Certification Practice Statement (CPS)

for

Digital Signature Certification Services

(***Version 4.4***)

August 24, 2009

OID: 2.16.356.100.1.4.2

Certifying Authority
National Informatics Centre
Department of Information Technology
Ministry of Communications & Information Technology
Government of India

NIC Certifying Authority
National Informatics Centre
Department of Information Technology
Ministry of Communications & Information Technology
A-Block, CGO Complex, Lodhi Road,
New Delhi – 110 003.

Certification Practice Statement (CPS) V4.4

DOCUMENTATION VERSION CONTROL

VERSION	DATE	AUTHOR (S)	REASON FOR CHANGE
0.1	Dec 2001	Ratnaboli G Dinda C S Rao	Initial draft
1.0	14-01-02	Ratnaboli G Dinda C S Rao	Reworking
1.1	17-01-02	Ratnaboli G Dinda C S Rao	To incorporate changes after installation of HSM
1.2	August 2002	Ratnaboli G Dinda C S Rao	ICICI Infotech CA S/w License expiration
2.0	10-01-03	Manoj Kulshreshth Sumeet Jethra	New Software Next update due on 30th April 2003
2.0	6-02-03	P K Saha, Manoj K Kulshreshth	Changes made as per comments received from CCA
2.0	22-04-03	P K Saha, Anupama Mandal, Manoj K Kulshrshth	Changes made after Auditors Comment. Next update due on 30th June 2003
2.1	20-03-04	S K Roy Manoj Kulshreshth	Extending validity of certificates for two years, mandatory requirement for DN
3.0	30-03-05	S K Roy Manoj Kulshreshth	Certificate fees for PSU, Statutory Bodies, Serving revocation/ suspension request within 72 hours
4.0	01.09.05	S K Roy Manoj Kulshreshth S Khan	Issuance of DSCs to Government Registered Private Companies, Encryption Certificates, inclusion of more types of certificates
4.1	16.02.06	Manoj Kulshreshth Nagendra Kumar	Issuance of DSC on crypto device
4.2	16.03.07	S K Roy P K Saha Anupama Mandal Manoj Kulshreshth S Khan	Exclusion of single key-pair signing and encryption and Inclusion of Declaration form for encryption
4.3	06.11.07	P K Saha Anupama Mandal Manoj Kulshreshth Anuradha Valsa Raj S Khan	Inclusion of Individual from Govt., PSU/Statutory Bodies, Government Registered Companies in the eligibility criteria for encryption certificates
4.4	24.08.09	P K Saha Anupama Mandal Manoj Kulshreshth Anuradha Valsa Raj	Inclusion of Sub-CA & Replacing DSC Fees with pointer to NICCA website for Fee Structure, adding clarity to certain sections/sub-sections of the CPS.

OID Structure

OID of NIC-CA	**:**	**2.16.356.100.1.4**
OID of CPS of NIC-CA	**:**	**2.16.356.100.1.4.2**
OID of CP of NIC-CA	**:**	**2.16.356.100.1.4.3-n**
OID of CCA of India	**:**	**2.16.356.100**
OID of India Object Identifiers	**:**	**2.16.356**
OID of Joint assignments by country	**:**	**2.16**
OID of ISO/ITU-T jointly assigned	**:**	**2**

-

Contents

1. INTRODUCTION 9
1.1. Policy Overview 10
1.1.1. Certificates Classes 10
1.1.2. Types of Certificates 11
1.1.2.1. Signing Certificate 11
1.1.2.2. Encryption Certificate 11
1.1.2.3. Mandatory Declaration by Subscriber for Encryption Certificate 12
1.1.2.4. Web Server Certificate 12
1.1.2.5. Client Certificate 12
1.1.2.6. Object Signing Certificate 13
1.1.2.7. IP Sec Tunnel 13
1.1.2.8. IP Sec User 13
1.1.2.9. OCSP Responder 13
1.1.2.10. OCSP Signing 13
1.1.2.11. Time Stamping 13
1.1.2.12. Smart card Logon 14
1.2. Applicability 14
1.3. Certifying Authority 14
1.3a Sub-CA 14
1.4. Registration Authorities 14
1.5. End-Entities 14
1.6. Applications 15
1.7. Contact Details 15
2. GENERAL PROVISIONS 16
2.1. Obligations 16
2.1.1. CA Obligations 16
2.1.1.1. Compliance 16
2.1.1.2. Certificate Requests 16
2.1.1.3. Validity of Certificates 17
2.1.2. Obligations of the NIC Coordinator at the requesting organisation 17
2.1.2.1. Compliance 17
2.1.2.2. Authentication of the RA's credentials 17
2.1.2.3. Maintain Certificate Application Information 17
2.1.3. Subscriber Obligations 17
2.1.3.1. Accuracy of Representations in Certificate Applications 17
2.1.3.2. Key Pair Generation 17
2.1.3.3. Protection of the Entity's Private Key 18
2.1.3.4. Notification of CA upon Private Key Compromise 18
2.1.3.5. Notification of CA upon any change in their Certificate Content 18
2.1.3.6. Restrictions on Private Key and Certificate use 18
2.1.3.7. Personal Data 18
2.1.3.8. E-mail ID 18
2.1.3.9. Enrollment 18
2.1.3.10. Submission of Public Key 19
2.1.3.11. Protection of Private Key 19
2.1.3.12. Private Key Usage 19
2.1.3.13. Duplicate Certificate Requests 19
2.1.3.14. Accept Root Certificate of CA 19
2.1.3.15. Use of Certificate 19
2.1.3.16. Certificate Acceptance 20
2.1.4. Relying Party Obligations 20
2.1.5. Repository Obligations 20
2.1.6. RA Personnel Obligations 20
2.2. Liability 21
2.2.1. Disclaimer 21
2.2.2. Loss Limitations 21

2.3. Financial Responsibility 21
2.3.1. Indemnification of Certificate Authority by Relying Parties and Subscribers 21
2.3.2. Fiduciary Relationships between various Entities 21
2.3.3. Administrative Processes 21
2.4. Interpretation and Enforcement 22
2.4.1. Governing Laws 22
2.4.2. Sever ability of Provisions 22
2.4.3. Dispute Resolution Procedures 22
2.5. Fees 22
2.5.1. Certificate Issuance Fees 22
2.5.2. Certificate Access Fees 23
2.5.3. Revocation or Status information Access Fees 23
2.5.4. Fees for other services such as Policy Information 23
2.5.5. Refund Policy 23
2.6. Publication and Repository 23
2.6.1. Publication of CA Information 23
2.6.2. Frequency of publication 23
2.6.3. Access Controls 23
2.6.4. Repositories 23
2.7. Compliance Audit 23
2.7.1. Frequency of Entity Compliance Audit 24
2.7.2. Identity/Qualifications of Auditor 24
2.7.3. Topics covered by Audit 24
2.7.4. Auditors Relationship with NICCA 24
2.7.5. Actions taken as a Result of Deficiency 24
2.7.6. Communication of Results 24
2.8. Confidentiality 24
2.8.1. Types of Information to be kept Confidential 25
2.8.2. Types of Information not considered Confidential 25
2.8.3. Disclosure of Certificate Revocation/Suspension Information 25
2.8.4. Release to Law Enforcement Officials 25
2.8.5. Information that can be revealed as part of civil discovery 25
2.8.6. Disclosure upon Owner's Request 25
2.8.7. Other information Release Circumstances 25
2.9. Intellectual Property Rights 25
3. IDENTIFICATION AND AUTHENTICATION 27
3.1. Initial Registration 27
3.1.1. Types of Names 27
3.1.1.1. Country 27
3.1.1.2. Name (Common Name) 27
3.1.1.3. Organization 27
3.1.1.4. Organizational Unit 27
3.1.1.5. E-Mail 28
3.1.1.6. State 28
3.1.1.7. Locality 28
3.1.2. Need for Names to be Meaningful 28
3.1.3. Rules for interpreting Various Name Forms 28
3.1.4. Name Claim Dispute Resolution Procedure 28
3.1.5. Method to prove Possession of Private Key 28
3.1.6. Authentication of Organization Identity 28
3.1.7. Authentication of Individual Identity 28
3.2. Routine Re-key 29
3.3. New Certificate after Revocation 29
3.4. Revocation/Suspension Request 29
3.4.1. Suspension Request 29
3.4.2. Revocation Request 30
4. OPERATIONAL REQUIREMENTS 31
4.1. Certificate Application 31
4.2. Certificate Issuance 31
4.3. Certificate Acceptance 31

4.4. Certificate Suspension and Revocation 32
4.4.1. Circumstances for Revocation 32
4.4.2. Who can Request Revocation 32
4.4.3. Procedure for Revocation Request 32
4.4.3.1. Root Certificate Revocation 35
4.4.4. Revocation Request Grace Period 35
4.4.5. Circumstances for Suspension 35
4.4.6. Who can Request Suspension 35
4.4.7. Procedure for Suspension Request 35
4.4.8. Limits on Suspension Period 35
4.4.9. CRL Issuance Frequency 35
4.4.10. CRL Checking Requirements 36
4.4.11. On-line Revocation/Status Checking Availability 36
4.4.12. On-line Revocation Checking Requirements 36
4.4.13. Other forms of Revocation Advertisements available 36
4.4.14. Checking Requirements for other forms of Revocation Advertisements 36
4.4.15. Special requirements Re-key compromise 36
4.5. Security Audit Procedures 36
4.5.1. Types of Events Recorded 36
4.5.2. Frequency of Processing Log 37
4.5.3. Retention Period for Audit Log 37
4.5.4. Protection of Audit Log 37
4.5.5. Audit Log Backup Procedures 37
4.5.6. Vulnerability Assessments 37
4.6. Records Archival 37
4.6.1. Types of Event Recorded 37
4.6.2. Retention Period for Archive 38
4.6.3. Protection of Archive 38
4.6.4. Archive Backup Procedures 38
4.6.5. Requirements for Time-Stamping of Records 38
4.6.6. Archive Collection System (Internal or External) 38
4.6.7. Procedures to obtain and Verify Archive Information 38
4.7. Key Changeover 38
4.8. Compromise and Disaster Recovery 38
4.8.1. Computing Resources, Software, and/or Data are Corrupted 38
4.8.2. Entity Public Key is Revoked 39
4.8.2.1. Subscriber's Public Key 39
4.8.2.2. CA Public Key 39
4.8.3. Entity Key is Compromised 39
4.8.3.1. Subscriber’s Key is Compromised 39
4.8.3.2. CA Key is Compromised 39
4.8.4. Secure Facility after a Natural or other type of Disaster 39
4.9. CA Termination 40
5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY 41
5.1. Physical Security Control 41
5.1.1. Site Location and Construction 41
5.1.2. Physical Access 41
5.1.3. Power and Air conditioning 41
5.1.4. Water Exposures 41
5.1.5. Fire Prevention and Protection 41
5.1.6. Media Storage 42
5.1.7. Waste Disposal 42
5.1.8. Off-Site Backup 42
5.2. Procedural Controls 42
5.2.1. Trusted Roles 42
5.2.2. Number of Persons Required Per Task 43
5.2.3. Identification and Authentication for Each Role 43
5.3. Personnel Controls 43
5.3.1. Background, Qualifications, Experience, and Clearance Requirements 43
5.3.2. Background Check Procedures 43

5.3.3. Training Requirements 44
5.3.4. Retraining Frequency and Requirements 44
5.3.5. Job Rotation Frequency and Sequence 44
5.3.6. Sanctions for Unauthorized Actions 44
5.3.7. Contracting Personnel Requirements 44
5.3.8. Documentation Supplied to Personnel 44
6. TECHNICAL SECURITY CONTROLS 45
6.1. Key Pair Generation and Installation 45
6.1.1. Key Pair Generation 45
6.1.2. Private Key Delivery to Entity 45
6.1.3. Public Key Delivery to Certificate Issuer 45
6.1.4. CA Public Key Delivery to Users 45
6.1.6. Public Key Parameters Generation 45
6.1.7. Parameter Quality Checking 45
6.1.8. Hardware/Software Key Generation 45
6.1.9. Key Usage Purposes (as per X.509 v3 key usage field) 46
6.2. Private Key Protection 46
6.2.1. Standards for Cryptographic Module 46
6.2.2. Private Key (n out of m) Multi-Person Control 46
6.2.3. Private Key Escrow 46
6.2.4. Private Key Backup 46
6.2.5. Private Key Archival 46
6.2.6. Private Key entry into Cryptographic Module 46
6.2.7. Method of Activating Private Key 46
6.2.8. Method of Deactivating Private Key 46
6.2.9. Method of Destroying Private Key 47
6.3. Other Aspects of Key Pair Management 47
6.3.1. Public Key Archival 47
6.3.2. Usage periods for the Public and Private Keys 47
6.4. Activation Data 47
6.4.1. Activation Data Generation and Installation 47
6.4.2. Activation Data Protection 47
6.4.3. Other Aspects of Activation Data 47
6.5. Computer Security Control 47
6.5.1. Specific Computer Security Technical Requirements 47
6.5.2. Computer Security Rating 48
6.6. Life Cycle Technical Controls 48
6.6.1. System Development Controls 48
6.6.2. Security Management Controls 48
6.6.3. Life Cycle Security Ratings 48
6.7. Network Security Controls 48
6.8. Cryptographic Module Engineering Controls 48
7. CERTIFICATE AND CRL PROFILE 49
7.1. Certificate Profile 49
7.1.1. Version Number(s) 49
7.1.2. Certificate Extensions 49
7.1.2.1. Key Usage 49
7.1.2.2. Certificate Policies Extension 49
7.1.2.3. Subject Alternative Names 49
7.1.2.4. Basic Constraints 49
7.1.2.5. Extended Key Usage 49
7.1.2.6. CRL Distribution Points 50
7.1.2.7. Authority Key Identifier 50
7.1.2.8. Subject Key Identifier 50
7.1.3. Algorithm Object Identifiers 50
7.1.4. Name Forms 50
7.1.5. Name Constraints 50
7.1.6. Certificate policy Object Identifier 50
7.1.7. Usage of Policy Constraints Extension 50
7.1.8. Policy Qualifiers Syntax and Semantics 50

7.1.9. Processing Semantics for the Critical Certificate Policy Extension 51
7.2. CRL Profile 51
7.2.1. Version Number(s) 51
7.2.2. CRL and CRL Entry Extensions 51
8. SPECIFICATION ADMINISTRATION 52
8.1. Specification Change Procedures 52
8.1.1. Items that Can Change Without Notification 52
8.1.2. Changes requiring Notification 52
8.1.2.1. List of Items 52
8.1.2.2. Notification Mechanism 52
8.1.2.3. Comment Period 52
8.1.2.4. Mechanism to Handle Comments 52
8.2. Publication and Notification Policies 52
8.2.1. Items Not Published in the CPS 52
8.2.2. Distribution of the CPS 53
8.3. CPS Approval Procedures 53
DISCLAIMER 54

1. INTRODUCTION

This document is the Certification Practice Statement (CPS Version 4.4) of NICCA. It states the practices that the NIC Certifying Authority (NICCA) employs in providing certification services as per the Information Technology Act 2000. These include but are not limited to:

- Issuing of Certificates,
- Managing of Certificates,
- Revoking of Certificates, and
- Renewing of Certificates

This CPS is specifically applicable to NIC's Certifying Authority services for the subscribers in Government, PSU & Statutory Bodies, and also to the authorized representatives of Govt. registered companies in India till specified otherwise.

This CPS describes, the:

- Obligations of Certifying Authority, Registration Authorities, Subscribers and Relying parties of this CA.
- Audit and related Security Practice Reviews that users' of the NICCA services shall undertake.
- Methods used to confirm the credentials/identity of Certificate applicants to the NICCA for each class of Certificates offered
- Operational procedures for Certificate lifecycle services undertaken by the NICCA: Certificate application, issuance, acceptance, suspension and revocation.
- Operational procedures for audit logging, records' retention and disaster recovery used for the NICCA.
- Physical, personnel, and logical security practices of the NICCA.
- Key Management and Repository Maintenance for the functioning of the NICCA.
- Certificate and Certificate Revocation List contents of the Certificates issued by the NICCA.
- Administration of the CPS including the methods of amending it.

It is assumed that the reader is generally familiar with Digital Signature Certificate (DSC), Digital Signature, Public Key Infrastructure (PKI) and networking. If not, NICCA advises that the reader obtain some knowledge of the use of public key cryptography and public key infrastructure as implemented in the NICCA. General information and relevant documents of the same are accessible from the URL - **https://nicca.nic.in**

The structure of this CPS generally corresponds to the 'Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework', known as RFC 2527 of the Internet Engineering Task Force, an Internet standards body. In this document, NICCA has conformed to the RFC 2527 structure wherever possible, though there may be some variations in details and headings in order to meet the requirements of the NICCA, which is specific to the requirements of the Government domain.

1.1. Policy Overview

1.1.1. Certificates Classes

The NICCA is offering certification services of the class-1, class-2 & class-3. Each level or class of Certificate provides certain functionality and security features, and corresponds to a specific level of trust. The Digital Signature Certificates (DSCs) issued by the NICCA are published in the NICCA's Repository. The various classes of Certificates are mentioned as follows:-

Class-1 Certificate	**OID 2.16.356.100.1.4.3.1**
Category	Issued to the Individual from Govt., PSU/Statutory Bodies, Government Registered Companies and Web Servers/Servers.
Suggested Usage	Signing certificate primarily be used for signing personal emails and encryption certificate is to be used for encrypting digital emails and SSL certificate is used to establish secure communications through the use of secure socket layer (SSL).
Assurance Level	Provides minimum level of assurance. Subscriber's identity is proved only with help of Distinguished Name - DN and hence provides limited assurance of the identity.
Verification Process	Simply Checks for the certainty of the details given in the DSC Request Form as authenticated by Head of Office. For SSL Certificates, appropriate Domain Registry shall be queried for verification of details.
Class-2 Certificate	**OID 2.16.356.100.1.4.3.2**
Category	Issued to the Individual from Govt., PSU/Statutory Bodies, Government Registered Companies and Web Servers/Servers.
Suggested Usage	In addition to the 'suggested usage' mentioned in class I, the class II Signing certificate may also be used for digital signing, code signing, authentication for VPN Client, web form signing, smart card logon, user authentication, single sign-on and signing involved in e-procurement/e-governance applications. In addition to the 'suggested usage' mentioned in class I, the class II Encryption certificate may also be used for encryption involved in e-procurement/e-governance applications. SSL certificate is used to establish secure communications through the use of secure socket layer (SSL).
Assurance Level	Provides higher level of assurance confirming the details submitted in the DSC Request Form, including photograph and

	documentary proof in respect of at least one of the identification details.
Verification Process	Checks for the certainty of the details given in the DSC Request Form as authenticated by Head of Applicant's Organisation, which is further forwarded by State Informatics Officer (SIO)/ NIC-Coordinator to NICCA. Applicant's Organisation utilizes various procedures to obtain evidence in respect of identity of the applicants by way of documentary evidence of one of the items under point no 9 (Identification details), resulting in stronger assurance level. For SSL Certificates, appropriate Domain Registry shall be queried for verification of details.
Class-3 Certificate	**OID 2.16.356.100.1.4.3.3**
Category	Issued to individuals from Government entities/Head of the Institutions, Statutory/Autonomous bodies, Government registered Companies
Suggested Usage	In addition to the 'suggested usage' mentioned in class-1 and class-2, the class-3 Signing Certificate may also be used for digital signing for discharging his/her duties as per official designation. Class-3 Encryption Certificate may also be used for encryption requirement as per his/her official capacity.
Assurance Level	Provides highest level of assurances, as verification process is very stringent.
Verification Process	In addition to the verification process required for the class II certificates, the subscribers of Class III certificates are required to be personally present with some proof of identity at NICCA/RA, for issuance of DSC. For SSL Certificates, Domain Registration Certificate shall also be required.

1.1.2. Types of Certificates

1.1.2.1. Signing Certificate

The signing certificate is corresponding to the signing private key. The signing key pair is used to digitally sign the messages. The key pair is generated in a secure medium in Crypto device in the presence of the subscriber and is inherent to keep his private key in safe custody. To authenticate the precision of his public key, the subscriber encloses a copy of this certificate with all the messages he sends with his signature. The recipient uses the public key in the enclosed certificate to verify the signature of the subscriber.

1.1.2.2. Encryption Certificate

The private key of the subscriber is used for decrypting the message, which was encrypted using public keys of Encryption Certificate holder. A separate key pair shall be used for the purpose of Encryption.

- There should be a Policy/Procedure in place, approved by the Subscriber's Head of the Organisation, which describes the complete process for Encryption Key Pair Generation, Backup Procedure for Encryption key pair, safe-keeping of Backups and associated Key Recovery Procedures. The Subscriber shall submit a formal declaration in prescribed format, signed by the Subscriber's Head of the Office.

- Encryption Certificate shall be made available for importing to Crypto devices (Smart Card/USB token). Once imported to the Crypto device, the Subscriber should delete the file containing the Encryption private key from the System.

- Subscriber shall be required to sign an additional declaration form, which mentions, inter alias, that he/she shall be responsible for compliance to the relevant sections of the IT Act/Indian Telegraphic Act and other Acts/laws of the Indian legal system, pertaining to Encryption/Decryption, and he/she shall be liable for associated penal actions, for any breaches thereof.

- Key Escrow/Key Archival of Encryption keys shall not be done by NICCA.

1.1.2.3. Mandatory Declaration by Subscriber for Encryption Certificate

- I am solely responsible for the usage of the Certificates/Tokens/ Technology. I shall not hold NICCA responsible for any data loss/damage, arising from the usage of the same.

- I am aware that Key Escrow/Key Archiving of Encryption keys is not done by NICCA and I shall not hold NICCA responsible or approach NICCA for recovery of my private Encryption Key, in case of its loss or otherwise.

- I shall be responsible for compliance to the relevant sections of the IT Act/Indian Telegraphic Act and other Acts/laws of the Indian legal system, pertaining to Encryption/Decryption of any message or document or electronic data, and I shall be liable for associated penal actions, for any breaches thereof.

- NICCA shall not be held responsible and no legal proceedings shall be taken against NICCA for any loss and damage that may occur due to any reason whatsoever including technology upgradation, malfunctioning or partial functioning of the software, USB token, Smart Card or any other system component.

- I am aware that the Encryption Certificate, issued by NICCA is valid only for the suggested usage and for the period mentioned in the certificate. I undertake not to use the Certificate for any other purpose.

- I am conversant with PKI technology, and understand the underlying risks and obligations involved in usage of the Encryption Certificate.

1.1.2.4. Web Server Certificate

A web server certificate enables users to authenticate the server and establish a secure connection. The web server certificate also contains a public key, which is used in creating a secure connection between the client and server. The applicant has to submit certificate request in PKCS#10 format to NICCA for issuing web server certificate.

1.1.2.5. Client Certificate

Client certificates are electronic documents that contain information about clients. These certificates, like server certificates, contain not only this information but also public encryption keys that form part of the SSL security feature. The public keys, or encryption

codes, from the server and the client certificates facilitate encryption and decryption of transmitted data over an open network, such as the Internet. The typical client certificate contains several items of information: the identity of the user, the identity of the certification authority, a public key that is used for establishing secure communications, and validation information, such as an expiration date and serial number.

1.1.2.6. Object Signing Certificate

Object Signing helps users develop confidence in downloaded code. It allows users to identify the signer, to determine if someone other than the signer has modified objects. Object Signing uses standard techniques of public-key cryptography to let users get reliable information about code they download in much the same way they can get reliable information about shrink-wrapped software. Signed objects can be Java applets, JavaScripts, plugins, Active X controls or any other kind of code

1.1.2.7. IP Sec Tunnel

The IP Sec Tunnel works with VPN device to create a secure connection, called a tunnel, between your computer and a private network. It uses Internet Key Exchange (IKE) and IP Security (IPSec) tunneling protocols to establish and manage the secure connection.

1.1.2.8. IP Sec User

IP Sec user digital certificates are used to setup communication between two peers using IKE protocol in VPN. This removes the need to manually exchange public keys with each peer or to manually specify a shared key at each peer.

1.1.2.9. OCSP Responder

This Certificate may be used to check the authenticity of OCSP Client i.e. to check whether OCSP client is authorized to send a OCSP request/query to the OCSP Responder. Hence in cases where the OCSP Responder Server requires that the client should send signed request to the OCSP Responder, this type of certificate may be issued to the clients.

1.1.2.10. OCSP Signing

The OCSP Signing Certificate is issued to OCSP Responder Server, which provides online status of the Certificate to the OSCP compliant client/application. By using OCSP Responder Certificate, the OCSP Clients can trust the status of Certificate in question. The OCSP Signing Certificate must be issued directly to the Responder by the cognizant CA. By doing so, Certificate's Issuer (CA) explicitly delegates authorization to OCSP Responder/OCSP Signing Authority to provide the online certificate status. The OCSP Signer’s Certificate Certificate contains a unique value for extendedKeyUsage.

1.1.2.11. Time Stamping

This certificate may be used for time stamping data to prove the existence of data at particular point of time.

1.1.2.12. Smart card Logon

This certificate may be used for logon to the system.

1.2. Applicability

The community governed by this CPS is primarily the Government sector. However, this CPS accommodates a large and widely distributed community of users within the Government, PSUs, Statutory Bodies, and Govt. Registered Companies in India.

1.3. Certifying Authority

The NIC Certifying Authority (hereafter called as NICCA) is responsible for the issuance and maintenance of Certificates for subscribers in the Government, PSUs, Statutory Bodies, and Govt. Registered Companies in India.

1.3a Sub-CA

Sub-CAs are allowed to be created for different organizations and agencies, for ease of operations and management. However, Sub-CAs shall be created purely in a technical context, to be part of the NICCA's technical infrastructure. The keys created for Sub-CA shall be located only on NICCA's technical infrastructure. Agencies for whom the Sub-CAs are created, have to be reflected in the corresponding certificate as ''NICCA – Sub-CA for <name of agency for whom Sub-CA has been set up>''. The public key of the Sub-CA key pair shall be certified by NICCA's key, which is in turn certified by CCA. The certificate issuing authority for the Sub-CA shall remain only with NICCA.

1.4. Registration Authorities

At present NICCA functions through State/District office of NIC. Although verification of credentials of the applicants are carried out by the head of respective organizations/departments.

The NICCA may also function through Registration Authorities (RAs) in each organization interested in having Digital Certificates issued to its employees. The head of office of the organization or any person authorized by the organization may function as the RA. These RAs have complete charge of the authentication and validation of each Subscriber within the organization.

1.5. End-Entities

The Subscribers or users of the Digital Certificates issued by the NICCA are officials within the Government domain, Govt. nominated Agencies/Institutions domain and authorized representative of registered companies.

1.6. Applications

Digital Signature Certificates issued by NICCA may be used as per 'suggested usage' defined in various classes of the certificates and the key usage mentioned in the certificate.

1.7. Contact Details

The organisation administering this CPS is the 'NIC Certifying Authority' of the National Informatics Centre. Inquiries about the CPS or otherwise to the NIC Certifying Authority shall be addressed to:

Chief Operations Manager
NIC-Certifying Authority
National Informatics Centre
A-Block, CGO Complex, Lodi Road
New Delhi – 110003, INDIA.
E-mail: **support@camail.nic.in**
Tel No: +91-11-24366176, + 91-1600118585 (IVR)

2. GENERAL PROVISIONS

2.1. Obligations

2.1.1. CA Obligations

2.1.1.1. Compliance

The NICCA will publish or make publicly available the CPS describing the practices employed in issuing the Digital Certificates. The CA operates in accordance with this CPS, and the Information Technology ACT 2000 and it's subsequent amendments, if any.

2.1.1.2. Certificate Requests

- The NICCA accepts Certificate requests from entities according to the agreed procedures contained in this CPS.
- The NICCA authenticates entities requesting a Certificate, with the help of the RA setup at the concerned Government organization and with the help of the NIC Coordinator of that organization.(Detailed procedure given in the Digital Signature Certificate Request Form available at https://nicca.nic.in/repository/ dscrequest.pdf)
- The NICCA issues Certificates based on the requests from authenticated entities.
- The Certificates issued by NICCA are published in NICCA Repository and made available to the public. These Certificates are also submitted to CCA for publishing in the National Repository.

Terms of Issuance

When a Certificate references this CPS, the following conditions apply and all relying parties that reasonably and in good faith rely on the information contained in the Certificate during its operational period shall accept the following:

a. The NICCA complies with the requirements of this CPS and its applicable Certificate policies when authenticating the Subscriber and issuing the Certificate.
b. Information provided by the Subscriber in the application for Certificate issuance, for inclusion in the Certificate, is accurately transcribed to the Certificate.
c. The NICCA takes reasonable steps to verify information in the Certificate, unless otherwise noted in this CPS. There will be no misrepresentations of fact in the Certificate known to the NICCA.
d. The NICCA checks for the completeness of the application form filled, and issues the digital Certificate, which is valid subject to the applicability of revocation rules, mentioned in this CPS.

e. The digital Certificate is published in an accessible Directory server. The NICCA will comply with procedures laid down for publishing the Certificates in the National Repository maintained by the office of the CCA.
f. The Digital Certificate revoked/suspended are updated in the CRL in the time frame mentioned in the CPS (clause 2.1.5). This CRL is published in the NICCA's repository as well as communicated to the National Repository maintained by the office of the CCA.

2.1.1.3. Validity of Certificates

Certificates issued will normally be valid for a maximum period of two years from the date of issue, but may vary from case to case at the discretion of NICCA.

2.1.2. Obligations of the NIC Coordinator at the requesting organisation

2.1.2.1. Compliance

The NIC Coordinator operates in accordance with this CPS.

The NIC Coordinator interacting with a concerned organization that is requesting Certificates for its employee(s) is responsible for the sections 2.1.2.2 and 2.1.2.3.

2.1.2.2. Authentication of the RA's credentials

The NIC Coordinator/NICCA authenticates the identity of the Registration Authority Administrator (RAA), who is responsible for authenticating the end-user to be certified, using procedures specified in Section 3.1.

2.1.2.3. Maintain Certificate Application Information

The NICCA RA maintains DSC Application Forms and Supporting evidence for any Certificate request made to the NICCA, in accordance with this CPS.

2.1.3. Subscriber Obligations

The Subscriber should have the knowledge of the INFORMATION BOOKLET issued by the CCA, which contains IT Act 2000, IT Rules 2000 and IT Regulations 2001 (**http://nicca.nic.in/repository/itact2000.pdf**).

The Subscriber is obliged for the following:

2.1.3.1. Accuracy of Representations in Certificate Applications

Subscribers MUST accurately represent the information required of them in the application for a Certificate request.

2.1.3.2. Key Pair Generation

Subscribers will generate their key pair using a trustworthy method. Such a system consists of computer hardware, software and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are

reasonably suited to performing their intended functions and enforce the applicable security policy.

2.1.3.3. Protection of the Entity's Private Key

Subscribers MUST properly protect their private key at all times against loss, disclosure to any other party, modification and unauthorized use, in accordance with this CPS. Since the time of creation of their private and public key pair, Subscribers are personally and solely responsible for the confidentiality and integrity of their private keys. Every usage of the private key is assumed to be the act of its owner.

2.1.3.4. Notification of CA upon Private Key Compromise

Upon suspicion that their private keys have been compromised Subscribers MUST notify the NICCA by sending a certificate revocation request immediately (as specified in 3.4.2), using the prescribed form, in accordance with the regulation 6 of IT regulations 2001.

2.1.3.5. Notification of CA upon any change in their Certificate Content

Upon any change in the information content of their Certificates (such as name, address etc), Subscribers MUST notify the NICCA using the prescribed form. It is then, at the sole discretion of the NICCA, whether to issue a new Certificate or not. If a new Certificate reflecting the changes is to be issued, the Subscriber shall have to submit a request for revocation of the existing Certificate and also submit a request for a new Certificate.

2.1.3.6. Restrictions on Private Key and Certificate use

Subscribers MUST use the keys and Certificates only for the purposes authorized by the NICCA, as given in Section 1.2.

2.1.3.7. Personal Data

Subscribers are responsible for the usage and conservation of their personal data at all times.

2.1.3.8. E-mail ID

A Subscriber requesting for a Certificate should have a functional and valid official e-mail address. E-mail addresses issued/generated from mail servers in Govt. domain are preferred.

2.1.3.9. Enrollment

For the issuance of a certificate by the NICCA, the Subscriber is required to fill the DSC Request form and submit to NICCA.

Duly filled forms are signed by the Head of Office of the same organization after verifying the applicant details as per the ‘verification process’ mentioned ‘Policy Overview-1.1’. The Head

of Office of the department is responsible for the authenticity of the officer requesting for the Certificate.

The **Head of the Office** keeps one copy of the DSC application for record.

Class-1 Certificate: HO sends the second copy of the DSC application to NICCA for further processing.

Class-2 & Class-3 Certificate: HO sends the other copy to the NIC Coordinator/SIO/DIO, who in turn verifies the applicant details as per the 'verification process' mentioned 'Policy Overview-1.1' and countersigns the application before sending it to the NICCA for further processing.

NICCA creates a new subscriber account with user-id & password and posts the same to the NIC Coordinator/SIO/DIO in a sealed envelope along with a photocopy of the application form.

2.1.3.10. Submission of Public Key

The public key can only be submitted to NICCA by accessing the NICCA Web site (**http://nicca.nic.in**) and logging into the user account of the subscriber. The user has the option to either create the key pair using NICCA Software or by own Software. Submission of Public key to NICCA is automatic if NICCA Software is used. In case user generates key pair by own software, he has to submit the public key in PKCS#10 format to NICCA. This can be done by cut/paste method on the space provided in the user account menu of NICCA site**.**

2.1.3.11. Protection of Private Key

The private key remains in the safe custody of the Subscriber himself. The Subscriber is fully responsible for safeguarding his private key and the pass phrase, which protects the private key.

2.1.3.12. Private Key Usage

No Stipulation.

2.1.3.13. Duplicate Certificate Requests

No Stipulation

2.1.3.14. Accept Certificate of NICCA

The Subscriber must accept the NICCA Certificate needed to facilitate Certificate path construction of the Subscriber's Certificate.

2.1.3.15. Use of Certificate

The Subscriber should use the Certificate exclusively for authorized and legal purposes, consistent with this CPS and only for the purpose mentioned in the Certificate.

2.1.3.16. Certificate Acceptance

The subscriber may accept the Digital Signature Certificate issued by NICCA after verifying the contents of the Certificate.

2.1.4. Relying Party Obligations

A relying party may rely on a Certificate that references this CPS only if the Certificate is used and relied upon for usage in applications mentioned in 1.6 and under circumstances where the following occur:

a. The relying party should have knowledge of the INFORMATION BOOKLET issued by the CCA, which contains IT Act 2000, IT Rules 2000 and IT Regulations 2001 (**http://nicca.nic.in/repository/itact2000.pdf**).
b. The reliance is reasonable and in good faith in light of all the circumstances known to the relying party at the time of the reliance.
c. The Certificate is used exclusively for purposes mentioned in the Certificate.
d. The purpose for which the Certificate is used is appropriate under this CPS.
e. The Certificate is being used within its operational period.
f. The relying party checked the status of the Certificate by using the CRL published in the repositories prior to reliance, or a check of the Certificate's status would have indicated that the Certificate was valid.

2.1.5. Repository Obligations

The NICCA maintains a repository of certificates it issues and a Certification Revocation List (CRL) for the Certificates it revoked/suspended. The NICCA publishes an issued public certificates/CRL in the NICCA repository and sends the same to the CCA's National Repository as per prescribed method.

The NICCA will immediately update CRL after suspension/revocation of a DSC.

The publication of the CRL is scheduled, at least once in every week.

The NICCA will immediately update and publish CRL after Suspension/Revocation of DSCs.

2.1.6. RA Personnel Obligations

a. Take necessary approval from the NICCA through NIC Coordinator to function as RA Administrator for NICCA for the concerned office.
b. Verify the authenticity of the subscriber requesting the Certificate for issuance or revocation and forward the same to the designated NIC Coordinator.
c. Verify the information provided by the subscriber and make sure that the DN (Distinguished Name) is unique.\
d. Request for revocation or suspension of a Certificate for any reason such as transfer, suspension, long leave, change of duties, superannuation and death.

e. Maintain records of requests for application, revocation, suspension of Certificates.

2.2. Liability

2.2.1. Disclaimer

The NIC is not liable for any loss:

a. Of NICCA services due to war, natural disasters, acts of terrorism or other uncontrollable forces.
b. Incurred between the times a Certificate Revocation request is received and the stipulated period of revocation as per Section 3.4.2 .
c. Due to unauthorized use of Certificates issued by the NICCA, and use of Certificates beyond that prescribed.
d. Caused by fraudulent or negligent use of Certificates or Certificate revocation lists issued by the NICCA.
e. Due to disclosure of information contained within Certificates and revocation lists.
f. Of indirect, consequential or punitive damages arising from or in connection with its services.

The NICCA has no liability for indirect, special, incidental or consequential damages, or for any loss of data/information or other indirect, consequential or punitive damages arising from or in connection with its services. Except as expressly provided in this CPS, the NICCA disclaims all other warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of information provided.

2.2.2. Loss Limitations

The NIC disclaims any liability that may arise from the use of the Digital Certificate(s) issued by NICCA.

2.3. Financial Responsibility

2.3.1. Indemnification of Certificate Authority by Relying Parties and Subscribers

The NICCA will not be responsible for loss due to failure of the Subscribers and relying parties to fulfill their obligations under this CPS. In particular, the NICCA will not be responsible for loss due to the compromise of the Subscriber's private key and for loss due to the inaccuracy of information provided by the Subscriber.

2.3.2. Fiduciary Relationships between various Entities

Issuance of Certificates in accordance with this CPS does not make any fiduciary relationship between the NICCA and a Subscriber and a relying party.

2.3.3. Administrative Processes

No stipulation

2.4. Interpretation and Enforcement

2.4.1. Governing Laws

The Information Technology Act, 2000, Information Technology (Certifying Authorities) Rules, 2000 and Information Technology (Certifying Authority) Regulations, 2001 or any subsequent updates shall govern the validity of this CPS, the construction of its terms, and the interpretation and enforcement of the rights and duties of the parties hereto.

2.4.2. Severability of Provisions

If any provision of this CPS, or the application thereof, shall for any reason and to any extent, be invalid or unenforceable, the remainder of this CPS and application of such provision to other persons or circumstances shall not be affected thereby and shall be interpreted so as best to reasonably effect the intent of the parties. IT IS EXPRESSLY UNDERSTOOD THAT EACH AND EVERY PROVISION OF THIS CPS THAT PROVIDES FOR ANY LIMITATION, DISCLAIMER OR EXCLUSION OF LIABILITY, WARRANTIES, OR DAMAGES IS INTENDED BY THE PARTIES TO BE SEVERABLE AND INDEPENDENT OF ANY OTHER PROVISION AND TO BE ENFORCED AS SUCH.

Notice

Whenever a Subscriber or User desires to give any notice, demand, or request to the NICCA with respect to this CPS, such a communication shall either be in writing and shall be effective only if it is delivered by a courier service that confirms delivery in writing or is mailed, through certified or registered mail, postage prepaid, return receipt requested, addressed to '*Chief Operations Manager, NIC-Certifying Authority, National Informatics Centre, A Block, CGO Complex, New Delhi – 110 003, INDIA'* or by a signed mail to **support@camail.nic.in**, that could carry online forms as an attachment.

2.4.3. Dispute Resolution Procedures

The Controller of Certifying Authorities resolves any conflict of interests between the Certifying Authorities and the subscribers, as per the IT Act, Central Govt. Rules and Directives.

2.5. Fees

2.5.1. Certificate Issuance Fees

The Certificate Fee Structure is published on the NICCA website (url http://nicca.nic.in) under the link <Support>. The Fee Structure is subject to revision and any such change shall be published on the NICCA website immediately.

2.5.2. Certificate Access Fees

No fees.

2.5.3. Revocation or Status information Access Fees

No fees.

2.5.4. Fees for other services such as Policy Information

No fees.

2.5.5. Refund Policy

Not Applicable.

2.6. Publication and Repository

2.6.1. Publication of CA Information

The NICCA Certificate, CRL, Certificate Practice Statement and DSC Repository are publicly available at the NICCA website (url http://nicca.nic.in) under the <Repository> tab.

2.6.2. Frequency of publication

CRL publication is in accordance with this CPS (2.1.5).
CPS publication is in accordance with this CPS.

2.6.3. Access Controls

There is no access control on reading and downloading the CPS.
There is no access control on reading the Certificates from the repository.
The Certificates and the CPS in the electronic Repository are protected against any unauthorized modification.

2.6.4. Repositories

The NICCA maintains an electronic Repository, which complies with this CPS. The Repository allows access to the NICCA Digital Signature Certificate related and CRL information. The updation of the Repository is periodic, in compliance with this CPS.

2.7. Compliance Audit

The NICCA will be audited for compliance with the Information Technology Act, Rules, Regulations and Guidelines.

2.7.1. Frequency of Entity Compliance Audit

The NICCA shall get its operations audited as per Rule 31 of the Notification No. GSR 789(E), dated 17/10/2000, under the IT Act.

2.7.2. Identity/Qualifications of Auditor

The compliance audits shall be carried out by one of the empanelled Auditors duly authorized by the CCA.

2.7.3. Topics covered by Audit

The NICCA shall be audited on the following:

- Security policy and planning
- Physical security
- Technology evaluation
- NICCA's services administration
- NICCA CPS.
- Compliance to NICCA's CPS
- Contracts/agreements
- Requirements under the IT Act, Rules, Regulations and Guidelines.

2.7.4. Auditors Relationship with NICCA

The auditor shall be independent of NICCA and shall not be software or hardware vendor or any service provider of NICCA. They shall not have any current or planned financial, legal or any other relationship, other than that of an auditor and the audited party. The auditor should be one of the empanelled auditors duly authorized by the CCA.

2.7.5. Actions taken as a Result of Deficiency

The NICCA shall take immediate and appropriate actions determined by the significant exceptions and deficiencies identified during the compliance audit, in order to rectify such deficiencies.

2.7.6. Communication of Results

A copy of the results of the compliance audit shall be submitted to the CCA's office, as required by Rule 31 of the Information Technology (Certifying Authorities) Rules, 2000.

2.8. Confidentiality

The NICCA collects personal information about the Subscribers (e.g. full name, organization, and e-mail address). These data are processed in a way that ensures privacy protection.

2.8.1. Types of Information to be kept Confidential

All Subscribers' information that is not present in the Certificate issued by the NICCA is considered confidential and SHALL not be released outside without explicit Subscriber's authorization.

Also contingency plans, Audit reports, Disaster recovery plans, security measures and details about the trusted personnel are kept confidential.

2.8.2. Types of Information not considered Confidential

Information included in public Certificates issued by the NICCA and the CRLs published by the NICCA are not considered confidential. Information contained in the CPS is also not confidential. Without limiting the foregoing, information that (i) was or becomes known through no fault of the NICCA (ii) was rightfully known or becomes rightfully known to the NICCA without confidential or proprietary restriction from a source other than the Subscriber, (iii) is independently developed by the NICCA, or (iv) is approved by a Subscriber for disclosure, shall not be considered confidential.

2.8.3. Disclosure of Certificate Revocation/Suspension Information

When a Certificate is revoked/suspended, a reason code MAY be included in the CRL entry for the action. This reason code is not considered confidential and may be shared with all other users and relying parties. However, no other details concerning the revocation are normally disclosed. In the event of suspension/revocation of a Digital Signature Certificate issued by the NICCA, a serial number will be included in the CRL entry for such a revoked Digital Signature Certificate.

2.8.4. Release to Law Enforcement Officials

The NICCA does not disclose confidential information to any third party, except when required by law enforcement officials that exhibit regular warrant.

2.8.5. Information that can be revealed as part of civil discovery

Same as above

2.8.6. Disclosure upon Owner's Request

The NICCA may release information if authorized by the Subscriber in writing.

2.8.7. Other information Release Circumstances

No stipulation.

2.9. Intellectual Property Rights

The NICCA retains all right, title, and interest (including all intellectual property rights), in, to and under all NICCA Digital Signature Certificates, except for any information that is

supplied by an Applicant or a Subscriber and that is included in an NICCA Digital Signature Certificate, which information shall remain the property of the Applicant or Subscriber.

The NICCA retains all Intellectual Property Rights in and to this CPS. A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such a Certificate Applicant. Key pairs corresponding to Subscribers' Digital Signature Certificates are their property regardless of the physical medium within which they are stored and protected, and such Subscriber retain all Intellectual Property Rights in and to these key pairs.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Initial Registration

An applicant has to fill the 'DSC Request Form' (available on the NICCA web site https://nicca.nic.in) for issue of a Digital Signature Certificate from NICCA. The detail filled by the applicant has to be verified from the available records and authenticated by the Head of Office of the Organization/Department/Ministry.

3.1.1. Types of Names

The NICCA uses X.501 Distinguished Name (DN) format, which serves as a unique identifier of the entity.

The naming attributes of the Subscriber to be requested in the Certificate used to identify and authenticate the requester depend on the type of Certificate that the Subscriber requires. The choice of the types and format of names used in the fields of the Certificate shall conform to RFC 2459.

The following naming attributes may be used in entities 'Distinguished Names' for certificates.

3.1.1.1. Country

Necessity: Mandatory.
Comments: This is the 2-digit country code of residence of the Subscriber. For the NICCA, this naming attribute for all Subscribers is 'IN'.

3.1.1.2. Name (Common Name)

Necessity: Mandatory.
Comments: For certificates, this is the first name followed optionally by initials, followed by surname. For Organisation Certificates, this is the Name of the Head of Organisation.

3.1.1.3. Organization

Necessity: Mandatory.
Comments: For certificates, this is the official name of the Institution employing the Subscriber. For Organisation Certificates, this is the name of the respective Organisation.

3.1.1.4. Organizational Unit

Necessity: Mandatory.
Comments: For certificates, this is the official name of the organisational unit or department in which the Subscriber works. For Organisation Certificates, this is the name of the Organisation Unit.

3.1.1.5. E-Mail

Necessity: Mandatory.
Comments: For certificates, this is the functional and valid official e-mail address of the subscriber.

3.1.1.6. State

Necessity: Mandatory.
Comments: For certificates, this is the State of residence of the subscriber.

3.1.1.7. Locality

Necessity: Mandatory.
Comments: For certificates this is the locality of residence of the Subscriber.

3.1.2. Need for Names to be Meaningful

All names must be meaningful using commonly understood semantics to determine the identity of the Subscriber. The Common Name DN attribute contains the legal name as presented in Government issued photo-identification for all classes of Certificates issued. Each NICCA issued Digital Certificate is with a unique DN attribute for each Subscriber.

3.1.3. Rules for interpreting Various Name Forms

Taking all components (including the Subscriber's Name and e-mail id) of the name together, the Subscriber Name shall be unambiguous and unique. However, this CPS does not require that a specific component or element of a name be unique or unambiguous by itself.

3.1.4. Name Claim Dispute Resolution Procedure

The decisions of the NICCA or any NIC personnel on its behalf, in matters concerning name disputes are discretionary, final, and not subject to appeal.

3.1.5. Method to prove Possession of Private Key

Since the DSC request is submitted in PKCS#10 format only, NICCA can verify the possession of corresponding private key by the applicant by verifying the digitally signed certificate request, which is an inherent part of PKCS#10 request.

3.1.6. Authentication of Organization Identity

No Stipulation.

3.1.7. Authentication of Individual Identity

The procedure of initial authentication of individual identity complies with the classes of Certificates as mentioned in 'Policy Overview-1.1'

3.2. Routine Re-key

Re-key facility is currently not available.

3.3. New Certificate after Revocation

Where the information contained in a Certificate has changed, or there is a known or suspected compromise of the private key, the Subscriber has to request for a fresh certificate (DSC) in the same manner as for initial registration.

A new Certificate is given in place of the revoked Certificate after necessary identification and authentication of the Subscriber.

A public key whose Certificate has been revoked for private key compromise will not be re-certified.

Request for new certificate after revocation of a Certificate is logged.

3.4. Revocation/Suspension Request

3.4.1. Suspension Request

The Subscriber, the RA of the subscriber's organisation, respective NIC Coordinator or NICCA can request for suspension of a Subscriber's Certificate by the following way:

1. signed e-mail
2. over phone
3. web request by a subscriber
4. post/registered post

The requirement for suspension of DSC may arise due to the reasons as stated in the CPS (clause No. 4.4.1). The respective NIC Coordinator can send a request for suspension/hold of a Subscriber's Certificate over phone or in written form by post/registered post. Alternatively if the NICCA has sufficient and authenticated knowledge that the key of the subscriber is compromised, the NICCA shall request a suspension of Digital Signature Certificate. The NICCA can hold the Certificate under suspension for a maximum period of 15 days.

It may be noted the facility for suspension of DSC over phone has been provided to the requester to meet emergency situations and address security concerns. NICCA will however verify the authenticity of the requester to the extent possible before initiating suspension.

The suspended certificate will be revoked/re-instated after proper verification/inquiry within the stipulated period of 15 days.

3.4.2. Revocation Request

The Subscriber, the RA of the subscriber's organisation, respective NIC Coordinator or NICCA can request for revocation of a Subscriber's Certificate by the following way:

1. signed e-mail
2. submission of dully filled revocation form
3. web request for revocation
4. NICCA decides to revoke

Revocation requests are authenticated either by procedures described in this CPS or by verifying the Digital Signature of the revocation request. NICCA will suspend the DSC of the subscriber after preliminary verification of all requests for revocation of DSC within 72 hrs of receipt of the request. The actual revocation of DSC will be carried out after authentication of the revocation request within a maximum period of 15 days.

Request for revocation/suspension of a Certificate is logged.

A notification stating suspension/revocation of the Subscriber's Certificates is sent to the Subscriber by a mail digitally signed by the trusted role of NICCA.

4. OPERATIONAL REQUIREMENTS

The NIC has established a process for requesting and receiving a Certificate to ensure that Certificates are issued only to properly authenticate the applicants. Once a Certificate is delivered and accepted, the NICCA operations manage the processes of suspending, revoking, or renewing Certificates as required. The NICCA records and monitors security related activities to ensure the integrity of the certification process.

4.1. Certificate Application

A Certificate applicant must complete a Certificate application in the prescribed format. For obtaining a Certificate from the NICCA, the application form has to be filled by the Applicant. The applicant is required to send only one copy to NICCA. However the applicant is advised to retain a copy of the same which shall be required while filling up of Online information for key pair generation. The form is available from the NICCA upon request, as well as electronically in the NICCA website. This form should be signed by the Head of office of the same organisation and forwarded by the SIO/NIC Coordinator. The Head of the office of the organisation is responsible for the authenticity of the officer requesting for the Certificate.

The NICCA accepts all application forms, reviews each, and approves or rejects the applications. The act of completing the application process includes the Subscriber's consent for the NICCA to issue the Certificate.

The applicants applying for a Certificate should complete the following general procedures for each Certificate application:

- Submit duly filled application form to the NICCA as stated in 2.1.3.9.
- Generate a Key pair using a Trustworthy System, as in section 2.1.3.2.
- Take reasonable precautions to protect the private key from compromise, as in section 2.1.3.3.
- Submit the public key to the NICCA.

4.2. Certificate Issuance

Upon successful completion of the Subscriber's identification and authentication process as per this CPS, and the complete and final approval of the Certificate application, the NICCA issues the requested Certificate, and makes the Certificate available to him. At the discretion of the NICCA, the NICCA may refuse to issue a Certificate to any application without incurring any liability or responsibility for any loss or for any expenses arising as a result of the refusal.

4.3. Certificate Acceptance

On receipt of a Digital Signature Certificate, the Subscriber is responsible for checking that the Certificate is not damaged or corrupted. In the event that the Certificate is damaged or corrupted, the Subscriber will contact the NICCA before accepting the Digital Signature Certificate.

If the subscriber is satisfied with the Digital Signature Certificate issued by the NICCA, the subscriber accepts the Certificate and then downloads the same onto his local machine.

In the event of any actual or suspected loss, disclosure or other Compromise of the Subscriber's Private Key the Subscriber will request that the Certificate be revoked and recreated. Any revocation will be done in accordance with this CPS.

4.4. Certificate Suspension and Revocation

The NICCA revokes a Certificate, if the Subscriber, or the corresponding RA of his organisation, or the NIC Coordinator requests Certificate revocation.

4.4.1. Circumstances for Revocation

A Certificate may be revoked by the NICCA, at its absolute discretion, on receipt of revocation request:

1. The associated private key is known to be compromised or misused.
2. The associated private key is suspected to be compromised or misused.
3. The Subscriber's information in the Certificate has changed.
4. The Subscriber is known to have violated his obligations.
5. The authorized requester requested the Certificate revocation.
6. The Subscriber has permanently left the organisation (retired, resigned, taken VRS, died while in service).
7. The Subscriber has been transferred to another department.

4.4.2. Who can Request Revocation?

The following entities can request the revocation of a Certificate:

1. The subscriber.
2. The NICCA.
3. The RA of the organization of the Subscriber.
4. The respective NIC Coordinator.

4.4.3. Procedure for Revocation Request

In case where the NICCA can independently confirm that the Certificate has been compromised or misused, the NICCA will revoke the Certificate, even if the request to do so comes from an unauthenticated source and/or the holder of the Certificate is unreachable.

NICCA initiates revocation procedure for a Digital Signature Certificate issued by it, if it is of opinion that

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;
(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;
(c) the NICCA's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(d) Subscriber has been declared dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

In all other cases the NICCA will authenticate the revocation request and try to contact the Subscriber before revoking the Certificate. If the Subscriber is temporarily unreachable, the Certificate will be suspended till actual authentication of the revocation request. If the subscriber could not be reached, the certificate is revoked at the end of 15 days.

A Subscriber may submit a Certificate revocation request to the NICCA directly by letter mail, signed e-mail, or in person.

Where the revocation request is made directly to the NICCA, it will upon receipt of the request put a "hold" upon the Certificate, which effectively suspends the validity of the Certificate. The NICCA will revoke the Certificate and thereby terminate its validity permanently, upon receipt of final confirmation of revocation directly from the Subscriber. Such final confirmation of revocation can be initiated by the NICCA, if it receives:

- an e-mail digitally signed by the Subscriber's private key
- a fax of an original letter signed by the Subscriber in the prescribed format with proper identification and authorization where the original letter is then forwarded to the NICCA by letter mail
- an original letter signed by the Subscriber.
- a Request through the Certificate Revocation Form signed by the Subscriber. The ‘Request for Certificate Revocation Form’ can be obtained from the NICCA upon request or electronically from the NICCA Repository.
- no response from the Subscriber comes within 15 days.

The NICCA will endeavor to issue a Notice of Revocation to the Subscriber within one week following the receipt of the request for revocation and/or of the final confirmation of revocation.

The certificate can be suspended i.e. put on hold either by a request from the subscriber himself or by NICCA. The latter can put the certificate “on hold” in case it suspects some misuse or is informed of some malicious intentions with respect to usage of the certificate in question.

In case NICCA receives a request for activation from the subscriber, either online or through the prescribed Form DOC-ID NIC-CA/FRM/CRT.117, then NICCA shall carefully verify the details from the records and the certificate holder, and activate or revoke the certificate, as the case may be.

In case NICCA has initiated the suspension process, all efforts shall be made to verify the information regarding the subscriber, to the maximum extent possible. The certificate shall then be activated or revoked, depending on the findings and other circumstantial evidence on the matter.

A Subscriber can submit a final confirmation of revocation as set out above, without first making any other request for revocation. Receipt of such final confirmation will terminate the validity of the Certificate permanently.

Suspended or revoked Certificates, shall be included in the Certificate Revocation List. Where the Subscriber has requested revocation, the reason code used in the List identifying the reason for the Certificate revocation may indicate an “unspecified” reason for revocation, as Subscribers need not have or give any particular reason to request revocation. However, in case of Certificate suspension, the reason code is “Certificate Hold”. Any further details for keeping certificate on hold may be mentioned in the space for “comments” . A Certificate that is resumed from a "hold" status shall not be included in the succeeding Certificate Revocation Lists.

Certificate Revocation List Update

a) As mentioned in section 3.4.1 & 3.4.2, upon receipt of suspension/revocation request, NICCA will suspend the DSC **within 72 hours** after preliminary verification. Thereafter, updated CRL will also be published immediately i.e. **within 72 hours** of receipt of suspension/revocation request.

b) The suspended certificate will be revoked/re-instated within a maximum period of 15 days after proper verification/enquiry by NICCA as mentioned in section 3.4.1 & 3.4.2. Once the suspended certificate is revoked/re-instated, the CRL would be updated and published immediately i.e. within a maximum period of 15 days of the actual receipt of request for suspension/revocation of certificate.

c) Subscribers must not use a Certificate in a transaction on becoming aware of any ground upon which the NICCA could revoke it under the terms of the CPS and must not use it in a transaction after the Subscriber has made a revocation request or been notified of the intention of the NICCA to suspend or revoke the Certificate. The NICCA shall be under no liability to Subscribers in respect of any such transactions if, despite the foregoing, they do use the Certificate in a transaction.

d) Further, upon becoming aware of any ground upon which the NICCA could revoke the Certificate, or upon making a revocation request or upon being notified by the NICCA of its intention to revoke the Certificate, Subscribers must immediately notify Relying Parties in any transaction that remains to be completed at the time, that the Certificate used in that transaction is liable to be revoked (either by the NICCA or at the Subscriber's request) and state in clear terms that, as this is the case, the Relying Parties should not rely upon the Certificate in respect of the transaction. The NICCA shall be under no liability in respect of such transactions to Subscribers who fail to notify Relying Parties, and under no liability to Relying Parties who receive such a notification from Subscribers but who complete the transaction despite such notification.

e) The NICCA shall be under no liability to Relying Parties in respect of the period between NICCA’s decision to suspend or revoke a Certificate (either in response to a request or otherwise) and the appearance of this information on the Certificate Revocation List. Any such liability is limited as set out elsewhere in this CPS.

Effect of Revocation

Revocation terminates the validity of a Certificate from the time that the NICCA completes the revocation action and posts it to the Certificate Revocation List.

4.4.3.1. NICCA Certificate Revocation

If the revoked Certificate is the NICCA Certificate, NICCA informs the Subscribers that it will terminate the Certificate and CRLs distribution service for all Certificates/CRLs issued using the compromised private key.

4.4.4. Revocation Request Grace Period

The NICCA responds within three days (excluding weekends and public holidays) to revocation requests. It however handles revocation requests with priority as soon as the request is recognized as such.

4.4.5. Circumstances for Suspension

The NICCA will suspend a Certificate only while there is uncertainty over its current status:

1. At the request of the Subscriber or the head of office of the Subscriber's organisation (RA) or the NIC Coordinator of the organisation.
2. If a revocation request for the Certificate is on hold pending contact with the Subscriber.
3. It is the opinion that the Digital Signature Certificate should be suspended in the public interest.

4.4.6. Who can Request Suspension?

A Certificate suspension can be requested either by the Subscriber or the head of office of the Subscriber's organisation, or by the NIC Coordinator of that organisation or the NICCA.

4.4.7. Procedure for Suspension Request

Suspension requests are accepted only by

- an e-mail digitally signed by the Subscriber's private key
- a fax of an original letter signed by the Subscriber with proper identification and authorization where the original letter is then forwarded to the NICCA by letter mail
- an original letter signed by the Subscriber.
- Telephone call.
- NICCA S/W (logs on to **https://nicca.nic.in/**)

4.4.8. Limits on Suspension Period

The Suspension period will be for a maximum period of 15 days.

4.4.9. CRL Issuance Frequency

The NICCA will immediately update CRL after suspension/revocation of a DSC.

4.4.10. CRL Checking Requirements

The checking of CRLs is the responsibility of the Certificate Relying party. Relying parties' update their local copies of CRLs from the CRLs posted in the NICCA/NRDC Repository from time to time.

4.4.11. On-line Revocation/Status Checking Availability

As of now, NICCA does not support this facility.

4.4.12. On-line Revocation Checking Requirements

Same as procedures laid down for revocation in section 4.4.10 and 4.4.11 of this CPS.

4.4.13. Other forms of Revocation Advertisements available

The Subscriber is notified of the revocation of his Certificate by signed e-mail.

4.4.14. Checking Requirements for other forms of Revocation Advertisements

No Stipulation

4.4.15. Special requirements Re-key compromise

No stipulation

4.5. Security Audit Procedures

4.5.1. Types of Events Recorded

Significant security events in the NICCA system are manually or automatically recorded to protect audit trail files. These events include, but are not limited to, the following examples:

- Suspicious network activity
- Repeated failed access attempts
- Events related to equipment and software installation, modification, and configuration of the NICCA operations
- Privileged accesses to all NICCA components

The following types of events are recorded by the NICCA:

1. System startup and shutdown.
2. CA's application startup and shutdown.
3. Login and logouts to the NICCA Servers.
4. Attempts to create, remove, set passwords or change the system privileges of the NICCA trusted roles.
5. Changes to Digital Signature Certificate creation policies.
6. Unauthorized attempts at network access to the NICCA's systems.

7. Unauthorized attempts to access to system files.
8. Creation and revocation of the NICCA Digital Signature Certificates.
9. Attempts to initialize remove, enable, and disable subscribers.
10. Errors
11. End user key pair generation, certificate generation, suspension, revocation and activation.

4.5.2. Frequency of Processing Log

The audit log files are analyzed at least once every two-month. Adequate backup of audit logs are processed on a monthly basis to provide audit trails of actions, transactions and processes of the NICCA.

4.5.3. Retention Period for Audit Log

Audit logs are retained as archive records. The audit logs should be retained on the NICCA system for at least 12 months and subsequently moved to the NICCA archive for retention for a minimum period of seven years.

4.5.4. Protection of Audit Log

Only authorized NICCA personnel are allowed to view and process audit log files.

4.5.5. Audit Log Backup Procedures

A backup of the audit logs on physical removable media is performed as per the backup policy of NICCA. The backup media are saved in safe storage.

4.5.6. Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. A vulnerability assessment is performed, reviewed and revised, if necessary, following an examination of these monitored events.

4.6. Records Archival

4.6.1. Types of Event Recorded

The following type of events are archived:

1. Certificate requests and related messages exchanged between the Subscriber and the NICCA.
2. Certificates issued by the NICCA.
3. Unsuccessful attempt for Certificate issuance and revocation.
4. Revocation requests and related messages exchanged by the NICCA with the requester and/or the Subscriber.
5. CRLs issued by the NICCA as per this CPS.

4.6.2. Retention Period for Archive

Digital Signature Certificates stored by the NICCA and issued CRLs will be archived for at least seven years after key expiration. Audit information detailed in section 4.5.1, Subscriber agreements, RA agreements and Relying Parties agreements will also be retained for a period of two years.

4.6.3. Protection of Archive

The archive media is protected through storage in a restricted-access facility to which only the NICCA trusted roles have access.

4.6.4. Archive Backup Procedures

Archive files are backed up as they are created. All information pertaining to the NICCA's operation, Subscriber's application, verification, identification, authentication, Subscriber agreement, RA agreement, Relying Parties agreements are archived.

4.6.5. Requirements for Time-Stamping of Records

Certificates, CRLs, other revocation databases and usage entries contain time and date information provided by System time, which is synchronized with IST through NPL.

4.6.6. Archive Collection System (Internal or External)

The archive collection system is internal to the NICCA.

4.6.7. Procedures to obtain and Verify Archive Information

Only NICCA trusted roles are permitted to access the archived data. Electronically archived data is protected against unauthorized viewing, modification, deletion, or other tampering through the implementation of appropriate physical and logical access controls.

4.7. Key Changeover

The NICCA will notify a Subscriber one month before his/her key is to expire, so that the user can request for a fresh DSC.

4.8. Compromise and Disaster Recovery

4.8.1. Computing Resources, Software, and/or Data are corrupted

In the case where the NICCA computing resource, software and/or data have been corrupted, the responsible personnel will immediately start the recovery procedures:

1. Backup public Repository and services systems are started when needed.
2. The cause of the corruption is diagnosed.
3. The corrupted parts of the system are repaired or replaced.
4. The corrupted data are replaced from backups if possible.

5. When the extent of the corruption cannot be exactly specified, the entire system should be rebuilt.
6. The system is restarted and the users are notified.

4.8.2. Entity Public Key is revoked

4.8.2.1. Subscriber's Public Key

As in the sections 3.3 and 3.4 of the NICCA's CPS.

4.8.2.2. CA Public Key

1. The key is revoked.
2. The CRL is updated and published.
3. The NICCA system is brought down.
4. New CA key pair is generated as indicated in Section 6.1
5. Users are notified.

4.8.3. Entity Key is compromised

4.8.3.1. Subscriber's Key is compromised

Whenever the Subscriber's key is compromised, the Subscriber is obliged to notify the NICCA as soon as possible. The revocation procedure is in accordance with the Section 3.3 and Section 3.4 of this CPS.

4.8.3.2. CA Key is compromised

In case that the NICCA private key is compromised, the following actions shall be undertaken:

1. The CCA is informed about the key compromise.
2. All certificates issued by NICCA will be revoked and new CRL will be published.
3. The key is revoked.
4. The NICCA system is brought down.
5. The cause of the compromise is analyzed to minimize the risk in future.
6. New CA key pair is generated as indicated in Section 6.1.
7. The public key of the NICCA's new key pair is sent to the CCA for certification.
8. Users are notified about the revocation and asked to request for re-key.

4.8.4. Secure Facility after a Natural or other type of Disaster

Presently NICCA does not have any Disaster Recovery (DR) site, but plans are being made to have one soon. However, in the case of a natural or other type of disaster, the NICCA will start the recovery as soon as possible using stored backups.

4.9. CA Termination

The NICCA can decide to cease its services. In that case the following steps shall be undertaken:

Notify the CCA of its intention to cease acting as a CA at least ninety days before it ceases to act as a Certifying Authority or ninety days before the date of expiry of license.

NICCA shall advertise the intention of NICCA's cessation in a manner approved by the CCA, sixty days before the expiry of the license or ceasing to act as Certifying Authority.

1. The notice shall be sent to the CCA and affected Subscribers by digitally signed e-mail sixty days before the expiry of the license or ceasing to act as Certifying Authority.
2. The NICCA will inform all Subscribers, and Relying parties with which the NICCA has agreements or other form of established relations about the decision.
3. The NICCA shall make a reasonable effort to ensure that discontinuation of certification services causes minimal disruption to Subscribers and relying parties needing to verify the Digital Signatures by reference to the public keys contained in outstanding Digital Signature Certificates.
4. Any Certificates issued after the announcement of the termination date shall have the expiration date not exceeding the termination date.
5. On the termination date, all the Certificates issued by NICCA shall be revoked. NICCA shall also generate a final CRL and make it available through NICCA web site with the next update past the termination date of NICCA. The NICCA Certificate status shall also be displayed on NICCA web site.
6. NICCA has made necessary arrangements for preserving the records for a period of seven years, as stipulated in the IT Act 2000.
7. No compensation shall be given to subscribers.
8. NICCA shall destroy the certificate signing private key after the date of expiry mentioned in the license and confirm the date and time of destruction of the private key to the CCA.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY

This component describes non-technical security controls such as physical, procedural and personnel controls used by the NICCA. These controls are intended to perform securely the functions of key generation, Subscriber authentication, Certificate issuance, Certificate revocation, audit and archival.

These controls must function as intended to avoid the generation of Certificates or CRLs with erroneous information or compromise of the NICCA private key.

5.1. Physical Security Control

5.1.1. Site Location and Construction

The NICCA main facility is located in New Delhi. All NICCA operations are carried out in a physically secured environment.

Disaster recovery site is not presently available and is proposed for the future.

5.1.2. Physical Access

The NICCA has implemented necessary physical security controls to restrict access to the NICCA Hardware and Software. The controls are applied to the NICCA servers, workstations and other devices used for performing the CA operations. The control includes physical and electronic locks to prevent penetration. The access to the NICCA facility is limited to the trusted roles only. The trusted roles gain access to the NICCA facility by means of Trusted Role Identification Card. The physical access is logged manually as well as electronically.

5.1.3. Power and Air conditioning

The NICCA servers, workstations and devices are powered by Uninterruptible Power Supply (UPS).

The necessary ambience control measures (air conditioning, ventilation etc.) are used to facilitate the continuous operation of the NICCA servers and workstations.

5.1.4. Water Exposures

The NICCA has taken reasonable precautions to minimize the impact of water exposure to NICCA facilities.

5.1.5. Fire Prevention and Protection

The NICCA has taken reasonable precautions to prevent and extinguish fires. The facilities provided for fire prevention and protection measures have been designed to comply with the fire safety regulations of respective civic bodies.

5.1.6. Media Storage

The software distribution media for production software, backup media, archive media are stored securely.

5.1.7. Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to store data backups, audit trails, software backups and sensitive information are rendered unreadable before disposal.

5.1.8. Off-Site Backup

Presently not available, it is proposed for future.

5.2. Procedural Controls

5.2.1. Trusted Roles

Trusted Roles are those people who have an access to the NICCA and perform various functions of the NICCA. If their work is carried out improperly, either maliciously or accidentally, it may introduce security problems in the NICCA facilities such as issuance, use, suspension, or revocation of an NICCA Digital Signature Certificate.

Trusted Roles include all employees of the NICCA. These trusted roles are collectively known as trusted personnel. As these trusted personnel have access to the NICCA facilities, they may affect the:

- Validation of the information given in the Certificate Request and Revocation Request.
- Acceptance of the Certificate Request and the Issuance of the Certificate.
- Validation of the Certificate content.
- Suspension and Revocation of the Certificate.
- Maintenance of Repositories and data archives.
- Functioning of H.S.M.

The trusted personnel include but are not limited to the following:

- System Administration personnel including the Network Administrators, Repository Administrators, NICCA Server Administrators, System Administrators.
- Officials designated to approve Certificate request including CA Administrator, RA Administrator, CA Officer, RA Officer.
- Officials designated to manage the infrastructure including Chief Infrastructure Maintenance Officer.
- NICCA Management Officials including Chief Information Security Officer, Chief Applications Manager, Chief Operations Manager, Internal Auditor.

5.2.2. Number of Persons Required Per Task

In order to safeguard the security of the NICCA server, the responsibilities for various operations of the NICCA server are delegated to the NICCA trusted personnel. This ensures the accountability of the trusted personnel for the role they are performing.

For the following tasks, a minimum of two trusted personnel is required:

- Validation of content in the Certificate request, Renewal request, Revocation request and approval.
- Decision to suspend and revoke the Certificate by the NICCA.

5.2.3. Identification and Authentication for Each Role

NICCA shall subject individuals to an identification process before assigning trusted roles. The identification include their personal presence before Trusted Personnel of the NICCA performing security functions and by authentication using well recognized forms of Government issued identification such as official identity card. The Trusted roles are also made to sign a Non-disclosure Agreement for maintaining secrecy of information. The Trusted Personnel are provided with necessary authentication mechanisms for gaining logical access to the NICCA systems. A User-ID and Password is provided to gain access to the CA Application system, for the purpose of verification and signing of subscribers details. Trusted roles are given class-III certificates, issued in crypto smart cards, for their respective roles of RA & CA. The same is also verified by the application, before giving access to the systems. The access controls have also been setup to perform the required functions by the NICCA official, performing the role of system security officer.

5.3. Personnel Controls

5.3.1. Background, Qualifications, Experience, and Clearance Requirements

The NICCA designates a person in a trusted role only after the person seeking to become a trusted person presents the necessary proof for background, qualification and experience. Trusted Personnel within the NICCA require different qualifications and experience that commensurate with tasks performed by the role.

A person is cleared after the background check requirements listed in 5.3.2. are completed.

5.3.2. Background Check Procedures

The background check requirement for Government officials and contractors, consultants are different.

For Government officials the following checks are carried out:

- The employees of NIC and Government Ministries to be designated as trusted personnel are already cleared of the background check requirements for Government service. An undertaking from the officials that their background checks are performed and proof of the same from the head of the respective office is required.

- Their experience and qualification and whether it is in consistence with the NICCA requirements of different roles is verified.

For Non-Government personnel the following mechanism is used:

- The employer of the person shall provide necessary undertaking for the trustworthiness, qualification and experience of the person seeking to become a trusted person in a specific role in accordance with requirements of the NICCA for the specific trusted role.
- The methods used by the employer to carry out the background checks.

5.3.3. Training Requirements

The NICCA will arrange necessary training programs for its employees to perform their job responsibilities competently and satisfactorily. The training programs include:

- Aspects of Security Policy framed by the NICCA.
- Technical training relevant to the responsibility.
- Data handling techniques.

5.3.4. Retraining Frequency and Requirements

No stipulation

5.3.5. Job Rotation Frequency and Sequence

No job rotation considered presently and proposed to be considered in future.

5.3.6. Sanctions for Unauthorized Actions

If unauthorized actions are performed or attempted by the trusted personnel, the NICCA will initiate disciplinary actions in accordance with Government rules.

5.3.7. Contracting Personnel Requirements

NICCA may hire contract personnel from NICSI for application verification, Crypto device personalization and other secretarial work.

5.3.8. Documentation Supplied to Personnel

All personnel involved in the operations of the NICCA are provided with technical documentation needed to discharge their duties in a consistent, competent and satisfactory manner. In addition, documentation defining the duties and responsibilities defined by the NICCA Management for the respective Trusted Roles are also provided.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

The subscriber's key pair shall be generated by the subscriber or at RA office in the presence of the subscriber.

6.1.2. Private Key Delivery to Entity

Normally a subscriber generates his own key pair as explained in section 2.1.3.10 and submits the public key in PKCS#10 format to NICCA. However, private keys of end users are delivered in person, if Digital Signature Certificate (DSC) is issued on Crypto device (PKCS#11).

6.1.3. Public Key Delivery to Certificate Issuer

The NICCA accepts Certificate requests in PKCS#10 request format.(See RFC 2314).

The preferred transport method for certification requests is SSL protected HTTP.

6.1.4. CA Public Key Delivery to Users

The NICCA public keys are published on the NICCA Certificate Repository and the NICCA web site. Additionally, the same is also available on the CCA Certificate Repository and the CCA web site.

6.1.5. Key Sizes

The NICCA uses RSA public key algorithm.

The NICCA private key is 2048 bits in size.

All other private keys are of at least 1024 bit key size.

6.1.6. Public Key Parameters Generation

Public key parameters are generated by the relevant applications.

6.1.7. Parameter Quality Checking

No Stipulation.

6.1.8. Hardware/Software Key Generation

Key pair for the NICCA is generated by using a hardware security module conforming to FIPS 140-1 level 4 standards. The Subscriber keys may be generated in

hardware/software. However Class 3 certificates shall be generated in hardware (Crypto smart card/USB token) only.

The Subscriber keys may be generated in software.

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

The X.509 v3 Key Usage and Enhanced Key Usage fields are set according to the requirements stated in section 7 of this CPS.

6.2. Private Key Protection

6.2.1. Standards for Cryptographic Module

A hardware module conforming to FIPS 140-1 level 4 standards is used for generation of NICCA keys.

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

The NICCA uses 2 out of 4 private key control.

6.2.3. Private Key Escrow

The NICCA private keys are presently not escrowed.

6.2.4. Private Key Backup

The Backed up keys are stored in the same manner on hardware Security Module HSM 140-1 Level 4 and additionally on non-rewritable CD, in the form of password protected unintelligible key blob, with the same physical protection as that of the primary NICCA key.

6.2.5. Private Key Archival

The NICCA private keys are encrypted and archived on media. The whole process, including the storage of media is done securely.

6.2.6. Private Key entry into Cryptographic Module

The NICCA private key is generated using FIPS 140-1 level 4 hardware security modules.

6.2.7. Method of Activating Private Key

The NICCA private key is accessed by multiple controls.

6.2.8. Method of Deactivating Private Key

Cryptographic modules that have been activated are never left unattended. They are deactivated after use.

6.2.9. Method of Destroying Private Key

The NICCA private keys are archived. After the retention period of seven years the archive media may be destroyed.

Private keys on magnetic media (such as floppy disks, Crypto device) are destroyed by overwriting the key files. Private keys on CD-ROMs are destroyed by physically damaging the media and rendering the data unreadable.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Public keys may be restored from backup.

6.3.2. Usage periods for the Public and Private Keys

The validity period of a NICCA issued Certificate ends upon its expiration or revocation. The usage period of the key pairs is the same as the usage period for the NICCA Digital Signature Certificate.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

Activation data is generated and used in accordance with section 6.2.2 of this CPS.

6.4.2. Activation Data Protection

The NICCA pass phrase is known to trusted NICCA personnel only. The pass phrase must be used only in secure physical environment.

6.4.3. Other Aspects of Activation Data

No stipulation

6.5. Computer Security Control

6.5.1. Specific Computer Security Technical Requirements

The NICCA computer system satisfies the following requirements:

1. The NICCA is run on dedicated computer systems.
2. Only the software needed to perform the NICCA tasks is installed on the system.
3. Access to the operating system and the NICCA software is allowed only to the authorized NICCA trusted personnel.
4. Physical access to the system is allowed only to the authorized NICCA trusted personnel.

5. All security related events are audited in the NICCA system.

These computer security technical requirements are in accordance with specific computer security requirements of the Information Technology Security Guidelines given at Schedule 2 and 3 of the Information Technology (Certifying Authority) Rules, 2000.

6.5.2. Computer Security Rating

No stipulation

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

The development of the software shall be carried out in a controlled secure environment.

Production and development environment are totally separated.

6.6.2. Security Management Controls

The logs, the configuration files and the entire file systems of the NICCA computer systems are regularly checked.

6.6.3. Life Cycle Security Ratings

No Stipulation

6.7. Network Security Controls

These are implemented in conformance with the security policy of NICCA. It includes detailing on Network Communications Security, Firewall, Anti-Virus protection with associated System integrity and other security measures.

6.8. Cryptographic Module Engineering Controls

The Hardware Security Module provides cryptographic functions.

7. CERTIFICATE AND CRL PROFILE

7.1. Certificate Profile

This section defines Certificate Profile and Certificate content requirements for Certificates issued under this CPS.

The NICCA Certificates issued under this CPS conform to the following:

- X-509 Version 3 digital Certificate
- X-509 Version 2 CRL
- RFC 2459 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999"

7.1.1. Version Number(s)

All NICCA end entities Certificates are X-509 Version 3 Certificates.

7.1.2. Certificate Extensions

The NICCA currently does not use private extensions in the issued Certificates.

7.1.2.1. Key Usage

The Key Usage extension field is not set critical in end entity Certificates.

7.1.2.2. Certificate Policies Extension

The Certificate Policies Extension field is set in end entity Certificates.

7.1.2.3. Subject Alternative Names

The NICCA uses RFC822 Names as Subject Alternative Names in end entity Certificates and it is not set critical.

7.1.2.4. Basic Constraints

The Basic Constraints Extension field is set in end entity Certificates.

7.1.2.5. Extended Key Usage

The Extended Key Usage Extension field is set in end entity Certificates.

7.1.2.6. CRL Distribution Points

End entity Subscriber Certificates use the CRL Distribution Points extension containing the URL of the location where a Relying Party can obtain a CRL to check the Certificate status. The criticality field of this extension is set to FALSE. Presently, the NICCA uses a single CRL distribution point, but the NICCA may add additional CRL distribution points as and when it is required/necessitates.

7.1.2.7. Authority Key Identifier

Certificates issued under this CPS are populated with the Authority Key Identifier extension. The Authority Key Identifier is composed of the 160-bit SHA-1 hash of the public key of the NICCA issuing the Certificate. The criticality field of this extension is set to FALSE.

7.1.2.8. Subject Key Identifier

All end entity Certificates are populated with a Subject Key Identifier extension, and the Key Identifier based on the public key of the Subject of the Certificate is generated. Where this extension is used, the criticality field of this extension is set to FALSE. It is not set currently.

7.1.3. Algorithm Object Identifiers

The NICCA X.509 Version 3 Certificates are signed with SHA1RSA in accordance with RFC 2459.

7.1.4. Name Forms

No stipulation

7.1.5. Name Constraints

No stipulation

7.1.6. Certificate policy Object Identifier

The Object Identifiers (OID) allotted for different classes of certificates, will be the part end entity certificate under this CPS.

7.1.7. Usage of Policy Constraints Extension

No stipulation

7.1.8. Policy Qualifiers Syntax and Semantics

No stipulation

7.1.9. Processing Semantics for the Critical Certificate Policy Extension

No stipulation

7.2. CRL Profile

7.2.1. Version Number(s)

The NICCA currently issues X.509 Version 2 CRLs.

7.2.2. CRL and CRL Entry Extensions

No stipulation.

8. SPECIFICATION ADMINISTRATION

8.1. Specification Change Procedures

All changes in this NICCA CPS shall be brought to the notice of the CCA before being published on the NICCA Repository. The NICCA Management shall make amendments to this CPS and the new CPS will be available at **https://nicca.nic.in/**. Updates supersede any designated or conflicting provisions of the referenced version of the CPS. The most recent version of the NICCA CPS shall supersede all previous versions and impose a legal obligation on Subscribers and the NICCA. Any changes in CPS shall not contravene any provision of the act, rule and regulation made there under.

8.1.1. Items that Can Change Without Notification

No items can be changed without notification to the CCA.

8.1.2. Changes requiring Notification

8.1.2.1. List of Items

The NICCA notifies the customers the changes in this CPS, if the changes, according to the NICCA judgment may have significant impact on the users of Certificates and revocation lists issued by the NICCA under this CPS.

8.1.2.2. Notification Mechanism

The updated CPS with amendments is posted at the site **https://nicca.nic.in/** after taking approval from CCA.

8.1.2.3. Comment Period

No Stipulation

8.1.2.4. Mechanism to Handle Comments

No Stipulation

8.2. Publication and Notification Policies

8.2.1. Items Not Published in the CPS

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

8.2.2. Distribution of the CPS

This CPS is published in electronic form at site **https://nicca.nic.in/.**

8.3. CPS Approval Procedures

The draft CPS is presented before the NICCA Policy approval committee appointed by the NICCA Management. The Policy approval committee approves the CPS and amendments after necessary examination. This will be forwarded for the CCA's approval before being published in the Repository.

DISCLAIMER

NICCA is not responsible for any data loss/damage arising from the use of these Certificates/Tokens/Technology. The user is solely responsible for the same.

Encrypting/decrypting/storing/sharing/transmitting of any message or document or electronic data should be in conformity with the Indian Telegraphic Act, IT Act and all other relevant parts of the Indian legal system and will be the sole responsibility of the user and the relying parties. NICCA shall not be held responsible and no legal proceedings shall be taken against NICCA for any loss and damage that may occur due to any reason whatsoever including technology up gradation, malfunctioning or partial functioning of the software, Crypto device or any other system component.

Digital Certificates issued by NICCA are valid only for the suggested usage and for the period mentioned in the certificate. These Certificates shall not be valid for any other purpose.

The NICCA reserves the right to suspend or revoke Certificates issued by it, in accordance with the Sections 37 & 38 of the IT Act. Before revocation, Subscriber shall be given due opportunity of being heard in the matter.

It is assumed that the Users are conversant with PKI technology, and the underlying risks and obligations before applying and using Digital Signature Certificate, issued by NICCA.

It is the responsibility of the recipient of a Digital Signature to identify the level of identity assurance provided by the Certificate and to decide if it should be relied upon. Even if the Signature is valid, it is the responsibility of the recipient to decide if the action that will result from accepting the Signature warrants additional precautions and NICCA will not be held responsible for any consequences thereof arising from such action.

The CPS is subject to renewal from time to time. Subscribers with valid Digital Signature Certificates are automatically and legally bound by such changes made to the CPS at any time during the functioning of NICCA.