shall not be liable for any damages arising from its operations or use of certificates it issues. RADIANTCA shall not be liable, for any certificates obtained from it, by representing false or inaccurate or misleading or untrue information. Other liabilities of RADIANTCA will be as per prevailing laws, rules, regulations and guidelines of the Government of Nepal.

All warranties and any disclaimers thereof, and any limitations of liability among RADIANTCA, its Intermediaries (RAs/partners) and their respective customers shall be in strict adherence to the terms and conditions of the Agreement amongst them.

2.2.1.1. Warranties to Subscribers and Relying Parties

RADIANTCA warrants to subscribers that:

- No information is materially misrepresented or introduced in the certificate by the entities approving the certificate application or issuing the certificate.
- The entities issuing and approving certificates have exercised reasonable care in managing the application and creating the certificate and no errors in the information in the certificates that was introduced by these entities.
- The certificates conform to certificate management requirements such as revocation services, use of a repository and other material requirements as laid in the CPS.

Similarly RADIANTCA's warrants to relying parties that:

- Information in or incorporated by reference in Digital Signature Certificate, except non verified subscriber Information, is accurate as provided by the subscriber
- The requirements of this CPS will be complied with while issuing the certificate by RADIANTCA

2.2.1.2. Disclaimers of Warranties

RADIANTCA expressly disclaims to subscribers and relying parties, within lawfully permissible limits, all warranties including warranty of merchantability or fitness for a particular purpose.

2.2.1.3. Limitations of liability

The verification for certificate issuance by RADIANTCA is based on reasonable effort basis and neither RADIANTCA nor RA can underwrite the activities or conduct of the subscribers.

RADIANTCA shall not be liable for any indirect, exemplary, special, punitive, incidental, and consequential losses, damages, claims, liabilities, charges, costs, expenses or injuries (including without limitation loss of use, data, revenue, profits, business and for any claims of Subscribers or Users or other third parties including Relying parties).

RADIANTCA shall not be liable for any delay, default, failure, breach of its obligations under the Subscribers Agreement, Relying Party Terms & Conditions and Registration Authority Agreement

2.2.1.4. CA Liability Caps

Notwithstanding anything contained, the maximum liability of RADIANTCA to any Subscriber or Relying Party (whether in contract, tort or otherwise) shall not exceed the amount prescribed in the Subscriber Agreement.

2.2.1.5. Force Majeure

To the extent permitted by applicable law, RADIANTCA's subscriber agreements, Registration authority agreement and Relying Party Terms & Conditions include, and other subscriber agreements shall be subject to the conditions of force majeure clause. RADIANTCA, Registration Authority and Relying party shall not be responsible for any delay/default/inadequate performance/ non-performance / failure in its performance under the Subscribers Agreement, Relying Party Terms & Conditions or Registration Authority Agreement if the same is caused by extraordinary weather conditions or other natural catastrophes, war, riots, strikes, lockouts or other industrial disturbances, acts of any governmental agencies.

2.2.2. RA Liability

The obligations and the liabilities of the RA including its warranties towards CA while assisting the CA in issuing certificates to the subscribers are more particularly set out in the Registration Authority Agreement signed between the parties

2.2.3. Subscriber Warranties and Private Key Compromise

2.2.3.1. Subscriber Warranties

Subscriber agreement of RADIANTCA mandates its subscribers to warrant that:

- At the time of digital signature creation the certificate is valid and operational and not expired or revoked.
- The subscriber's private key was not disclosed and haven't been accessed by any third party.
- The Subscriber has only provided information in the certificate application which is true and accurate and the same is contained in the certificate.
- The Private Key shall not be used for any unlawful and unauthorized transactions.

- The Digital certificate obtained by the end user subscriber is not used for digitally signing any Sub CA certificates, Certificates and CRL.

2.2.3.2. Private Key Compromise (PKC)

The Electronic Transaction Act 2006 mandates that the subscriber shall be solely responsible for the protection of their designated private key. The end subscriber is required to take necessary precautions to ensure storage of the private keys in a secure medium and to protect against disclosure.

2.2.4. Relying Party Liability

All relying parties, who rely on the information provided in the Digital Signatures, under any Terms & Conditions, are required to make an informed decision based on the sufficiency of the information before them and RADIANTCA shall not guarantee or be liable for any decision taken by a relying Party.

2.3. Financial Responsibility

2.3.1. Indemnification by Subscribers

RADIANTCA subscriber agreement mandates all its Subscribers to, within lawfully permissible limits; indemnify RADIANTCAs or RAs for:

- Any inaccurate, false or misrepresentation of information in the subscriber's certificate application, as provided by the subscriber.
- Suppression of a material fact on the certificate application, if the omission was made negligently or with intent to deceive any party,
- Failing to protect the private key of the subscriber and failure to use a trustworthy system or failing to take necessary precautions to prevent the compromise, loss, disclosure, modification, or unauthorized use of the subscriber's private key.
- Any infringement of IPR of a third party caused by the subscriber's use of name not limiting to use of Common name, domain name, digital communication address).

2.3.2. Indemnification by relying parties

RADIANTCA's Relying Party Terms & Conditions mandates all relying parties, to indemnify, within lawfully permissible limits, RADIANTCAs or RAs for:

- Unreasonable reliance, by the relying party, on a certificate under the given circumstances
- For failing to perform the legal obligations of relying party as detailed in this CPS.
- Failure by the relying party to check the status of the certificate (revoked or expired).

2.3.3. Fiduciary Relationships

All RADIANTCA Subscriber Agreements and Relying Party Terms & Conditions disclaim, within lawful limits, any fiduciary relationship deemed between the RADIANTCA's or RA's on one side and the Subscriber or relying Party on the other.

2.3.4. Administrative Processes

RADIANTCA agrees that, during the subsistence of this Agreement, it shall have financial resources and infrastructure sufficient to perform the operations and duties thereof. The Managed PKI

Customers must put in place an insurance program, either with an insurance carrier or a self-insured retention, which shall cover a commercially reasonable level for errors and omissions. The above requirement is not applicable for government entities.

2.4. Interpretation and Enforcement

Notwithstanding anything to the contrary provided in law, this CPS shall be construed in accordance with the Provisions of the Electronic Transaction Act, 2006 and subsequent amendments to it.

2.4.1. Governing Law

This CPS is governed by the Electronic Transaction Act 2006 and all rules, regulations, amendments and any guidelines issued by the appropriate authority to it from time to time.

2.4.2. Severability, Survival, Merger, Notice

It is hereby required under this CPS that all RADIANTCA Agreements required to be entered into for the purposes mentioned herein, must contain clauses for severability, survival, and notice and merger clauses for the following purposes:

- Severability: While interpreting the clauses of an Agreement, if any clause is found to be severable from the rest of the Agreement, the invalidity of such clause shall not affect the validity of the other clauses in the agreement.
- Survival: While interpreting the clauses of an Agreement, certain specific clauses shall be deemed to survive the expiry or termination of the Agreement wherein such clauses are incorporated.
- Merger: while interpreting the clauses of an agreement it is deemed that all clauses that require understanding of the relationship between the parties and the purpose thereof are merged or provided in the Agreement.
- Notice: The Agreement shall state what all circumstances require a notice to be provided by the Parties and the place and to whom such notices shall be forwarded.

2.4.3. Dispute Resolution Procedures

2.4.3.1. Disputes among RADIANTCA and Customers

Any Dispute based on the contents of this CPS, between RADIANTCA and one of its customers who has availed specific services shall be resolved according to provisions in the applicable agreement between the parties.

2.4.3.2. Disputes with End-User Subscribers or Relying Parties

Any Dispute between RADIANTCA and one of its End user subscriber or relying parties, shall be resolved according to the dispute resolution clause in Subscriber agreement or the Relying Party Terms & Conditions.

2.4.4. Role of the OCC

The OCC is competent under the Electronic Transaction Act to resolve any dispute between CAs and Subscribers.

2.5. Fees

The fees for various types of Digital signature certificates will be available on the company's website at www.RadiantCa.com.np/repository and will be updated from time to time.

RADIANTCA is entitled to charge subscribers fees for management and issuance of certificates. The current fees for various types of certificates are listed in the above link.

RADIANTCA is not currently charging any fees to relying parties or other public for accessing the certificate information from the repository. The certificate search facility is provided free of cost at its website (www.RadiantCa.com.np/repository).

RADIANTCA shall update and make available the CRL, free of charge for access by relying parties (www.RadiantCa.com.np/repository).

RADIANTCA shall also provide OCSP validation services, prescribed of charges for access by relying parties to check Online Certificate Status. (ocsp.RadiantCa.com.np)

RADIANTCA will be providing access to policy information documents such as CPS, free of charge (www.RadiantCa.com.np/repository). This is however limited to the specific purpose of viewing. Any reproduction, derivative work creation, modification, etc, would be subject to license agreement with RADIANTCA.

The refund policy and other payments terms would be governed as per the terms in the subscriber agreement. In case the application is rejected the full amount would be refunded to the subscriber.

The above terms and fee structure are subject to change at the sole discretion of RADIANTCA.

2.6. Publication And Repository

RADIANTCA shall maintain an online repository of information relevant to the operations of PKI services under RADIANTCA hierarchy on best effort basis. The information in the RADIANTCA repository is subject to change and published periodically and also on need basis.

RADIANTCA shall reserve rights to not to publish any information that RADIANTCA considers as confidential or not to be disclosed due to the sensitivity of the information.

2.6.1. Publication of CA Information

The information published in RADIANTCA repository (www.RadiantCa.com.np/repository) include:

- RADIANTCA Certification Practice Statement.
- The Digital Signature Certificates issued under RADIANTCA hierarchy.
- The Digital Signature Certificates and public keys of RADIANTCA hierarchy.
- The Certification Revocation List of RADIANTCA hierarchy.
- Fees levied for services provided.
- A provision may available to search for the availability of a given Certificate.
- Application Procedure & Verification Guidelines

2.6.2. Frequency of Publication

RADIANTCA CPS and the CA certificate under RADIANTCA hierarchy shall be published as soon as they are updated and approved by OCC. The CRL shall be published in the repository once in 7 days with validity of not more than 30 days.

2.6.3. Access Control

The information published in RADIANTCA online repository is publicly accessible information and RADIANTCA provides read only access to the contents of the repository. RADIANTCA has put in place sufficient safeguards, logical and physical, to prevent any unauthorized access or alteration/modification of repository entries.

2.6.4. Repositories

The RADIANTCA online repositories are available at www.RadiantCa.com.np/repository.

2.7. Compliance Audit

As per the specifications of the Electronic Transaction Act 2006 and its associated rules, regulations and amendments RADIANTCA would be getting compliance audits done. This would be performed by one of the OCC empanelled set of auditors.

In addition to this Managed PKI customer will also undergo a compliance audit to the extent required by Electronic Transaction Act. Apart from this other entities such as RA would also be asked to undergo compliance audit to the extent required by Electronic Transaction Act by a OCC empanelled auditor selected by RADIANTCA.

2.7.1. Frequency of Audit

Compliance audits will be performed on an annual basis. In addition internal audits would be performed on a half-yearly basis.

2.7.2. Identity of Auditor

A OCC empanelled auditor will perform the audit.

2.7.3. Auditors relationship to audited party

The Audit firm would be independent of RADIANTCA and will not have other business dealings with RADIANTCA.

2.7.4. Topics covered by Audit

The scope of audit will be as per Electronic Transaction Act 2006 and its associated rules and regulations and will include physical controls, environmental controls, key management, personnel, security compliance, CPS and its adherence, regulation prescribed by controller and any other items deemed necessary by RADIANTCA and OCC.

2.7.5. Actions taken as result of deficiency

Significant exceptions and nonconformance as reported by the auditors will be reviewed by RADIANTCA Policy approval committee. If the exceptions are deemed to provide immediate risk to

the security of the system corrective actions will be planned and implemented by RADIANTCA within a reasonable commercially viable time frame. RADIANTCA Policy approval committee will be responsible for remedial planning and implementation of a remedial measure.

2.7.6. Communication of results

Compliance Audit results of RADIANTCA, as per Electronic Transaction Act shall be submitted to OCC. RADIANTCA reserves the right to share the results to other parties as deemed fit.

2.8. Confidentiality and Privacy

2.8.1. Types of Information to be kept Confidential and Private

The following records of Subscribers are kept confidential and private ("Confidential/Private Information"):

- Disclosure of any information pertaining to the digital signature certificate applications, irrespective of the status of such applications, is not permitted. Confidentiality shall also be maintained for any information collected and pertaining to registration and verification of the Digital Signature Certificate irrespective of whether such information is provided in the Digital Signature Certificate or otherwise.
- Transactional records (both full records and the audit trail of transactions).
- Access to the audit reports and any information that is considered sensitive, shall be provided exclusively to the RADIANTCA authorized trusted personnel and the OCC. The purposes for which such information will be used shall be in accordance with the provisions of applicable laws for the time being in force.
- Audit trail records created and or retained by RADIANTCA or a Customer.
- Contingency planning and disaster recovery plans.
- Security measures controlling the operations of RADIANTCA hardware and software and the administration of Certificate services and designated enrolment services.
- Any other records / data / information mandated to be kept confidential and private by the Electronic Transaction Act 2006, its associated rules and regulations.

2.8.2. Types of information not considered confidential or private

Confidential or Private Information shall not include:

- Information included in the issued Digital signature certificate.
- Information included in the CRL.
- Information that is publicly available at the time of its disclosure; or
- Information that becomes publicly available following disclosure; or
- Information that is already known to or was in the possession of RADIANTCA prior to disclosure under Subscriber Agreement or Relying Party Terms & Conditions; or
- Information that is disclosed to RADIANTCA from a third party, which party is not bound by any obligation of confidentiality; or
- Information that is or has been independently developed by RADIANTCA without using the Confidential Information;
- Information that is disclosed with the prior consent of the disclosing party.

2.8.3. Disclosure of Certificate Revocation/Suspension Information

RADIANTCA shall publish list of certificates that are Revoked / Suspended. The reason code of the revoked / suspended certificate shall not be confidential. Any other information related to revocation / suspension shall not be disclosed to anyone other than the subscriber or as required by law.

2.8.4. Release to Law Enforcement Officials

Any Confidential information shall be released by RADIANTCA and its RAs to the courts or Tribunal or law enforcement agencies in accordance with applicable legal requirements.

2.8.5. Release as Part of Civil Discovery

RADIANTCA shall disclose any confidential information in response to Judicial or legal process during any arbitration, litigation or judicial proceedings. In any such disclosure, RADIANTCA shall make reasonable efforts to restrict the disclosure of the information to the extent reasonably required by the proceedings.

2.8.6. Disclosure upon Owner's Request

Any confidential Information of RADIANTCA DSC Owner shall not be disclosed by RADIANTCA under any circumstances which may warrant liability to any other party, except when such confidential information is requested by the owner and the same shall be revealed to him upon such owner establishing the proof of his identity to RADIANTCA or when the confidential information are to be disclosed in response to any Legal / regulatory requirement. RADIANTCA shall not be liable for any disclosure made as per the terms above and the owner shall indemnify RADIANTCA on all situations for all losses, costs or damages incurred by RADIANTCA arising in connection with or incidental to such disclosure.

2.8.7. Other Information Release Circumstances

No stipulation.

2.9. Intellectual Property Rights

2.9.1. Property Rights in Certificates and Revocation Information

All Intellectual Property Rights in and to the certificates and revocation information that is issued under RADIANTCA hierarchy, shall be the sole and exclusive property of RADIANTCA. RADIANTCA and customers grant permission to reproduce and distribute certificates as well as use revocation information to perform relying party function on a nonexclusive basis subject to the Relying Party Terms & Conditions referenced in the certificate.

2.9.2. Property Rights in the CPS

All Intellectual Property Rights in and to this CPS, is recognized by the Participants including Subscribers, relying party, customers, partners, RA and other party belonging to RADIANTCA domain of services, to vest absolutely and irrevocably in the custody of RADIANTCA.

2.9.3. Property Rights in Names

All rights subsisting in any trademark, service mark or trade name as provided for in any certificate application and all distinguished name(s) in the certificate issued to the certificate applicant shall vest with such certificate applicant.

2.9.4. Property Rights in Keys and Key Material

CA and the Subscriber shall retain all rights, including intellectual property rights, in the key Pairs corresponding to the certificate to which they are subject, irrespective of the medium where the key pairs may be stored or protected.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Initial Registration

The applicant shall submit the application offline along with the supporting documents. The RADIANTCA shall verify the authenticity of the application submitted.

3.1.1. Types of Names

All names issued by RADIANTCA, in the Digital signature certificates, shall confirm to the X.500 naming conventions. The Digital signature certificates issued by RADIANTCA shall use Distinguished Names (DN) to facilitate the identities to subscribers. Distinguished Name may comprise of the following fields.

- Common Name (CN): It is a unique name of the Subscriber as provided in the identity documents for the personal certificates and FQDN (fully qualified domain name) for the server certificate
- Digital communication address (E) of the Subscriber.
- Organization (O). Name of the organization
- Organizational Unit (OU): to distinguish various organizational groups like department or sub-divisions within the same organization.
- City or Locality (L).
- State or Province (S), The name of the State / Province of Subscriber's residential or office address.
- Country(C): the country to which the Subscriber belongs.

In addition to the above mentioned fields, RADIANTCA may include more O and OU fields in subscriber certificates to indicate RA name or other details stipulated by OCC.

An example of DN details pertaining to RADIANTCAs is listed in following table:

CN	RADIANTCA	RADIANTCA Class 2 Individual CA	RADIANTCA Class 2 Individual Sub CA
Organization	Radiant InfoTech Nepal (P) Ltd..	Radiant InfoTech Nepal (P) Ltd..	Radiant InfoTech Nepal (P) Ltd..
Organizational Unit	RADIANTCA	RADIANTCA	RADIANTCA
Locality	Kathmandu	Kathmandu	Kathmandu
Zone	Bagmati	Bagmati	Bagmati
Country	NP	NP	NP

3.1.2. Need for names to be meaningful

The subject distinguished names in a digital signature certificate must be meaningful and must be able to determine the identity of the entity/subject. The common name in a certificate shall refer to the generally accepted personal name for individuals, a fully qualified domain name for devices, legal name of the organization, a unit within an organization, any other name identifying the device or any name legally owned or assigned to the organization.

The organization name (O) attribute type, when present in the subject distinguished name, represents the legal name of the Subscriber organization. Such information provided is for identity purposes only and shall not be construed to constitute any power of attorney or other rights.

3.1.3. Rules for Interpreting Various Name Forms

The names shall be interpreted as specified in the section 3.1.1 and 3.1.2 of this CPS. Uniqueness of an existing name can be enhanced by applying other terms, numbers, characters or letters to it.

3.1.4. Uniqueness of Names

The Distinguished names form the basis for the uniqueness of each assigned name. As specified in the CPS, the same Applicant/Subscriber can have multiple Digital signature certificates of different class or purpose.

The purpose of the Distinguished Name is to uniquely identify the subscriber in public repository in which it is published. In addition to the above, RADIANTCA Digital Signature certificate shall also have a unique serial number which enables identification, suspension, activation and revocation of the certificates issued.

3.1.5. Name Claim Dispute Resolution Procedure

Any disputes and claims arising with regard to names shall be settled by RADIANTCA who shall be the final arbiter of such assigned names in the certificates and its decision shall be conclusive and

binding. In addition to above, all certificate applicants are prohibited from using names that infringe on the Intellectual Property Rights of others. The final decision on approval/rejection of names shall lie with RADIANTCA.

3.1.6. Recognition, Authentication, and Role of Trademarks

Any Trademark, upon satisfactory proof of ownership produced to RADIANTCA, shall be reserved by RADIANTCA to its registered owner.

3.1.7. Method to prove possession of private key

The Private key corresponding to the Public Key displayed in the Digital Signature in the hand of the Certificate Subscriber shall be verified by RADIANTCA through the use of digitally signed certificate request pursuant to PKCS#10 or other cryptographically equivalent and any other demonstration approved by RADIANTCA.

3.1.8. Authentication of Organization Identity

The CA shall be responsible for verifying the identity of the organization which has requested for the organization certificates (Class 2 and 3 organization certificate). On a best effort basis, the CA shall perform appropriate validation and/or verification based on the information provided in the application form and the supporting documents in order to establish the identity of the organization. To establish the identity, the organization along with the application shall submit proof of ownership of the name, which shall include from the list of acceptable documents under the verification guidelines as listed in section 3.1.12 of this CPS.

All necessary proof that the person is duly authorized to obtain certificate on behalf the organization shall also be provided.

In addition for the Managed PKI Customers, RADIANTCA will ensure the existence of the Managed PKI customers as outlined above. For device certificates, in addition the customers will have to submit proof on existence of the servers / devices and also proof that the organization has authorized the issuance of a secure ID to the devices.

3.1.9. Authentication of the Identity of RAs

The organizations intend to become RAs under RADIANTCA PKI enter into an agreement with RADIANTCA. RADIANTCA authenticates the identity of the prospective RA before final approval of its status as RA.

3.1.10. Authentication of Individual Identity

The process of identification of a subscriber shall differ based on the class of certificate that is requested by the subscriber and shall include verification of stipulated documents. In case of Class III, the process shall also include face to face authentication. An application for a certificate must be made

(i) personally by an individual or, (ii) by the duly authorized representative of the organization in the case of Class I, Class II and Class III certificates.

3.1.11. Authentication of Device Identity

In cases where the certificate is issued for device (Such as servers, domain names, etc), it shall have a Human Sponsor. Such sponsor shall complete the authentication of Individual / Organization identity in addition to producing the registration information of such Device.
For such purpose, the application shall accompany necessary Equipment identification (Serial Number) or the Service name (FQDN or the Public IP Address). Such information shall be registered in the name of applicant Individual / Organization.

3.1.12. Verification documents required

The verification documents required for each class of digital signature certificate are available at www.RadiantCa.com.np/repository.
This shall cover:

1. List of documents for each hierarchy and class of certificate
2. Attestation procedures
3. Additional notes or guidelines, if any

The verification and validation processes for different hierarchy and classes will be at the discretion of RADIANTCA.

3.2. Rekey and Renewal Process

The procedure of Rekey will be followed for all hierarchy and classes of certificates listed in RADIANTCA repository. The subscriber should apply for renewal prior to expiration of his existing certificate. A new key pair has to be generated and a new certificate is issued against the request. The existing subscriber can use a challenge phrase to send in a request for rekey. .

3.3. Reissuance against Technical errors

In cases where Certificate is not delivered to the subscriber after being approved by CA, for the reason being 'technical error' in communication between CA and the subscriber, RADIANTCA shall reissue a fresh certificate, against a new key-pair without fresh set of documents.

In such cases, applicant/subscriber shall produce necessary proof of information regarding the error, and the loss of private-key.
Such requests shall reach RADIANTCA within minimum time from when the error occurred, along with satisfactory evidence. RADIANTCA reserves all rights to approve or reject such requests.

In such instances, RADIANTCA shall revoke the certificate generated and lost by error, before issuing a new one.

3.4. Rekey after Revocation

For the cases other than section 3.3

1. Once a Digital Signature Certificate is revoked by RADIANTCA, irrespective of the reasons, it shall not be renewed by RADIANTCA.
2. Any subscriber who wishes to re-subscribe to use the Digital Signature Certificate issued by RADIANTCA, has to complete the registration process, afresh as outlined in this CPS.

3.5. Revocation Request

For the cases other than section 3.3, RADIANTCA shall verify, whether the request for revocation of a certificate, is validly raised by the subscriber or the RA who approved the subscriber's application for certificate, before revoking a certificate. In addition, the procedures for authenticating a request for revocation include one or more of the following:

- If applicable, having the subscriber submit the challenge question (As part of the certificate application process, subscribers optionally choose and submit a challenge phrase with their enrolment information), and revoking the certificate if it matches the challenge phrase on record,
- Receiving a message proposed to be from a Subscriber who requested for revocation, inclusive of the Digital Signature of the certificate to be revoked for reference, and
- Online request from Subscriber. The Subscriber submits an online revocation request, or the Subscriber sends a revocation request message that is not digitally signed with reference to the certificate to be revoked.

In these cases, RADIANTCA confirms the revocation request by sending an electronic communication to the certificate subscriber (to the electronic communication contact details listed in the certificate to be revoked) and requests the subscriber to respond confirming the revocation. RADIANTCA revokes the certificate only after receiving the confirmation from the subscriber.

RADIANTCA RA and the Managed PKI clients shall have the right to authenticate for revocation of any Subscriber certificate whose applications are authenticated by them, using their access control rights given to them through their certificate.

RADIANTCA may revoke the certificates based on the online request without digital signature from the subscriber login that is made available for the subscriber.

4. OPERATIONAL REQUIREMENTS

4.1. Certificate Application

The initial registration process shall include the submission of application by offline mode by the applicant for issuing Digital signature certificate along with the supporting documents. Any such application shall be submitted to RA and forwarded to CA for necessary verification / validation. The application may also be directly submitted to CA for necessary verification / validation.

4.1.1. Certificate Applications for End-User Subscriber Certificates

Any end-user certificate applicant requesting for RADIANTCA certificate, needs to go through the registration process consisting of:

- Completing and submitting Application form for certificate along with required information/ documents
- Generating or requesting for generation a key-pair
- Delivering his/ her, or its public key, directly or through an RA, to RADIANTCA
- Demonstrating to RADIANTCA that the certificate Applicant has possession of the Private Key corresponding to the public key sent to RADIANTCA

- Giving consent to the Subscriber Agreement of RADIANTCA, in force at that time

Applications so submitted to RA/RADIANTCA/Managed PKI Customer may be approved or rejected. In case of approval, the issuance of the certificate will be done by one of the Sub CA in RADIANTCA PKI hierarchy.

4.1.2. Certificate Application for Sub CA

RADIANTCA does not require Managed PKI Customers to complete formal certificate applications. Instead, they enter into a contract with RADIANTCA. Managed PKI customer applicants provide their credentials as required demonstrating their identity. All Sub-CAs and Managed PKI customer certificate requests are created and approved by authorized RADIANTCA personnel through a controlled process that requires the participation of multiple trusted individuals. In addition RADIANTCAs certificate requests are also created and approved by authorized RADIANTCA personnel.

4.2. Certificate Issuance

4.2.1. Issuance of End-User Subscriber Certificates

On receipt of a completed application through an RA or Managed PKI Customer, the CA shall validate or reject the information. After thorough verification of all required information/authentication procedures, based on different class of certificates, if such information is found to be complete and correct, the RA approves the certificate application and if found otherwise the CA can reject the certificate application. On receipt of on approval of certificate application, a certificate is created and issued by RADIANTCA based on the information in the certificate application.

4.2.2. Issuance of Sub CA and Managed PKI Certificates

The identities of entities wishing to become Managed PKI Customers of RADIANTCA are authenticated by RADIANTCA. The certificates are issued to perform the MPKI customer services on successful validation by RADIANTCA. Sub-CA requests will be created by authorized RADIANTCA personnel. RADIANTCA shall enter in to a contract with such customer applicant after confirming their identity based on the credentials submitted. The execution of such a contract indicates the complete and final approval of the application by RADIANTCA. The decision to approve or reject customer application is solely at the discretion of RADIANTCA. Following such approval, RADIANTCA issues the certificate. It is to be noted that all certificate requests are validated through a controlled process by authorized RADIANTCA personnel with the aid of multiple trusted persons.

4.3. Certificate Acceptance

A notification is sent to subscriber that the certificate is ready to be downloaded. Along with this notification, a separate PIN or authentication number to download certificate is sent to subscriber. Certificates are made available to subscribers by allowing them to download them from RADIANTCA web site. Downloading the certificate constitutes the subscriber's acceptance of the certificate.

4.4. Certificate Suspension and Revocation

4.4.1. Circumstances for Revocation

4.4.1.1. Circumstances for Revocation of Subscriber Certificate

RADIANTCA shall revoke a subscriber certificate provided:

- The CA approving the subscriber's certificate application has reason to believe that
  - There has been a compromise of the subscriber's private key.
  - The certificate was issued in a manner not materially in accordance with the procedures required by this CPS.
  - The subscriber's data in the certificate is suspected to be inaccurate or belonging to a third party.
  - The information provided by applicant in the certificate application is false or untrue.
- The CA who approved the Subscriber's application for CERTIFICATE, finds out that one/some of the pre-requisites for CERTIFICATE issuance was not complied with properly or done inadequately , and / or;
- In case of organizational certificates, the subscriber's organization name or constitution changes or the relationship between the organization and the representative to whom the certificate was issued has ceased to exist and / or;
- The subscriber has breached materially an obligation or representation or warranty as per the Subscriber Agreement of RADIANTCA, in force at that time , and / or;
- The subscriber/RADIANTCA prefers to disagree on one or some or all the points of Subscriber Agreement with the subscriber, and expresses his/its intention to terminate the Subscriber Agreement and / or;
- The subscriber requests revocation of the certificate and / or;
- RADIANTCA received a request for reissuance against a technical error during download of certificate and / or;
- To comply with any judicial/ law enforcement proceedings.
- 4.4.1.2 Circumstances for Revocation of Sub-CA or RA Certificates
- RADIANTCA revokes a Sub-CA or RA Certificate if:
- It has sufficient information or reason to believe that the Private Key of the Sub-CA or RA is compromised.
- On termination of the agreement between RADIANTCA and the Sub-CA or RA.
- It has sufficient information or reason to believe that the certificate was not issued in conformity with the procedures laid out in this CPS.
- It has sufficient information or reason to believe that the certificate was issued to some entity other than the one named as Subject in the certificate or Certificate was issued without proper authorization from the entity named as Subject in the certificate.
- It has reason to believe that some material pre-requisite for certificate issuance was not satisfied fully or partially.
- The MPKI customer or RA requests revocation of the certificate.
- The Managed PKI customer organization has ceased to exist.
- The termination of agreement between CA and the Managed PKI customer.

4.4.2. Who Can Request Revocation

4.4.2.1. Who Can Request Revocation of Subscriber

Certificate RADIANTCA shall accept revocation requests from:

- The subscriber of the Certificate or his/her legal heir in case the Subscriber has expired
- The authorized personnel or representative of the organization
- The authorized personnel of an MPKI customer.

4.4.2.2. Who Can Request Revocation of a Sub-CA or RA Certificate

Revocation requests for RADIANTCA Sub CA, RA, RADIANTCA Customers and Managed PKI customer's certificates could be initiated by the concerned owner, entity, an authorized agent/entity or the legal heirs of the owner. RADIANTCA could initiate the revocation / request on its own for the above mentioned entities.

4.4.3. Procedure for Revocation Request

4.4.3.1. Procedure for Revocation Request of Subscriber Certificate

An entity requesting for revocation shall be a Subscriber or duly authorized representative, as applicable. Any such request is to be communicated to RADIANTCA or the RA that was involved in the issuance process.

The request will be online through a challenge phrase or in an offline mode through signed revocation request. On receipt of a valid revocation request, RADIANTCA on a best effort basis, will immediately revoke the certificate and notify the subscriber about the certificate revocation. For offline revocation requests, the requests will be processed on the next working day. The updation and publishing the CRL will be done as detailed in this CPS.

4.4.3.2. Procedure for Revocation Request of a Sub-CA or RA Certificate

A RA requesting revocation for RA certificate or authorized RADIANTCA personnel requesting revocation for Sub-CA certificate is required to communicate the request to RADIANTCA. Upon receiving a valid revocation request RADIANTCA will promptly revoke that certificate and notify the requester about the successful revocation. In case of the revocation of a Sub-CA, RADIANTCA will also notify the concerned RAs about the Sub-CA revocation.

4.4.4. Revocation Request Grace Period

Revocation requests are to be verified on receipt and action should be taken as detailed in the section 4.4.3.1 of this CPS

4.4.5. Circumstances for Suspension

RADIANTCA does not offer suspension services for sub-CA or subscriber certificates.

4.4.6. Who can Request Suspension

Not Applicable.

4.4.7. Procedure for Suspension Request

Not Applicable.

4.4.8. Limits on Suspension Period

Not Applicable.

4.4.9. CRL Issuance Frequency

RADIANTCA shall publish CRL's containing information on the revocation of certificates and shall also offer services to enable status check through its repository.

RADIANTCA updates and publishes the CRLs for subscriber Certificates at least once every week, even if no changes to the CRLs have been made.
RADIANTCA shall place a mechanism wherein expired certificates are removed from the CRL's in 30 days after the certificate's expiry date.

4.4.10. Certificate Revocation List Checking Requirements

Relying parties must verify the validity of a certificate against the recent/latest CRL that is published in the RADIANTCA repository to rely on the subject certificate.
The CRLs will be available in RADIANTCA's repository www.RadiantCa.com.np/repository.

4.4.11. On-Line Revocation/Status Checking Availability

In addition to publishing the CRL, RADIANTCA will also provide a web query mechanism to check the status of Certificates in the repository. In addition RADIANTCA will also provide OCSP service to relying parties. This service can be accessed using the OCSP URL published in the certificate.

4.4.12. On-Line Revocation Checking Requirements

In case a relying party does not check certificate status using CRL, they will have to adopt one of the checking mechanisms mentioned in section 4.4.11.

4.4.13. Other Forms of Revocation Advertisements Available

No stipulation

4.4.14. Special Requirements Regarding Key Compromise

In case there has been a key compromise of any RADIANTCA, RADIANTCA will make additional reasonable efforts to notify the relying parties.

4.5. Security Audit Procedures

4.5.1. Types of Events Recorded

RADIANTCA shall log the following significant events either manually or automatically:

CA Life cycle management events, including key generation, storage, archival, backup, recovery, and destruction of

- CA key
- Cryptographic devices

CA and Subscriber Certificate life cycle management events including registration, generation, issuance, revocation and publication of:

- CA certificate
- Sub-CA certificate
- RA certificate
- Subscriber Certificate
- Issuance of CRL.

Events including but not limited to Security such as:

- PKI system access
- PKI system security actions
- Read-Write-Deletion records of Sensitive data/files.
- Personnel changes
- System crashes, hardware failures and other anomalies
- Firewall and router activity
- Physical Access

Log entries should include the following parameters:

- Date and time of the event
- Identity of the entity causing the event

4.5.2. Frequency of Processing Log

System Audit logs will be examined for key security and operational events on a daily basis.

The processing of audit logs includes a review of the audit logs and recording of significant events in an audit log summary. RADIANTCA personnel shall verify that the log has not been tampered with, conduct brief inspection all log entries, and investigate thoroughly in case of any irregularities in the logs. Actions taken based on audit log reviews will be documented.

4.5.3. Retention Period for Audit Log

Audit logs are retained onsite at least twelve months after processing and thereafter archived.

4.5.4. Protection of Audit Log

Only authorized RADIANTCA personnel have access to view and process audit log files. Audit logs are protected from unauthorized viewing, modification, deletion, or other tampering through the use of any or all of various access control mechanism.

4.5.5. Audit Log Backup Procedures

Backup of audit logs on physical removable media are created periodically and protected from use by unauthorized personnel. In addition, audit logs and audit summaries are backed up or copied if in manual form in a safe storage area.

4.5.6. Audit Collection System

Audit data is collected in a combination of automated and manual process and is protected from any unauthorized access, viewing, modification, and deletion or tampering.

4.5.7. Notification to Event-Causing Subject

No notice is required to be served/given to the individual, organization, device, or application that caused any event, which is logged by the audit collection system.

4.5.8. Vulnerability Assessments

Events from Audit logs are captured and are monitored for possible vulnerabilities. Based on results of monitoring activity vulnerability assessment is carried out. The results are reviewed. The monitoring activities are revised based on review.

4.6. Records Archival

4.6.1. Types of Events Recorded

RADIANTCA retains an archive of information and actions that are material to each certificate application and to the creation, Issuance, revocation, expiration, and renewal of each certificate issued by RADIANTCA. These records include all relevant evidence regarding:

- Subscribers' identity and other facts as provided in the certificate and the necessary documentary evidence in support of the certificate application, and
- Those material facts, apart from information required for audit compliance, that may be foreseen
- Records are kept in the form of either digital -based messages or paper-based documents. It is ensured that the indexing, storage, preservation, and reproduction of records are accurate and complete.

4.6.2. Retention Period for Archive

Records associated with certificates will be archived for a period of 7 years.

4.6.3. Protection of Archive

All archive records of RADIANTCA are adequately protected against unauthorized access, view, alterations and tampering and are accessible exclusively by authorized personnel. All systems and media required to process and store the archive records are maintained in accordance with the provisions of the Electronic Transaction Act. .

4.6.4. Archive Backup Procedures

Backup copies for all archives are created on a regular basis and an offsite disaster recovery and warehouse facility is made available for storage of such copies including paper based records.

4.6.5. Requirements for Time-Stamping Of Records

All significant records including Certificates, CRLs, and other revocation database entries contain time and date information.

4.6.6. Archive Collection System

Archives are handled by trusted & authorized personnel of RADIANTCA.

4.6.7. Procedures to Obtain and Verify Archive Information

Access to archive records shall be granted, exclusively to, RADIANTCA trusted personnel and OCC on request.

4.7. Key Changeover

Changeover of Keys of RADIANTCA, RAs and Subscribers shall be carried out as stipulated by the Electronic Transaction Act and in accordance with this CPS. RADIANTCA shall give adequate notice in case of any change in key pair of RADIANTCA, as used for signing Certificates issued under RADIANTCA hierarchy, to the subscribers, RAs & relying parties. Subscriber's keys will not be changed in the case of a compromise.

On or before expiry of an existing certificate, the subscribers shall generate a new key pair and submit the public key along with the new application for issuance of a new Certificate.

4.8. Disaster Recovery and Key Compromise

RADIANTCA maintains off-site backups of data and information as required by Electronic Transaction Act. Backup of CA and Sub-CA private keys are generated and maintained and will be made available in the event of disaster. RADIANTCA maintains a Disaster Recovery centre as per the requirements of guidelines of Electronic Transaction Act, which will be able to handle Issuance and revocation of certificates and publishing of CRL and certification validation services.

In the event of RADIANTCA key compromise, the key management and operations personnel of RADIANTCA including the security, cryptographic operations, administration and management representatives will act as per the incident management and disaster recovery plan which has been approved by RADIANTCA Policy approval committee.

4.9. CA Termination

RADIANTCA reserves the right to terminate any Sub CA at its policy based discretion. In case of termination of a Sub-CA (including Managed PKI), or RADIANTCA, RADIANTCA will create and publish a termination plan that reasonably minimizes disruption to customers, subscribers, and relying parties. The termination plan covers issues including but not limited to:

- Providing notice to subscribers, relying Parties with which RADIANTCA has established contacts, customers, and the OCC who may be affected by such a termination.
- Following duly, the maintenance protocols of the archives, as provided under this CPS and the Act.
- Providing Customer services, revocation service & publishing of CRLs.
- Compensation for any certificates revoked under the termination plan (if found necessary) or assisting issuance of new certificate in lieu of the revoked certificate from another CA. In any case, such compensation shall not exceed the amount paid to RADIANTCA by the certificate holder in respect of the subject certificate.
- The procedure / process of destructing private keys of the CA and/or the Sub CA.
- Provisions needed for the transition of services to a successor Sub-CA.

4.10. Cross Certification

RADIANTCA is licensed by OCC Nepal and the public key of RADIANTCA is signed by RCAN established by OCC.

---

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1. Physical Controls

5.1.1. Site Location and Construction

RADIANTCA shall operate their systems in a physically secured place to prevent any unauthorized handling of sensitive data. The physical security standards are modelled as per the physical and operational security guidelines mentioned in the Electronic Transaction Act, 2006 Rules (Schedule II).

5.1.2. Physical Access

RADIANTCA operation premises including sensitive area inside the premises shall be actively monitored. Physical security is enforced in the facility by establishing multiple tiers and putting in place a set of controls through implementation of policies administrative procedures , use of bio metric systems ,access cards etc., Access to the site is restricted to trusted personnel on need basis and the same is logged .Persons visiting the data centre shall be escorted by trusted personnel after due permissions and the same is recorded by use of DVR's and the access registers.

RADIANTCA has put systems and procedures in place to ensure continuous monitoring on 24X7 basis.

5.1.3. Power and Air Conditioning

Primary and backup power systems / sources are available for providing uninterrupted power supply to the RADIANTCA's operational facility. Temperature and relative humidity (RH) is monitored and controlled on a regular basis by using the HVAC equipment

5.1.4. Water Exposures

RADIANTCA has put in place reasonable measures to ensure that the facility is protected against water exposure like floods etc.

5.1.5. Fire Prevention and Protection

Appropriate equipment has been implemented to minimize the damage due to smoke and fire exposure. The measures implemented are designed to meet various provisions of fire safety regulations applicable in Nepal

5.1.6. Media Storage

RADIANTCA data and information as required by Electronic Transaction Act are backed up and stored within primary site or secure offsite locations. The access to such location is controlled through various access control mechanism, procedures and is limited to RADIANTCA authorized personnel.

5.1.7. Waste Disposal

Paper documents and materials as found unusable shall be disposed. RADIANTCA shall dispose various materials using appropriate equipment or mechanism or as per manufacturer's guidelines. RADIANTCA has policies and procedures in place to dispose media based on sensitivity of information in the media to be destroyed.

5.1.8. Off-Site Backup

All critical data shall be backed up periodically and such backup copies shall be stored securely at an offsite location as identified by RADIANTCA.

5.1.9 Archive backup Procedure

RADIANT CA periodically backs up electronic and manual archives as and when they are created. Copies of the archive shall be stored at the protected disaster recovery site.

5.2. Procedural Controls

5.2.1. Trusted Roles

The trusted roles pertain to roles, performed by RADIANTCA personnel handling the following functions, but not limited to:

- validating information in applications
- accepting, rejecting, or other processing of applications, revocation requests, or renewal requests, or enrolment information
- issuance, or revocation of certificates,
- accessing restricted portions of RADIANTCA's repository
- Handling of subscriber information or requests.

Trusted Persons include, but are not limited to:

- PKI business operations personnel
- System administration personnel including systems, Database, cryptographic administrators
- Personnel that are assigned to perform roles for managing the infrastructure.

The details of trusted personnel is provided under Trusted Personnel List document

5.2.2. Number of Persons Required Per Task

RADIANTCA shall employ appropriate procedures and practices in identifying the number of persons required for handling sensitive functions in order to protect the integrity of CA activities. Where required, RADIANTCA shall implement m out of n control to handle certain sensitive functions.

5.2.3. Identification and Authentication for Each Role

RADIANTCA shall verify the identity of personnel seeking to become trusted personnel by conducting a background check as per the procedure. Additionally RADIANTCA shall request the personnel to appear physically before an authorized personnel or check the identity through a government issued identification. RADIANTCA ensures that a trusted person achieves trusted status to access the facility or to obtain logical access to perform the activity in RADIANTCA systems.

5.3. Personnel Controls

5.3.1. Background, Qualifications, Experience, and Clearance Requirements

RADIANTCA has policies and procedures in place to identify trusted personnel. Such persons shall be required to possess necessary technical and professional competence to discharge their job responsibilities and are required to provide proof of qualification and experience, Trusted personnel shall be subjected to background check at least once every 5 years.

5.3.2. Background Check Procedures

Background checks are performed for trusted personnel as per approved procedures that include, but not limited to:

- Previous employment history,
- Search of Police records,
- Place of Residence
- Education verification
- Reference check.
- RADIANTCA shall avail the services of a private agency or government agency to conduct such background check.

The factors like misrepresentations made, highly unfavourable or unreliable personal references, and certain criminal convictions, etc, revealed in a background check or otherwise, may be considered as valid reasons for rejecting a person's candidature for becoming Trusted Personnel or even for removal of an existing trusted personnel. RADIANTCA HR policy shall form the basis of such actions.

5.3.3. Training Requirements

RADIANTCA shall ensure that well qualified and trained personnel are appointed for the trusted role to perform the job satisfactorily. Any such personnel is provided training in the Electronic Transaction Act and its IT Security policy, RADIANTCA policies, procedures and processes.

RADIANTCA may provide relevant technical training to their personnel to perform their role. The adequacy of such training will be determined by RADIANTCA from time to time.

5.3.4. Retraining Frequency and Requirements

RADIANTCA provides periodic security awareness and any new technology changes training on an ongoing basis based on the newer versions or releases of the products. The frequency of such training will be determined by RADIANTCA from time to time.

5.3.5. Job Rotation Frequency and Sequence

Not stipulated.

5.3.6. Sanctions for Unauthorized Actions

Any violations or unauthorized actions of RADIANTCA policies and procedures will invite RADIANTCA disciplinary actions. Such Disciplinary actions may include without limitation termination of

employment.

5.3.7. Contracting Personnel Requirements

Independent contractors and consultants are permitted access to RADIANTCA secure facilities only to the extent they are escorted and directly supervised by trusted persons.

5.3.8. Documentation Supplied to Personnel

All the personnel involved in RADIANTCA services shall be required to read this CPS and other policy documents.

Relevant documents required to perform the roles are provided to personnel. Such relevancy will be determined by RADIANTCA based on the role performed by the personnel.

RADIANTCA shall make available to the personnel the Digital Signature Certificate policies it supports, its Certification Practice Statement, Information Technology Security Policy and any specific statutes, policies or contracts relevant to their position.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

RADIANTCA key pairs will be generated by multiple trained and trusted personnel in pre-planned key generation ceremonies as per the guidelines laid down in the Key Ceremony Handbook, Key Management Tool user's guide and security policy. This procedure will be documented, recorded and signed by all the individuals entrusted with this activity and will be stored for audit requirements for a period of time deemed appropriate by RADIANTCA Policy approval committee.

Key pairs for RADIANTCAs is generated in a hardware security module (HSM) certified to meet the requirements of FIPS 140-1 level 3 or higher.

Key pair generated and stored in all other cases will be in accordance to the standards prescribed by OCC.

Key usage shall be restricted by implementing appropriate parameters in extensions.

6.1.1. Private Key Delivery to Entity

Generally the end subscriber private key will be generated by the end subscriber and hence there will be no delivery to the end subscribers. In the case of hardware based tokens or smart cards, pre-formatted tokens will be sent to the subscribers and the associated PIN will be sent by an out of band process. The end user will then use the token and the client software provided to him to generate and store the private key and also initiate an online session with the CA server for certificate generation.

6.1.2. Public Key Delivery to Certificate Issuer

End user subscribers will generate a PKCS#10 requests containing their public key and send it to the CA server. This will be accomplished using the client software which will initiate an online session with the CA server and deliver the signed certificates to the subscriber. The online session will be secured by SSL.

6.1.3. CA Public Key Delivery to Users

RADIANTCA makes its CA Public Keys Certificates available to relying parties in repository available at

www.RadiantCa.com.np/repository

6.1.4. Key Sizes

The key length of RADIANTCAs (including Sub-CAs) shall be equivalent to 2048-bit RSA key pair. The key pairs used by RA and Subscribers shall be of 2048 bit key length.

6.1.5. Public Key Parameters Generation

Not stipulated.

6.1.6. Parameter Quality Checking

Not stipulated.

6.1.7. Hardware/Software Key Generation

RADIANTCA generates key pairs in FIPS 140-1 Level 3 compliant hardware security modules.

6.1.8. Key Usage Purposes

RADIANTCA, can at its discretion, using the Key Usage extension in its certificate, restrict the purposes for key usage. (Refer section 7.1.2 of this CPS).

6.2. Private Key Protection

RADIANTCA has put into practice a combination of physical, logical and procedural controls to ensure the security of private keys. Logical and procedural controls are described in this section. Physical access controls are described in section 5.1 of this CPS.

6.2.1. Standards for Cryptographic Modules

RADIANTCA performs all cryptographic operations with its own CA/Sub-CA private keys and client Sub-CA private keys on hardware cryptographic modules rated at a minimum of FIPS 140-1 level 3.

6.2.2. Private Key (N out of M) Multi-Person Control

RADIANTCA has implemented multi-person control to protect the activation data needed to activate CA/Sub-CA private keys within RADIANTCA PKI. RADIANTCA segregates the private key or activation data needed to operate the private key into separate parts called “Secret Shares” Each ‘secret share’ is held by a distinct RADIANTCA trusted personnel referred to as the Custodian. A threshold number of secret shares (n) out of the total number of secret shares (m) are required to operate the private key. Such Secret sharing methodology is applied even in case of RADIANTCA to protect the data needed to activate private keys of RADIANTCA's disaster recovery site.

6.2.3. Private Key Escrow

RADIANTCA will only escrow Subscriber’s encryption private keys. The procedures as approved by OCC will be in place for escrowing subscriber private keys.

6.2.4. Private Key Backup

RADIANTCA creates backup of CA private keys. These are stored in encrypted form in a hardware cryptographic module.

6.2.5. Private Key Archival

At the end of the validity period, CA private key will be deleted and will not be archived. These keys will be destroyed as per requirements specified in section 6.2.9 of this CPS.

6.2.6. Private Key Entry into Cryptographic Module

CA key pairs of RADIANTCA are generated on the hardware cryptographic modules in which the keys will be used. RADIANTCA ensures a copy of such key pairs for disaster recovery purposes. All such copies are transferred in an encrypted form.

6.2.7. Method of Activating Private Key

In case of RADIANTCAs, activation of private key shall require m out of n secret shares as mentioned in section 6.2.2 and will be from the cryptographic hardware device that follows FIPS 140-1level 3 standards.

In case of RA and subscriber, private keys are activated by the client application either by a PIN or password.

6.2.8. Method of Deactivating Private Key

- Process of deactivation for different type of private keys include the following;
- CA's private key: Removal of keys from cryptographic module
- RA's private key: Removal of card from the card reader/tokens from the system or system log off.
- Subscriber's private key; removal of smartcard from the reader/ token from the system if the subscriber has opted for hard token mechanism. If soft token is being used then by logging off from the system. It can also be deactivated at the end of each operation. In any case it shall be the primary responsibility of the subscriber to protect the private key.

6.2.9. Method of Destroying Private Key

At the conclusion of an RADIANTCAs' operational lifetime, the private keys are securely destroyed. This procedure as established in RADIANTCA operation procedures involves multiple trusted personnel of RADIANTCA.

RADIANTCA, shall endeavor to destroy the CA private keys in a manner which ensures that the destroyed key cannot be reconstructed.

Zeroization function is employed in ensuring proper destruction of private keys of RADIANTCA. Procedures are also put in place to log such events. RADIANTCA may adopt and perform different methods to destroy its private keys based on the advancement of the technology.

6.3. Other Aspects Of Key Pair Management

6.3.1. Public Key Archival

All certificate containing public keys (including RADIANTCAs RAs and Subscribers) are archived upon

expiry as part of RADIANTCA's routine backup procedures and kept for a period of seven (7) years as per Electronic Transaction Act.

6.3.2. Usage Periods for the Public and Private Keys

The expiry date of RADIANTCA certificate will be as provided by OCC as per Electronic Transaction Regulation 2008. RADIANTCA may consider stopping issuance of new certificates at a suitable date prior to the expiration of its certificate under RADIANTCA hierarchy so that no certificate issued by a sub CA in the hierarchy expires after the expiration of the corresponding parent CA certificate.

Certificate	**Validity**
All certificates issued including RA, Subscriber	As prescribed by OCC

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

After personalization or initialization of HSM/Smart card/token, no activation data other than access control mechanisms (PIN) are required to operate cryptographic modules.

6.4.2. Activation Data Protection

Passwords or PIN shall not be accessible to anyone except the authorized personnel or certificate holder.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

RADIANTCA ensures that the systems maintaining CA software and data files are trustworthy systems secure from unauthorized access. In addition, RADIANTCA limits access to production servers to those individuals with a valid business reason for such access RADIANTCA production network is logically separated from other components. RADIANTCA uses firewalls and other measures to protect the production network from any internal and external intrusion. Direct access to databases supporting RADIANTCA repository is limited to trusted persons in RADIANTCA operations group having a valid business reason for such access.

6.5.2. Computer security rating

No stipulation

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

RADIANTCA develops implements and maintains Applications, as per its System Development and Change Management Standards.

6.6.2. Security Management Controls

RADIANTCA, ensures that the CA systems are controlled and monitored via its established mechanisms and controls. The integrity of the CA systems/software and configurations is verified, by comparing the hash values generated. RADIANTCA validates the integrity of the CA systems, during installation and thereafter periodically. Such periodicity will be defined by RADIANTCA as required.

6.6.3. Life Cycle Security Ratings

No stipulation

6.7. Network Security Controls

RADIANTCA shall comply with its approved procedures and protocols while performing its CA and RA functions using secured network channels to ensure authorized access. All communication of sensitive information shall be secured by RADIANTCA, through encryption techniques and digital signatures.

6.8. Cryptographic Module Engineering Controls

RADIANTCA shall utilize hardware cryptographic modules rated FIPS 140-2 Level 3 to perform all digital signing operations. All cryptographic module engineering threats are assessed and addressed.

7. CERTIFICATE AND CRL PROFILE

7.1. Certificate Profile

RADIANTCA Certificates complies with:

- ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997
- RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, August 2015 ("RFC 2459").
- At a minimum, RADIANTCA X.509 Certificates contain the basic X.509 Version 1 fields and indicated prescribed values or value constraints

BASIC FIELD	VALUE OR VALUE CONSTRAINT
Version	Version 3
Serial number	Integer value, unique for each certificate issued by the issuer
Signature Algorithm	Algorithm used by the issuer to sign the certificate
Issuer DN	The X.500 distinguished name of the entity signing the certificate
Validity	The certificate validity period represented by two dates: Validity not before - the date on which the certificate validity period begins, and Validity not after - the date on which the certificate validity period ends.
Subject DN	The X.500 distinguished name of the entity associated with the public key certified in the subject public key field of the certificate
Subject Public Key	Encoded in accordance with RFC 2459
Signature	Generated and encoded in accordance with RFC 2459

7.1.1. Version Number(s) Supported

All RADIANTCA Certificates are X.509 version3 Certificates.

7.1.2. Certificate Extensions

RADIANTCA populates X.509 version 3 Certificates with the extensions listed in table below:

EXTENSION	VALUE OR VALUE CONSTRAINT	CRITICALITY
Key Usage	For RADIANTCAs: keyCertSign, CRLSign	TRUE
	For Subscribers: digital Signature, nonrepudiation, key Encipherment, data Encipherment, code Signing	FALSE
Basic Constraints	For RADIANTCAs: CA	TRUE
	For Subscribers: End Entity	
Extended Key Usage	For RADIANTCAs: not stipulated	FALSE
	For Subscribers: ServerAuth, ClientAuth, Code Signing, Email Protection, OCSPSigning	FALSE
Authority Key Identifier	SHA-1 hash value of issuer's public key	FALSE
Subject Key Identifier	SHA-1 hash value of subscriber's public key	FALSE

Subject Alternative		
Name	As per RFC 2459	FALSE
Issuer Alternative Names	As per RFC 2459	FALSE
CRL Distribution Points	URI of the CRL	FALSE

7.1.3. Algorithm Object Identifiers

RADIANTCA issued certificates are signed using sha2With RSA Encryption algorithm.

7.1.4. Name Forms

RADIANTCA issued certificates are populated with an issuer and subject distinguished name.

7.1.5. Name Constraints

No Stipulation.

7.1.6. Certificate Policy Object Identifier

No stipulation.

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

RADIANTCA populates all certificates with a CPS pointer policy qualifier with corresponding OID

---

having a value pointing to the URL of RADIANTCA CPS.

7.1.9. Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.2. CRL Profile

RADIANTCAs issue CRLs that confirm to RFC 2459.

BASIC FIELD	VALUE OR VALUE CONSTRAINT
Version	Version 2
Signature Algorithm	Algorithm used by the issuer to sign the CRL
Issuer DN	The X.500 distinguished name of the entity signing the certificate
Effective Date	Issue date of the CRL. RADIANTCA issued CRLs is effective upon issuance
Next Update	Date by which the next CRL will be issued
Revoked Certificates	List of revoked certificates, including the serial number of revoked certificate and revocation date.

7.2.1. Version Number(s) Supported

All RADIANTCA CRLs are X.509 version 2 CRLs

7.2.2. CRL AND CRL Entry Extensions

No stipulation.

8. SPECIFICATION ADMINISTRATION

8.1. Specification Change Procedures

Amendments to this CPS shall be made by RADIANTCA Policy Approval Committee and need to be approved by the OCC before they become effective.

Updates can be a new document containing the revised CPS or it can contain only the updated information. Proposed new versions or updates shall be posted in RADIANTCA repository.

8.1.1. Items that Can Change Without Notification

RADIANTCA will notify non-material changes such as corrections of typographical errors, changes to URLs, and changes to contact information to the OCC. These changes will be updated in the next release of CPS with the approval of OCC.

8.1.2. Items that Can Change with Notification

8.1.2.1. List of Items

All updates, except those covered in section 8.1.1, to the CPS shall require notification prior to becoming effective.

8.1.2.2. Notification Mechanism

Except as noted under section 8.1.1, RADIANTCA Policy Approval Committee shall submit the proposed updates in electronic and/or paper form to the OCC for approval. After obtaining the OCC's approval the proposed updates to the CPS shall be posted in RADIANTCA repository, which is located at www.RadiantCa.com.np/repository

8.2. Publication and Notification Procedures

8.2.1. Items not published in the CPS

Security documents considered confidential by RADIANTCA are not disclosed to the public.

8.2.2. Distribution of the CPS

This latest version of this CPS is available for viewing in electronic form within RADIANTCA repository at www.RadiantCa.com.np/repository

RADIANTCA also makes the CPS available upon request sent to: info@RadiantCa.com.np

The paper copy of the CPS is available from RADIANTCA upon requests sent to:

Radiant InfoTech Nepal (P) Ltd.
Gairidhara, Kathmandu, Nepal.

Phone: +977-1-4445765, Email: info@RadiantCa.com.np, Website: www.RadiantCa.com.np

8.3. CPS Approval Procedures

The CPS purported for use in RADIANTCA PKI as approved by the RADIANTCA Policy Approval Committee must be finally approved by the OCC.

9. GLOSSARY

9.1. Definitions

A DIGITAL SIGNATURE CERTIFICATE

To demonstrate approval of a Digital signature certificate by a Digital signature certificate applicant while knowing or having notice of its informational contents.

ACCESS

Gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

ACCESS CONTROL

The process of limiting access to the resources of a computer system only to authorized users, programs or other computer systems.

AUTHORITY REVOCATION LIST (ARL)

A list of revoked Certifying Authority Certificates. An ARL is a CRL for Certifying Authority cross-Certificates.

ARCHIVE

To store records and associated journals for a given period of time for security, backup, or auditing purposes.

ASYMMETRIC CRYPTO SYSTEM

A system of a secure key pair consisting of a private key for creating a Digital Signature and a public key to verify the Digital Signature. Detection

AUDIT

A procedure used to validate that controls are in place and adequate for their purposes. Includes recording and analysing activities to detect intrusions or abuses into an information system. Inadequacies found by an audit are reported to appropriate management personnel.

AUDIT TRAIL

A chronological record of system activities providing documentary evidence of processing that enables management staff to reconstruct, review, and examine the sequence of states and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results. Confirm

AUTHENTICATION

A process used to confirm the identity of a person or to prove the integrity of specific information. Message authentication involves determining its source and verifying that it has not been modified or replaced in transit. (See also VERIFY (a DIGITAL SIGNATURE))

AUTHORIZATION

The granting of rights, including the ability to access specific information or resources.

AVAILABILITY

The extent to which information or processes are reasonably accessible and usable, upon demand, by an authorized entity, allowing authorized access to resources and timely performance of time-critical operations.

BACKUP

The process of copying critical information, data and software for the purpose of recovering essential processing back to the time the backup was taken.

CERTIFICATE

A Digital signature certificate issued by Certifying Authority.

CERTIFICATE CHAIN

An ordered list of Certificates containing an end-user Subscriber Certificate and Certifying Authority Certificates (See VALID CERTIFICATE).

CERTIFICATE EXPIRATION

The time and date specified in the Digital signature certificate when the operational period ends, without regard to any earlier suspension or revocation.

CERTIFICATE EXTENSION

An extension field to a Digital signature certificate which may convey additional information about the public key being certified, the certified Subscriber, the Digital signature certificate issuer, and/or the certification process. Standard extensions are defined in Amendment 1 to ISO/IEC 9594-8:1995 (X.509). Custom extensions can also be defined by communities of interest. Render

CERTIFICATE ISSUANCE

The actions performed by a Certifying Authority in creating a Digital Signature

Certificate and notifying the Digital signature certificate applicant (anticipated to become a Subscriber) listed in the Digital signature certificate of its contents.

CERTIFICATE MANAGEMENT [MANAGEMENT OF DIGITAL SIGNATURE CERTIFICATE]

Certificate management includes, but is not limited to, storage, distribution, dissemination, accounting, publication, compromise, recovery, revocation, suspension and administration of Digital signature certificates. A Certifying Authority undertakes Digital signature certificate management functions by serving as a Registration Authority for Subscriber Digital signature certificates. A Certifying Authority designates issued and accepted Digital signature certificates as valid by publication.

CERTIFICATE POLICY

A specialized form of administrative policy tuned to electronic transactions performed during Digital signature certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of Digital signature certificates. Indirectly, a Certificate policy can also govern the transactions conducted

using a communications system protected by a Certificate based security system. By controlling critical Certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

CERTIFICATE REVOCATION (SEE REVOKE A CERTIFICATE) CERTIFICATE REVOCATION LIST (CRL)

A periodically (or exigently) issued list, digitally signed by a Certifying Authority, of identified Digital signature certificates that have been suspended or revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the suspended or revoked Digital signature certificates' serial numbers, and the specific times and reasons for suspension and revocation.

CERTIFICATE SERIAL NUMBER

A value that unambiguously identifies a Digital signature certificate generated by a Certifying Authority.

CERTIFICATION / CERTIFY

The process of issuing a Digital signature certificate by a Certifying Authority.

CERTIFYING AUTHORITY SYSTEM

All the hardware and software system (e.g. Computer, PKI servers, network devices etc.) used by the Certifying Authority for generation, production, issue and management of Digital signature certificate.

CERTIFICATION PRACTICE STATEMENT (CPS)

A statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital signature certificates.

CERTIFIER (See ISSUING AUTHORITY) CHALLENGE PHRASE

A set of numbers and/or letters that are chosen by a Digital signature certificate applicant, communicated to the Certifying Authority with a Digital signature certificate application, and used by the Certifying Authority to authenticate the Subscriber for various purposes as required by the Certification Practice Statement. A challenge phrase is also used by a secret shareholder to authenticate himself, herself, or itself to a secret share issuer.

CERTIFICATE CLASS

A Digital signature certificate of a specified level of trust.

CLIENT APPLICATION

An application that runs on an electronic device and relies on a server to perform some operation.

COMMON KEY

Some systems of cryptographic hardware require arming through a secret-sharing process and require that the last of these shares remain physically attached to the hardware in order for it to stay armed.

In this case, “common key” refers to this last share. It is not assumed to be secret as it is not continually in an individual’s possession.

COMMUNICATION/NETWORK SYSTEM

A set of related, remotely connected devices and communications facilities including more than one computer system with the capability to transmit data among them through the communications facilities (covering ISDN, lease lines, dial-up, LAN, WAN, etc.).

COMPROMISE

A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. (Cf., DATA INTEGRITY)

COMPUTER

Any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.

CONFIDENTIALITY

The condition in which sensitive data is kept secret and disclosed only to authorized parties.

CONFIRM

To ascertain through appropriate inquiry and investigation. (See also AUTHENTICATION; VERIFY A DIGITAL SIGNATURE)

CONTINGENCY PLANS

The establishment of emergency response, back up operation, and post-disaster recovery processes maintained by an information processing facility or for an information system.

Establish the strategy for recovering from unplanned disruption of information processing operations. The strategy includes the identification and priority of what must be done, who performs the required action, and what tools must be used.

A document developed in conjunction with application owners and maintained at the primary and backup computer installation, which describes procedures and identifies the personnel necessary to respond to abnormal situations such as disasters. Contingency plans help managers ensure that computer application owners continue to process (with or without computers) mission-critical applications in the event that computer support is interrupted.

CONTROLS

Measures taken to ensure the integrity and quality of a process.

CORRESPOND

To belong to the same key pair. (See also PUBLIC KEY; PRIVATE KEY)

CRITICAL INFORMATION

Data determined by the data owner as mission critical or essential to business purposes.

CROSS-CERTIFICATE

A Certificate used to establish a trust relationship between two Certifying Authorities.

CRYPTOGRAPHY (See also PUBLIC KEY CRYPTOGRAPHY)

The mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key.

A discipline that embodies the principles, means, and methods for transforming data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorized uses.

DAMAGE

Means to destroy, alter, delete, add, modify or rearrange any digital resource by any means.

DATA

Means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a digital system or electronic network, and may be in any form (including printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of an electronic device.

DATA CONFIDENTIALITY (See CONFIDENTIALITY)

DIGITAL SIGNATURE CERTIFICATE APPLICANT

A person that requests the issuance of a public key Digital signature certificate by a Certifying Authority. (See also CA APPLICANT; SUBSCRIBER)

DIGITAL SIGNATURE CERTIFICATE APPLICATION

A request from a Digital signature certificate applicant (or authorized agent) to a Certifying Authority for the issuance of a Digital signature certificate. (See also CERTIFICATE APPLICANT; CERTIFICATE SIGNING REQUEST)

DIGITAL SIGNATURE

Means authentication of any electronic record by a Subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of the Electronic Transaction Act, 2006.

DIGITAL SIGNATURE CERTIFICATE

Means a Digital signature certificate issued under sub-section (4) of section 35 of the Electronic Transaction Act, 2006.

DISTINGUISHED NAME

A set of data that identifies a real-world entity, such as a person in a digital context.

DOCUMENT

A record consisting of information inscribed on a tangible medium such as paper rather than digital - based information. (See also MESSAGE; RECORD)

ELECTRONIC FORM

With reference to information means any information generated, sent, received or stored in media,

---

magnetic, optical, device memory, microfilm, electronic device generated microfiche or similar device.

DIGITAL COMMUNICATION ADDRESS

Messages sent, received or forwarded in Digital form via electronic devices based communication mechanism.

ELECTRONIC DEVICE

A device depending on the principles of electronics and using the manipulation of electron flow for its operation. It includes computers, mobiles or any other form of electronic devices.

ELECTRONIC RECORD

Means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or electronic devices generated microfiche.

ENCRYPTION

The process of transforming plaintext data into an unintelligible form (cipher text) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).

EXTENSIONS

Extension fields in X.509 v3 Certificates. (See X.509)

FIREWALL/DOUBLE FIREWALL

One of several types of intelligent devices (such as routers or gateways) used to isolate networks. Firewalls make it difficult for attackers to jump from network to network. A double firewall is two firewalls connected together. Double firewalls are used to minimize risk if one firewall gets compromised or provide address translation functions.

FUNCTION

In relation to a an electronic device, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within an electronic device..

GENERATE A KEY PAIR

A trustworthy process of creating private keys during Digital signature certificate application whose corresponding public keys are submitted to the applicable Certifying Authority during Digital signature certificate application in a manner that demonstrates the applicant's capacity to use the private key.

HASH (HASH FUNCTION)

An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:

(i) A message yields the same result every time the algorithm is executed using the same message as input.

ii) It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.

It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

IDENTIFICATION / IDENTIFY

The process of confirming the identity of a person. Identification is facilitated in public key cryptography by means of Certificates.

IDENTITY

A unique piece of information that marks or signifies a particular entity within a domain. Such information is only unique within a particular domain.

INFORMATION

Includes data, text, images, sound, voice, codes, programmes, software and databases or microfilm or electronic device generated microfiche.

INFORMATION TECHNOLOGY SECURITY

All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability.

INFORMATION TECHNOLOGY SECURITY POLICY

Rules, directives and practices that govern how information assets, including sensitive information, are managed, protected and distributed within an organization and its Information Technology systems.

KEY

A sequence of symbols that controls the operation of a cryptographic transformation

(E.g. encipherment, decipherment, cryptographic checks function computation, Signature generation, or Signature verification).

KEY GENERATION

The trustworthy process of creating a private key/public key pair.

KEY MANAGEMENT

The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.

KEY PAIR

In an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a Digital Signature created by the private key.

LICENCE

Means a license granted to a Certifying Authority.

LOCAL AREA NETWORK (LAN)

A geographically small network of computers and supporting components used by a group or department to share related software and hardware resources.

MANAGEMENT OF DIGITAL SIGNATURE CERTIFICATE (SEE CERTIFICATE MANAGEMENT)

MEDIA
The material or configuration on which data is recorded. Examples include magnetic taps and disks.

MESSAGE
A Digital representation of information; an electronic device based record. A subset of RECORD. (See also RECORD)

NAME
A set of identifying attributes purported to describe an entity of a certain type.

NETWORK
A set of related, remotely connected devices and communications facilities including more than one electronic device system with the capability to transmit data among them through the communications facilities.

NONREPUDIATION
Provides proof of the origin or delivery of data in order to protect the sender against a false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent. Note: Only a trier of fact (someone with the authority to resolve disputes) can make an ultimate determination of non-repudiation. By way of illustration, a Digital Signature verified pursuant to this Certification Practice Statement can provide proof in support of a determination of non-repudiation by a trier of fact, but does not by itself constitute non-repudiation.

ON-LINE
Communications that provide a real-time connection.

OPERATIONS ZONE
An area where access is limited to personnel who work there and to properly escorted visitors. Operations Zones should be monitored at least periodically, based on a threat risk assessment (TRA), and should preferably be accessible from a Reception Zone.

OPERATIONAL PERIOD
The period starting with the date and time a Digital signature certificate is issued (or on a later date and time certain if stated in the Digital signature certificate) and ending with the date and time on which the Digital signature certificate expires or is earlier suspended or revoked.

ORGANIZATION
An entity with which a user is affiliated. An organization may also be a user.

PASSWORD (PASS PHRASE; PIN NUMBER)
Confidential authentication information usually composed of a string of characters used to provide access to an electronic device.

PC CARD (SEE ALSO SMART CARD)

A hardware token compliant with standards promulgated by the Personal Computer Memory Card International Association (PCMCIA) providing expansion capabilities to computers, including the facilitation of information security.

PERSON

Means any company or association or individual or body of individuals, whether incorporated or not.

PERSONAL PRESENCE

The act of appearing (physically rather than virtually or figuratively) before a Certifying Authority or its designee and proving one's identity as a prerequisite to Digital signature certificate issuance under certain circumstances.

PKI (PUBLIC KEY INFRASTRUCTURE) / PKI SERVER

A set of policies, processes, server platforms, software and workstations used for the purpose of administering Digital signature certificates and public-private key pairs, including the ability to generate, issue, maintain, and revoke public key Certificates.

PKI HIERARCHY

A set of Certifying Authorities whose functions are organized according to the principle of delegation of authority and related to each other as subordinate and superior Certifying Authority.

POLICY

A brief document that states the high-level organization position, states the scope, and establishes who is responsible for compliance with the policy and the corresponding standards. Following is an abbreviated example of what a policy may contain:

- Introduction
- Definitions
- Policy Statement identifying the need for “something” (e.g. data security)
- Scope
- People playing a role and their responsibilities
- Statement of Enforcement, including responsibility

PRIVATE KEY

The key of a key pair used to create a Digital Signature.

PROCEDURE

A set of steps performed to ensure that a guideline is met.

PUBLIC KEY

The key of a key pair used to verify a Digital Signature and listed in the Digital signature certificate.

PUBLIC KEY CERTIFICATE (See CERTIFICATE)

PUBLIC KEY CRYPTOGRAPHY (See CRYPTOGRAPHY)

A type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a Digital Signature; the private key is kept secret by its holder and can decrypt information or generate a Digital Signature.

PUBLIC KEY INFRASTRUCTURE (PKI)

The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. It includes a set of policies, processes, server platforms, software and workstations, used for the purpose of administering Digital signature certificates and keys.

PUBLIC/PRIVATE KEY PAIR (See PUBLIC KEY; PRIVATE KEY; KEY PAIR)

RECIPIENT (of a DIGITAL SIGNATURE)

A person who receives a Digital Signature and who is in a position to rely on it, whether or not such reliance occurs. (See also RELYING PARTY)

RECORD

Information that is inscribed on a tangible medium (a document) or stored in an electronic or other medium and retrievable in perceivable form. The term “record” is a superset of the two terms “document” and “message”. (See also DOCUMENT; MESSAGE)

RE-ENROLLMENT (See also RENEWAL)

RELY / RELIANCE (on a CERTIFICATE and DIGITAL SIGNATURE)

To accept a Digital Signature and act in a manner that could be detrimental to oneself were the Digital Signature to be ineffective. (See also RELYING PARTY; RECIPIENT)

RELYING PARTY

A recipient who acts in reliance on a Certificate and Digital Signature. (See also RECIPIENT; RELY OR RELIANCE (on a CERTIFICATE and DIGITAL SIGNATURE))

RENEWAL

The process of obtaining a new Digital signature certificate of the same class and type for the same subject once an existing Digital signature certificate has expired.

REPOSITORY

A database of Digital signature certificates and other relevant information accessible on-line.

REPUDIATION (See also NONREPUDIATION)

The denial or attempted denial by an entity involved in a communication of having participated in all or part of the communication.

REVOKE A CERTIFICATE

The process of permanently ending the operational period of a Digital signature certificate from a specified time forward.

RISK

The potential of damage to a system or associated assets that exists as a result of the combination of security threat and vulnerability.

SECRET SHARE

A portion of a cryptographic secret split among a number of physical tokens.

SECURITY PROCEDURE

Means the security procedure prescribed under section 16 of the Electronic Transaction Act, 2006.

SECURITY

The quality or state of being protected from unauthorized access or uncontrolled losses or effects. Absolute security is impossible to achieve in practice and the quality of a given security system is relative. Within a state-model security system, security is a specific "state" to be preserved under various operations.

SECURITY POLICY

A document which articulates requirements and good practices regarding the protections maintained by a trustworthy system.

SERIAL NUMBER (See CERTIFICATE SERIAL NUMBER)

SERVER

A computer system that responds to requests from client systems.

SMART CARD

A hardware token that incorporates one or more integrated circuit (IC) chips to implement cryptographic functions and that possesses some inherent resistance to tampering.

S/MIME

A specification for E-mail security exploiting cryptographic message syntax in an Internet MIME environment.

SUBJECT (OF A CERTIFICATE)

The holder of a private key corresponding to a public key. The term “subject” can refer to both the equipment and device that holds a private key and to the individual person, any, who controls that equipment or device. A subject is assigned an unambiguous name, which is bound to the public key contained in the subject’s Digital signature certificate.

SUBJECT NAME

The unambiguous value in the subject name field of a Digital signature certificate, which is bound to the public key.

SUBSCRIBER
A person in whose name the Digital signature certificate is issued.

SUBSCRIBER AGREEMENT
The agreement executed between a Subscriber and a Certifying Authority for the provision of designated public certification services in accordance with this Certification Practice Statement.

SUBSCRIBER INFORMATION
Information supplied to a certification authority as part of a Digital signature certificate application. (See also CERTIFICATE APPLICATION)

SYSTEM ADMINISTRATOR
The person at a computer installation who designs, controls, and manages the use of the computer system.

THREAT
A circumstance or event with the potential to cause harm to a system, including the destruction, unauthorized disclosure, or modification of data and/or denial of service.

TOKEN
A hardware security token containing a user's private key(s), public key Certificate, and, optionally, a cache of other Certificates, including all Certificates in the user's certification chain.

TRANSACTION
A electronic device based transfer of business information, which consists of specific processes to facilitate communication over global networks.

TRUST
Generally, the assumption that an entity will behave substantially as expected. Trust may apply only for a specific function. The key role of this term in an authentication framework is to describe the relationship between an authenticating entity and a Certifying Authority. An authenticating entity must be certain that it can trust the Certifying Authority to create only valid and reliable Digital signature certificates, and users of those Digital signature certificates rely upon the authenticating entity's determination of trust.

TRUSTED POSITION
A role that includes access to or control over cryptographic operations that may materially affect the issuance, use, suspension, or revocation of Digital signature certificates, including operations that restrict access to a repository.

TRUSTWORTHY SYSTEM
Electronic device, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.

TYPE (OF CERTIFICATE)

The defining properties of a Digital signature certificate, which limit its intended purpose to a class of applications uniquely, associated with that type.

UNIFORM RESOURCE LOCATOR (URL)

A standardized device for identifying and locating certain records and other resources located on the World Wide Web.

USER

An authorized entity that uses a Certificate as applicant, Subscriber, recipient or relying party, but not including the Certifying Authority issuing the Digital signature certificate. (See also CERTIFICATE APPLICANT; ENTITY; PERSON; SUBSCRIBER)

VALIDATION (OF CERTIFICATE APPLICATION)

The process performed by the Certifying Authority or its agent following submission of a Digital signature certificate application as a prerequisite to approval of the application and the issuance of a Digital signature certificate. (See also AUTHENTICATION; SOFTWARE VALIDATION)

VERIFY (A DIGITAL SIGNATURE)

In relation to a Digital Signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether —

(a) The initial electronic record was affixed with the Digital Signature by the use of private key corresponding to the public key of the Subscriber;

(b) The initial electronic record is retained intact or has been altered since such electronic record was so affixed with the Digital Signature.

VULNERABILITY

A weakness that could be exploited to cause damage to the system or the assets it contains.

WEB BROWSER

A software application used to locate and display web pages.

WORLD WIDE WEB (WWW)

A hypertext-based, distributed information system in which users may create, edit, or browse hypertext documents. A graphical document publishing and retrieval medium; a collection of linked documents that reside on the Internet.

X.509

The ITU-T (International Telecommunications Union-T) standard for Digital signature certificates. X.509 v3 refers to Certificates containing or capable of containing extensions.