Certification Practice Statement (CPS)

for

Digital Signature Certification Services

(Version 6.0, Dated 11th October 2013)

OID : 2.16.356.100.2

Certifying Authority

National Informatics Centre

Department of Electronics and Information Technology (DeitY)

Ministry of Communications & Information Technology

Government of India

Document Details:

Name: Certification Practice Statement (CPS)

Doc ID: 1

Classification: **General**

Revision History:

VER	DATE	AUTHOR	REVIEWED BY	REASON FOR CHANGE
0.1	Dec 2001	Ratnaboli G Dinda C S Rao	Committee	Initial draft
1.0	14-01-02	Ratnaboli G Dinda C S Rao	Committee	Reworking
1.1	17-01-02	Ratnaboli G Dinda C S Rao	Committee	To incorporate changes after installation of HSM
1.2	August 2002	Ratnaboli G Dinda C S Rao	Committee	ICICI Infotech CA S/w License expiration
2.0	10-01-03	Manoj Kulshreshth SumeetJethra	Committee	New Software Next update due on 30th April 2003
2.0	6-02-03	P K Saha, Manoj K Kulshreshth	Committee	Changes made as per comments received from CCA
2.0	22-04-03	P K Saha, Anupama Mandal, Manoj K Kulshreshth	Committee	Changes made after Auditors Comment. Next update due on 30th June 2003
2.1	20-03-04	S K Roy Manoj Kulshreshth	Committee	Extending validity of certificates for two years, mandatory requirement for DN
3.0	30-03-05	S K Roy Manoj Kulshreshth	Committee	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	Committee	Issuance of DSCs to Government Registered Private Companies, Encryption Certificates, inclusion of more types of certificates
4.1	16.02.06	Manoj KulshreshthNagendra Kumar	Committee	Issuance of DSC on crypto device

4.2	16.03.07	S K Roy P K Saha Anupama Mandal Manoj Kulshreshth S Khan	Committee	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 AnuradhaValsa Raj S Khan	Committee	Inclusion of Individual from Govt., PSU/Statutory Bodies, Government Registered Companies in the eligibility criteria for encryption certificates
4.4	01.06.09	P K Saha Anupama Mandal Manoj Kulshreshth AnuradhaValsa Raj	Committee	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.
6.0	Feb 2013 and Oct 2013	Manoj K Kulshreshth Anuradha Valsa Raj Shamsuddin Khan	Committee	Pre and Post External Audit 2011, interfacing with Interoperability Guidelines V2.4 from CCA, defining authentication and verification process by RA to ensure the existence of domain name for SSL Certificate for enrolling CA/NICCA certificate in Mozilla Browser, provision for test certificates. Inclusion of Class-0 certificates for test purpose, DSC Request Forms, Physical Verification Centres, DSC applicant's eligibility, inclusion of contractual employees, Certification Classes and their verification process and OID, Types of Certificates, Responsibilities of HO, Guidelines for RA, CA Termination Policy, Key Size, SHA2, Certificate Profile, Sub-CAetc, DSC Forms, post audit with limited scope held in 30 Sep and 7 Oct 2013

Table of Contents

1 DEFINITIONS AND ACRONYMS

S. No	Term	Description
1.	CCA	Controller of Certifying Authority
2.	NICCA	National Informatics Centre Certifying Authority
3.	Sub-CA	Subordinate Certifying Authority
4.	NICRA	NIC Registration Authorities opened up by NIC
5.	ORA	Organisational Registration Authorities opened up by an organisation
6.	CPS	Certificate Practice Statement
7.	DSC	Digital Signature Certificate
8.	CRL	Certificate Revocation List
9.	CRL DP	CRL Distribution Point
10.	PAC	Physical Appearance Centre
11.	CISO	Chief Information Security Officer
12.	CAA	Certifying Authority Administrator
13.	RAA	Registration Authority Administrator
14.	Sub-CAA	Sub Certifying Authority Administrator
15.	NC	NIC Coordinator
16.	DIO	District Informatics Officer
17.	DIA	District Informatics Associate
18.	OID	Object Identifier
19.	HO	Head of the Office
20.	RA	Registration Authority

2 INTRODUCTION

This document is the Certification Practice Statement (CPS) of NICCA, a Certifying Authority licensed under IT Act 2000 by CCA. 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 describes, the:

- Obligations of Certifying Authority, Registration Authorities, Subscribers and Relying parties of this CA.
- Audit and related Security Practice Reviews that users' of NICCA services shall undertake.
- Methods used to confirm the credentials/identity of Certificate applicants to NICCA for each class of Certificates offered
- Operational procedures for Certificate lifecycle services undertaken by NICCA: Certificate application, issuance, acceptance, suspension and revocation.
- Operational procedures for audit logging, records' retention and disaster recovery used for NICCA.
- Physical, personnel, and logical security practices of NICCA.
- Key Management and Repository Maintenance for the functioning of NICCA.
- Certificate and Certificate Revocation List contents of the Certificates issued by 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 NICCA. General information and relevant documents of the same are accessible from the URL - **https://nicca.nic.in; http://cca.gov.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 NICCA, which is specific to the requirements of the Government domain.

2.1 PRECEDENCE

CISO/COM, NICCA override these instructions if there are any conflicts

2.2 FUTURE CHANGES

The CPS shall be updated as and when policy of NICCA modified.

2.3 POLICY OVERVIEW

2.3.1 DSC APPLICANT'S ELIGIBILITY

NICCA issues DSC to serving officials(Only Indian Nationals) in (a) Government sector (posted in India/Outside) (b) Public Sector Undertaking(PSU) (c) statutory bodies (d) autonomous bodies (e) judiciary(f) Member of Parliament (MPs) (g) Member of Legislative Assembly (MLAs) (h) councillors (i) Elected member of Village Panchayat/Gram Sabha (j) Companies of Govt. Sector under section -25 of Company Act (k)temporary deployed/engaged in e-governance projects e.g. consultants etc.

Individuals temporary deployed/engaged in e-governance projects are issued only class-1 and class-2 Digital SignatureCertificates.

2.3.2 ORGANISATIONAL AND FUNCTIONING STRUCTURE

2.3.2.1 Certifying Authority

The NIC Certifying Authority (hereafter called as NICCA) is responsible for the issuance and maintenance of Certificates. As of now NICCA organisation structure is hierarchal starting from Root Certifying Authority of India, NIC Certifying Authority and Sub Certifying Authority.

2.3.2.2 Subordinate Certifying Authority

As of now, two Subordinate Certifying Authorities (Sub-CA), namely NIC Sub-CA and e-passport Sub-CA have been created. These subordinate authorities have been created purely in a technical context, to be part of NICCA's technical infrastructure. The keys created for Sub-CA are located only on NICCA's technical infrastructure. The public key of the Sub-CA key pair are certified by NICCA's key, which is in turn certified by CCA.

2.3.2.3 Registration Authorities

NICCA functions through two kinds of Registration Authorities (RAs) (**a**) opened up by NIC at NIC State/District offices, which are managed by NIC officers who discharge their duty as Registration Authority Administrator (RA) after duly appointed by NICCA. These RAs are termed as NICRA (**b**) opened up by user organisation of Govt./PSU department (e.g. ECIL, BARC etc)

forissuing DSCs to only its employees, which are managed by senior officers of that department after duly appointment as RA by NICCA. These RAs are termed as organisational RA (ORA).

At present there are total twenty nine RAs, out of which five are from other departments. No outsourced agencies are engaged to function as RA and these RAs are functioning as an extension of NICCA**.**

2.3.2.4 Physical Appearance Centre (PAC)

All NIC Centres, State Units/District Centres/Cells at various Ministries, which are located countrywide function as Physical Appearance Centre (PAC), where Class-3 DSC applicant needs to appear in person to complete the physical verification process. The NIC official at State Units/District Centres/Cells discharges his duty as Verification Officer.

2.3.2.5 Head of the office/Department/Secretariat/Panchayat (HO)

Head of the office/department/Secretariat/Panchayat is an official appointed/nominated by the department, who represents the department and is a senior level officer not necessarilybe the reporting officer of the applicant. The term HO is being used to represent head of the corresponding departmentsor nominated person for all type of eligible DSC applicant as stated in 2.3.1 of CPS.If HO himself/herself is an applicant, He/She has to sign both as an applicant as well as HO. The NICCA does not employ any procedure to check the credentials of HO.

2.3.2.6 Employer of Contractual Employee

The entity through which the contractual employees have been hired and are temporary deployed/engaged in e-governance projects by the departments.

2.3.2.7 NIC Coordinator (NC)

NIC Coordinator is NIC official of any level who coordinates with the department whose officials require to be issued Digital Signature Certificates.

2.3.2.8 Types of Certificates

NICCA provides certificates as per "Interoperability Guidelines for Digital Signature Certificate version 2.4 December 2009 updated on 14 June 2011" issued by CCA. The profile for below listed certificates is strictly in accordance with profiles given in the stated guidelines (**http://cca.gov.in**)

2.3.2.9 End User Certificate/Digital Signature Certificate

The Digital Signature Certificate is used for signing digital content. The signer signs the digital content using private key and the recipient uses the public key to verify the signature of the signer.

2.3.2.10 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. The applicant needs to have Digital Signature Certificate from NICCA before issuance of Encryption certificates. These certificates are issued in pkcs#12 formats, which needs to be kept safely and securely on crypto devices and backup is to be maintained by the DSC holder. The applicant needs to ensure following before applying for encryption certificate**

- 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 submits a formal declaration given in DSC Form, 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, after giving the key pair for safekeeping as per organisational procedure/policy.
- Subscriber signs an additional declaration in DSC 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.**

2.3.2.11 SSL/Web Server Certificate

A web server certificate enables users to authenticate the server and establish a secure connection by way of encrypting/decrypting communication between server and client using public key of server. The applicant has to submit certificate request in PKCS#10 formats to NICCA online for issuing web server certificate.

2.3.2.12 Code Signing Certificate

Code signing certificate is used to sign codes like Java applets, Java Scripts, plug-in, Active X controls or any other kind of codes. It allows users to identify the signer (genuineness of the code author), to determine if someone other than the signer has modified objects. **It is issued in the name of organisation or in the individual name.**

2.3.2.13 OCSP Responder

The OCSP Signing Certificate is issued to OCSP Responder/organisation, which provides online status of the Certificate to the OCSP compliant client/application. By using OCSP Responder Certificate, the OCSP Clients can trust the status of the Certificate queried. The CA issues

SigningCertificate to the OCSP Responder, by doing so, Certificate's Issuer (CA) explicitly delegates authorization to OCSP Responder/OCSP Signing Authority to provide the online certificate status. **It is issued in the name of OCSP responder/organisation.**

2.3.2.14 Time Stamping Authority Certificate

This certificate is issued to NIC CA to setup Time Stamping Authority to run time stamping services. Time tamping service is usedfor proving the existence of data at particular point in time by way of signing the digital content of the time stamp requester by Time Stamp Authority.

2.3.2.15 System Certificate

This certificate is issued to computer systems/devices for the purpose of machine to machine authentication. The certificate issued to computer systems/devices contains a unique identification relating to the systems.

2.3.2.16 Certificates classes, OID, ASSURANCE level and verification process

NICCA is offering certification services of the Class-0, Class-1, Class-2 &Class-3. Each level or class of Digital Signature Certificate corresponds to a specific level of trust/assurance. The assurance is defined on the basis of verification process employed in verifying the credentials of DSC applicant before issuing DSC to him/her. The classes of Digital Signature Certificates are in accordance with India PKI CP Ver 1.1 issued by CCA (**http://cca.gov.in**).

2.3.2.17 Certificate Classes and OID

Table 1 – Class, OID, Assurance Level and Completeness of DSC Forms

Sr. No.	Class of Certificate	OID	Assurance Level/Verification Process
1.	Class-0	2.16.356.100.2.	It carries no assurance, as it is created with general distinguished nameto be used ONLY for testing purposes.
2.	Class-1	2.16.356.100.2.	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.
3.	Class-2	2.16.356.100.2.	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.

Sr. No.	Class of Certificate	OID	Assurance Level/Verification Process
4.	Class-3	2.16.356.100.2.	Provides highest level of assurances, as verification process as in addition to the verification process required for the class-2 certificates, the applicantsare required to be personally present at Physical Appearance Centre (PAC) for completion of in-person verification process.

2.3.2.18 Verification Process for DSC issuance

The organisational Registration Authorities (ORA), who issues DSC to its employees only, have complete charge of authentication, validation credentials verification of DSC applicants i.e. their applicant do not require to visit NIC Coordinator for getting DSC form checked for its completeness and for physical appearance for Class-3. The complete verification is carried out by ORA including physical appearance for class-3.

The verification of credentials of DSC applicants to NICRA is carried out by **the head of respective organizations/departments (HO).** Registration Authorities of NICCA **shall rely on the verification carried out by the head of respective organizations/departments (HO) and shall not do verification themselves and thus onus of verification lies with Head of office (HO) of the Applicant.**

The **HO of respective organizations/departments of the applicant**utilizes various procedures to obtain evidence in respect of identity and employment in Government Sector for DSC applicant (regular and contractual persons deployed for e-governance project) by way of documentary evidences as mentioned in DSC Application Form (**https://nicca.nic.in)**. He carries out following steps for verification depending upon type of applicant/type of certificate

For Regular Government Employee

a) attests photocopy departmental/employment photo-id card
b) verifies the credential given in DSC FORM from available service /official records in the office
c) attests applicant's photograph in DSC form
d) for SSL, verifies the existence of URL/Domain Name, IP allocation & physical location of web server as given in the DSC form
e) for System certificate, verifies MAC Address/ Serial No./Unique id of CPU/device as given in the DSC form
f) puts his/her signature & seal on DSC form

For Contractual Employee (Only Class 1 and Class 2 Signing Certificates)

a) gets service verification letter from the companies/ vendors from where contractual employee has been hired and attests the same

b) attests photocopy departmental/employment photo-id card
c) attests applicant's photograph in DSC form
d) puts his/her signature & seal on DSC form

Applicants applying Class-3 certificates have to visit Physical Appearance Centre (PAC) as mentioned at 2.3.2.4 of CPS in-person along with dully filled in DSC FORM, which has been verified by HO. The NIC Verifying Officer takes following steps for in-person physical verification

a) checks departmental photo-id card
b) collects a photograph & self-attested photocopy of departmental-id card of the applicant
c) matches signature & photograph on DSC form with sign & photo available in departmental photo-id card
d) records applicant mobile no., departmental photo-id no., date & time of in-person appearance
e) attests photograph & signature as shown in Annexure-III
f) puts his signature & seal on Annexure-III

The NIC Coordinator, just checks for the completeness (no role in verification process) of DSC Form and ticks **[√]** in the checklist as shown below and forwards the same to NICCA

[ ] All asterisk (*) marked entries are filled
[ ] Payment details filled & DD attached (if required)
[ ] Attested &self signed copy of Departmental photo-Id attached
[ ] Attested &self signed copy of PAN card attached, if any
[ ] Signature of Applicant done
[ ] Verification by Head of Office (HO) with Signature & Official Seal
[ ] In person verification is done for Class-3 applicant as attached **Annexure-III** of DSC Form

He puts his/her signature & seal on DSC form

In addition to the above verification process, theOCSP responder certificates are issued after signing Memorandum of Understanding (MOU) between NICCA and the applicant's organisation.

2.4 APPLICABILITY

The community governed by this CPS is primarily the Government sector. This is a PKI that accommodates a large and widely distributed community of users defined in this CPS within the Government.

2.5 END-ENTITIES

The Subscribers who have been issued Digital Signature Certificates by NICCA.

2.6 APPLICATIONS

Digital Signature Certificates issued by NICCA shall be used as per the key usage field in the certificate.

2.7 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: **casupport@nic.in**
Tel No: +91-11-24366176

3 GENERAL PROVISIONS

3.1 OBLIGATIONS

3.1.1 CA OBLIGATIONS

3.1.1.1 Compliance

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

3.1.1.2 Certificate requests

- NICCA accepts Certificate requests from entities according to the agreed procedures contained in this CPS.
- NICCA authenticates entities requesting a Certificate, with the help of the **HO** of the concerned department as stated in section 2.3.4.2 of CPS also detailed procedure is given in the DSC Request Form available at **https://nicca.nic.in**.
- 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. 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. NICCA takes reasonable steps to check the completeness of filled DSC request Form and matches the information given in DSC Form along with DSC request submitted by the applicant before processing/issuing the DSC. The DSC issued is subject to the applicability of revocation rules, mentioned in this CPS.

d. The Certificate is published in an accessible Directory server. NICCA complies with procedures laid down for publishing the Certificates in the National Repository maintained by the office of the CCA.

e. The Certificate revoked/suspended is updated in the CRL in the time frame mentioned in the CPS (clause 3.1.4). This CRL is published in NICCA's repository as well as communicated to the National Repository maintained by the office of the CCA.

3.1.1.3 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.

3.1.2 SUBSCRIBER OBLIGATIONS

The Subscriber should have the knowledge of IT Act 2000, IT Rules 2000 and IT Regulations 2001 at (**https://nicca.nic.in**) or at (**https://cca.gov.in**).

The Subscriber is obliged for the following:

3.1.2.1 Accuracy of representations in certificate

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

3.1.2.2 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.

3.1.2.3 Protection of 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, since the time of creation of their private and public key pair. The Subscriber is fully responsible for safeguarding his private key and the pass phrase, which protects the private key.

The Subscriber **MUST** exercise reasonable care to retain control of the private key corresponding to the public key listed in the Digital Signature Certificate and MUST take all steps to prevent its disclosure to a person not authorised to affix the digital signature as stated under section 42(1) of IT Act 2000.

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.

Subscriber **MUST generatesigning key pairs** only in FIPS certified crypto devices as mandated by CCA.

3.1.2.4 Notification of CA upon Private Key Compromise

Upon suspicion that their private keys have been compromised Subscribers **MUST** notify NICCA by sending a certificate revocation request immediately (as specified in 5.5), using the prescribed form, in accordance with the section 42(2) of IT Act 2000 and regulation 6 of IT regulations 2001.

3.1.2.5 Notification of CA upon any change in their Certificate Content

Subscriber shall have to submit a request for revocation of the existing Certificate and also a DSC request form for a new DSC.

3.1.2.6 Restrictions on Private Key and Certificate use

Subscribers MUST use the keys and Certificates only for the purposes as indicated in DSC.

3.1.2.7 Personal Data

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

3.1.2.8 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. This email id shall be treated as registered email id for all communication purposes from NICCA.

3.1.2.9 Enrolment

There are two Digital Signature Certificate Request Forms (Form-1 and Form-2) attached at the end of CPS and also available on https://nicca.nic.in. The Form-1 is to be used for requesting signing/encryption/SSL/System/Code Signing and Form-2 is to be used to request OCSP responder.

The applicant is required to fill the DSC Request Form and submit to NICCA.

The HO of the organisation verifies the credentials of the DSC applicant as stated in 2.3.4.2 of CPS.

Class-3 applicant appears at PAC for competition of in-person verification. The NIC verifying officer does in-person verification as stated in 2.3.4.2 of CPS.

NIC Coordinator checks the completeness of the form as stated in 2.3.4.2 of CPS

NICCA/RA createsa subscriber account with user-id & password, which is communicated to the DSC applicant through email as given in DSC form.

NICCA/RA sends blank Crypto Devices to the DSC applicant or hands them over to NIC-Coordinator.

3.1.2.10 Submission of Public Key

The public key can only be submitted to NICCA only by accessing NICCA Web site (**https://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 inthe user account menu of NICCA site**.**

3.1.2.11 Protection of Private Key

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

3.1.2.12 Private Key Usage

No Stipulation.

3.1.2.13 Duplicate Certificate Requests

No Stipulation

3.1.2.14 Accept Root Certificate of CA

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

3.1.2.15 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.

3.1.2.16 Certificate Acceptance

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

3.1.3 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 IT Act 2000, IT Rules 2000 and IT Regulations 2001 (**https://nicca.nic.in**).

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 is checked by using the CRL published in the repositories prior to reliance, or a check of the Certificate's status that would have indicated that the Certificate was valid.

3.1.4 Repository Obligations

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

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

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

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

3.1.5 Registration Authority (RA) Personnel Obligations

a. Take necessary approval from NICCA to function as RA Administrator.

RA from organisation (ORA) verifies the authenticity of the subscriber and RA from NIC (NICRA) checks the completeness of the DSC Form for issuance/revocation/suspension.

a. Request for revocation or suspension of a Certificate for any reason such as transfer, suspension, long leave, change of duties, superannuation and death.

b. Maintain records of requests for application, revocation, and suspension of Certificates.

3.2 Liability

3.2.1 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 is revoked and the next scheduled issuance of a Certificate Revocation List (CRL).

c. Due to unauthorized use of Certificates issued by NICCA, and use of Certificates beyond the prescribed usage.

d. Caused by fraudulent or negligent use of Certificates or Certificate revocation lists issued by NICCA.

e. Due to disclosure of information contained within Certificates and revocation lists.

f. Due to indirect, consequential or punitive damages arising from or in connection with its services.

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, 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.

3.2.2 Loss Limitations

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

3.2.3 Financial Responsibility

3.2.4 Indemnification of Certificate Authority by Relying Parties and Subscribers

NICCA will not be responsible for loss due to failure of the Subscribers and relying parties to fulfil their obligations under this CPS. In particular, 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.

3.2.5 Fiduciary Relationships between various Entities

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

3.2.6 Administrative Processes

No stipulation

3.3 Interpretation and Enforcement

3.3.1 Governing Laws

The Information Technology Act, 2000, Information Technology (Certifying Authorities) Rules, 2000 and Information Technology (Certifying Authority) Regulations, 2001 or any subsequent amendments 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.

3.3.2 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 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.

3.3.3 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.

3.4 Fees

3.4.1 Certificate Issuance Fees

The Certificate Fee Structure is published on NICCA website (**https://nicca.nic.in**). The Fee Structure is subject to revision at any stage and any such change shall be published on NICCA website immediately.

3.4.2 Certificate Access Fees

No fees.

3.4.3 Revocation or Status information Access Fees

No fees.

3.4.4 Fees for other services such as Policy Information

No fees.

3.4.5 Refund Policy

Not Applicable.

3.5 Publication and Repository

3.5.1 Publication of CA Information

NICCA makes publicly available its Certificate Practice Statement (CPS), Root Certificates(NICCA and Sub CA) and Certificate Revocation Lists (CRL) at **https://nicca.nic.in**

Also Digital Certificate Repositories at (**ldap://cadir.nic.in/c=IN??sub?cn=*)** from where a DSC can be accessed.

3.5.2 Frequency of publication

CRL publication is in accordance with this CPS (3.1.4).

CPS publication as and when modified and approved by CCA.

3.5.3 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.

3.5.4 Repositories

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

3.6 Compliance Audit

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

3.6.1 Frequency of Entity Compliance Audit

NICCA shall get its operations audited as per Rule 31 of the Rules under the IT Act.

3.6.2 Identity/Qualifications of Auditor

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

3.6.3 Topics covered by Audit

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.

3.6.4 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 from the CCA empanelled auditor list.

3.6.5 Actions taken as a Result of Deficiency

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.

3.6.6 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.

3.7 Confidentiality

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 protection of privacy of the subscriber.

3.7.1 Types of Information to be kept Confidential

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

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

3.7.2 Types of Information not considered Confidential

Information included in public Certificates issued by NICCA and the CRLs published by 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 NICCA (ii) was rightfully known or becomes rightfully known to NICCA without confidential or proprietary restriction from a source other than the Subscriber, (iii) is independently developed by NICCA, or (iv) is approved by a Subscriber for disclosure, shall not be considered confidential.

3.7.3 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 NICCA, a serial number will be included in the CRL entry for such a revoked Digital Signature Certificate.

3.7.4 Release to Law Enforcement Officials

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

3.7.5 INFORMATION THAT CAN BE REVEALED AS PART OF CIVIL DISCOVERY

Same as above

3.7.6 DISCLOSURE UPON OWNER'S REQUEST

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

3.7.7 OTHER INFORMATION RELEASE CIRCUMSTANCES

No stipulation.

3.8 INTELLECTUAL PROPERTY RIGHTS

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.

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.

4 IDENTIFICATION AND AUTHENTICATION

4.1 INITIAL REGISTRATION

An applicant has to fill the 'DSC Request Form' (available on 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 (HO) of the Organization/Department. The guidelines for verification by HO are detailed in DSC Request Form under heading "**The Guidelines for verification by Head of Office (HO)**.

4.1.1 TYPES OF NAMES

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 "Interoperability Guidelines (**http://cca.gov.in**) for digital signature Certificate version 2.4 December 2009 updated on 14 June 2011" issued by CCA.

4.1.2 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.

4.1.3 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.

4.1.4 NAME CLAIM DISPUTE RESOLUTION PROCEDURE

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

4.1.5 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.

4.1.6 AUTHENTICATION OF ORGANIZATION IDENTITY

The procedure of authentication organisation is carried out by the Head of the Office (HO) as stated in DSC Form (https://nicca.nic.in) under heading "**The Guidelines for verification by Head of Office (HO)**" and accordingly the HO gives the declaration on DCS Form that information **given** is correct.

4.1.7 AUTHENTICATION OF INDIVIDUAL IDENTITY

The procedure of authentication of individual identity is carried out by the Head of the Office (HO) as stated in DSC Form (https://nicca.nic.in) under heading "**The Guidelines for verification by Head of Office (HO)**"and accordingly the HO gives the declaration on DCS Form that informationgiven is correct.

4.1.8 AUTHENTICATION OF DOMAIN NAME/IP FOR SSL/WEB SERVER CERTIFICATE

The Head of the Office (HO) as stated in DSC Form (https://nicca.nic.in) ensures the correctness of URL/IP address and verifies that IP allocation authority and physical location of web server.

The RA checks for the existence of owner of domain name by using tools available on the Internet. The information received from tools gives the owner/registrant/registrar(organization, contact person) details which are verified against the information provided in DSC Form.

4.1.9 AUTHENTICATION OF SERIAL NO/MAC/IP ADDRESS FOR SYSTEM CERTIFICATE

The Head of the Office (HO) as stated in DSC Form (https://nicca.nic.in) ensures the correctness of IP/MAC/Serial No/CPU/Device number for which certificate to be issued.

4.2 ROUTINE RE-KEY

Re-key facility is currently not available.

5 OPERATIONAL REQUIREMENTS

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

5.1 CERTIFICATE APPLICATION

A Certificate applicant must complete a Certificate application in the prescribed format. For obtaining a Certificate from 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 the online information for key pair generation. The form is available electronically in NICCA website, which is duly verified and signed by the Head of Office of the organisation and checked by NIC Coordinator.

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 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 NICCA as stated in 3.1.2.9.
- Generate a Key pair using a Trustworthy System, as in section 3.1.2.2.
- Take reasonable precautions to protect the private key from compromise, as in section 3.1.2.3.
- Submit the public key to NICCA as stated in section 3.1.2.10.

5.2 CERTIFICATE ISSUANCE

Upon successful completion of the Subscriber's identification and authentication process as per this CPS, NICCA issues the requested Certificate, and makes the Certificate available to him. At

the discretion of NICCA, 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.

5.2.1 RE-ISSUANCE OF CERTIFICATE FOR DOWNLOAD ERROR

In case there is certificate download error due to some technical reason, the issued certificate is/are revoked with reason "Error in Downloading" by getting initiated on line revocation request by the DSC applicant.

DSC applicant generate once again online request for DSC issuance and new DSC is issued with the existing verification details and DSC Form i.e. no new DSC Form is sought from the DSC applicant.

5.3 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 NICCA before accepting the Digital Signature Certificate.

If the subscriber finds that the contents of Digital Signature Certificate issued by NICCA are same as filled-up/requested in DSC Form, he/she accepts the Certificate and then downloads the same.

5.4 RE-ISSUANCE/RENEWAL OF CERTIFICATE

The certificate is renewed/re-issued only duly submission of DSC Form and new key pair is required to be generated, so renewal/re-issuance is same as fresh DSC issuance.

5.5 CERTIFICATE SUSPENSION AND REVOCATION

NICCA revokes a Certificate, if the Subscriber, Registration Authority officials/NIC Coordinator or unauthenticated source requests Certificate revocation, which is stated below.

5.5.1 REQUESTOR,CIRCUMSTANCES AND MODES FOR REVOCATION

5.5.1.1 Request from Subscriber/HO

The subscriber himself/herself or Head of the organisation may request for revocation of certificate on account of following reasons:

1. The associated private key is known/suspected to be compromised, lost or misused.
2. The Subscriber's information (Distinguished /Subject name) in the Certificate has changed/transferred to some other department.
3. The Subscriber has permanently left the organisation (retired, resigned, taken VRS, expired while in service)/left the project.
4. Certificate download error

The subscriber or HO may submit revocation request (a) digital signed email (b) ink signed letter (c) duly filled Revocation Form-3 (d) in-person (e) email (f) over phone (g) fax.

The subscriber may also submit his/her revocation request by logging to CA system.

If request is submitted by mode (d), (e) (f) and (g) as stated above, necessary verification is carried out by NICCA/RA before further processing.

5.5.1.2 Request from NICCA/Registration Authority officials

The NICCA/RA officials/NIC Coordinator may request for revocation of certificate on account of following reasons:

a. The Subscriber has permanently left the organisation (retired, resigned, taken VRS, expired while in service).

b. a material fact represented in the Digital Signature Certificate is false or has been concealed;

c. a requirement for issuance of the Digital Signature Certificate was not satisfied;

d. NICCA's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

e. Subscriber has been declared dead or where a subscriber is an organisation, which has been dissolved, wound-up or otherwise ceased to exist.

f. The associated private key is known/suspected to be compromised, lost or misused.

g. Any other reason fit for revocation

NIC Coordinator shall intimate to NICCA/RA officials for such cases by email/phone.

NICCA/RA officials submit online revocation requestalong with the reason as stated above and request is processed further.

5.5.1.3 Unauthenticated Source

In case where NICCA can independently confirm that the Certificate has been compromised or misused, 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.

In such cases, 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 put "hold" i.e. it shall be kept under suspension till actual authentication of the revocation request. If the subscriber could not be reached, the certificateis revoked at the end of 15 days. Such final confirmation of revocation can be initiated by NICCA, if it receives:

1. an e-mail digitally signed by the Subscriber's private key
2. 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 NICCA by letter mail
3. an original letter signed by the Subscriber.
4. a Request through the Certificate Revocation Form signed by the Subscriber. The 'Request for Certificate Revocation Form' can be obtained from electronically from NICCA Repository.

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. The maximum wait period is 15 days for confirmation from the subscriber.

NICCA will revoke the Certificate and thereby terminate its validity permanently, upon receipt of final confirmation of revocation request directly from the Subscriber.

They submit online revocation request along with reason and request is processed further.

5.5.2 REQUESTOR, CIRCUMSTANCES AND MODES FOR SUSPENSION

The certificate can be suspended i.e. put on hold as stated in sub-paras.

5.5.2.1 Request from Subscriber/HO

The subscriber himself/herself or Head of the organisation may request for suspension of certificate if (a) the subscriber is on leave (b) it is in the public interest to keep DSC on suspended state (c) it suspected some misuse or is informed of some malicious intentions with respect to usage of the certificate in question
The subscriber or HO may submit revocation request (a) digital signed email (b) ink signed letter (c) duly filled Revocation Form-3 (d) in-person (e) email (f) over phone (g) fax.

The subscriber may also submit his/her revocation request by logging to CA system.

If request is submitted by mode (d), (e), (f) and (g) as stated above, necessary verification is carried out by NICCA/RA before further processing.

5.5.2.2 Request from NICCA/Registration Authority officials

The NICCA/RA officials/NIC Coordinator may request for suspension of certificate on account of (a) to keeps DSC in suspended state is in the public interest (b) If a revocation request for the Certificate is on hold due to pending contact with the Subscriber (c) suspicion

some misuse or is informed of some malicious intentions with respect to usage of the certificate in question.

NICCA/RA officials submit online suspension request along with the reason as stated above and request is processed further.

5.5.2.3 Limits on suspension period

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

5.5.3 POST REVOCATION OR SUSPENSION REQUEST

In case NICCA receives a request for activation from the subscriber, either online or through the prescribed Form (Doc-Id: Form-3), 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.

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.

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

A notification stating suspension/revocation of the Subscriber’s Certificates is sent to the Subscriber by a registered mail.

NICCA updates **Certificate Revocation List (CRL)** is as follows:

a) 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 72hours** 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 above. 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 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 NICCA to suspend or revoke the Certificate. 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 NICCA could revoke the Certificate, or upon making a revocation request or upon being notified by 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 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. 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) 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.

5.5.4 USING THE COMPROMISED PRIVATE KEY &REVOCATION REQUEST GRACE PERIOD

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.

5.5.5 CRL ISSUANCE FREQUENCY

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

5.5.6 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 NICCA/NRDC Repository from time to time.

5.5.7 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

As of now, NICCA does not support this facility.

5.5.8 ON-LINE REVOCATION CHECKING REQUIREMENTS

Same as procedures laid down for revocation in section 5.4.10 and 5.4.11 of this CPS.

5.5.9 Other forms of Revocation Advertisements available

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

5.5.10 Checking Requirements for other forms of Revocation Advertisements

No Stipulation

5.5.11 Special requirements Re-key compromise

No stipulation

5.6 Security Audit Procedures

5.6.1 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 NICCA operations
- Privileged accesses to all NICCA components

The following types of events are recorded by NICCA:

System start-up and shutdown

1. CA's application start-up and shutdown.
2. Login and logouts to NICCA Servers.
3. Attempts to create, remove, set passwords or change the system privileges of NICCA trusted roles.
4. Changes to Digital Signature Certificate creation policies.
5. Unauthorized attempts at network access to the NICCA's systems.
6. Unauthorized attempts to access to system files.
7. Creation and revocation of NICCA Digital Signature Certificates.
8. Attempts to initialize remove, enable, and disable subscribers.
9. Errors.
10. End user keypair generation, certificate generation, suspension, revocation &activation.

5.6.2 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 NICCA.

5.6.3 Retention Period for Audit Log

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

5.6.4 Protection of Audit Log

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

5.6.5 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.

5.6.6 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.

5.7 Records Archival

5.7.1 Types of Event Recorded

The following types of events are archived:

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

5.7.2 Retention Period for Archive

Digital Signature Certificates stored by NICCA and issued CRLs will be archived for at least seven years after key expiration. Audit information detailed in section 5.6.3, Subscriber agreements, RA agreements and Relying Parties agreements will also be retained for a period of two years.

5.7.3 Protection of Archive

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

5.7.4 ARCHIVE BACKUP PROCEDURES

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

5.7.5 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.

5.7.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

The archive collection system is internal to NICCA.

5.7.7 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.

5.8 KEY CHANGEOVER

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

5.9 COMPROMISE AND DISASTER RECOVERY

5.9.1 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

In the case where 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.

5.9.2 ENTITY PUBLIC KEY IS REVOKED

5.9.2.1 Subscriber's Public Key

As in the section5.5.3of CPS.

5.9.2.2 CA Public Key

1. The key is revoked.
2. The CRL is updated and published.
3. NICCA system is brought down.
4. New CA key pair is generated as indicated in Section 7.1.6.
5. Users are notified.

5.9.3 ENTITY KEY IS COMPROMISED

5.9.3.1 Subscriber's Key is compromised

Whenever the Subscriber's key is compromised, the Subscriber is obliged to notify NICCA as soon as possible. The revocation procedure is in accordance with the Section 5.5 of this CPS.

5.9.3.2 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. 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 7.1.6.
7. The public key of NICCA's new key pair is sent to the CCA for certification.
8. Users are notified about the revocation.

5.9.4 SECURE FACILITY AFTER A NATURAL OR OTHER TYPE OF DISASTER

NICCA has commissioned its Disaster Recovery (DR) site, which has been put in synchronization with primary site so that mission critical operations of NICCA can be carried out in the event of natural disaster at Primary Site of NICCA at New Delhi. The Complete plan of action and the procedures to be followed by NICCA Trusted Roles to recover and restore partially or completely the interrupted NICCA services and functions, within a predetermined time after a disaster or extended disruption, so as to minimize the likelihood and impact (risk) of interruptions has been explained in the document namely "NICCA Disaster recovery (DRP)/Business Continuity Plan(BCP)".

5.10 CA TERMINATION POLICY

a. NICCA can decide to cease its services. In that case the following steps shall be undertaken:
b. Notify the CCA of its intention to cease acting as a Certifying Authority (CA) at least ninety days before it ceases to act as a CA or ninety days before the date of expiry of license.

c. 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 CA.
d. 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 CA.
e. NICCA will inform all Subscribers, and Relying parties with whom NICCA has agreements or other form of established relations about the decision.
f. NICCA shall make a reasonable effort to ensure that discontinuation of certification services causes minimal disruption to Subscribers and relying parties requiring to verify the Digital Signatures by reference to the public keys contained in outstanding Digital Signature Certificates.
g. Any Certificates issued after the announcement of the termination date shall have the expiration date not exceeding the termination date.
h. On the termination date, all the Certificates issued by NICCA shall be revoked, inclusive of DSCs which are un-recovered or unexpired on the termination date, and irrespective of whether the subscribers have requested for revocation or not. 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. NICCA Certificate status shall also be displayed on NICCA web site.
i. NICCA has made necessary arrangements for preserving the records for a period of seven years, as stipulated in the IT Act 2000.
j. No compensation shall be given to subscribers.
k. 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.

6 PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY

This component describes non-technical security controls such as physical, procedural and personnel controls used by 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 NICCA private key.

6.1 PHYSICAL SECURITY CONTROL

6.1.1 SITE LOCATION AND CONSTRUCTION

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

Disaster recovery facility is available at Hyderabad

6.1.2 PHYSICAL ACCESS

NICCA has implemented necessary physical security controls to restrict access to NICCA Hardware and Software. The controls are applied to 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 NICCA facility is limited to the trusted roles only. The trusted roles gain access to NICCA facility by means of Trusted Role Identification Card. The physical access is logged manually as well as electronically.

6.1.3 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.

6.1.4 WATER EXPOSURES

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

6.1.5 FIRE PREVENTION AND PROTECTION

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.

6.1.6 MEDIA STORAGE

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

6.1.7 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.

6.1.8 OFF-SITE BACKUP

NIC Pune centre is keeping off-site backup in addition backup at Primary Site (New Delhi) and Disaster Recovery Site (Hyderabad).

6.2 PROCEDURAL CONTROLS

6.2.1 TRUSTED ROLES

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

Trusted Roles include all employees of NICCA. These trusted roles are collectively known as trusted personnel. As these trusted personnel have access to 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/Sub-CA Administrator, RA Administrator.
- 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.

6.2.2 NUMBER OF PERSONS REQUIRED PER TASK

In order to safeguard the security of NICCA server, the responsibilities for various operations of the NICCA server are delegated to 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 NICCA.

6.2.3 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 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 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 NICCA official, performing the role of system security officer.

6.3 Personnel Controls

6.3.1 Background, Qualifications, Experience, and Clearance Requirements

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 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 6.3.2 are completed.

6.3.2 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 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 NICCA for the specific trusted role.
- The methods used by the employer to carry out the background checks.

6.3.3 Training Requirements

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 NICCA.
- Technical training relevant to the responsibility.
- Data handling techniques.

6.3.4 Retraining Frequency and Requirements

No stipulation

6.3.5 Job Rotation Frequency and Sequence

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

6.3.6 Sanctions for Unauthorized Actions

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

6.3.7 Contracting Personnel Requirements

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

6.3.8 Documentation Supplied to Personnel

All personnel involved in the operations of 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 NICCA Management for the respective Trusted Roles are also provided.

7 TECHNICAL SECURITY CONTROLS

7.1 KEY PAIR GENERATION AND INSTALLATION

7.1.1 KEY PAIR GENERATION

NICCA itself does not generate private key for the end users. It sends crypto device having no keys on it, which carries user personal information printed on it. The subscriber generates his/her key pairs at his/her place using web interface (**https://nicca.nic.in**) of NICCA after authentication based on user-id and password sent by mail, in case the subscriber finds some problem in generating key pairs they he can get in touch with RA for key generation assistance.

The subscriber also has option to generate key pair using his/her methods and submission of public key in PKCS#10 format using web interface (**https://nicca.nic.in**) of NICCA after authentication based on user-id and password.

7.1.2 PRIVATE KEY DELIVERY TO ENTITY

In case the subscriber chooses to generate his/her key pair through web interface (**https://nicca.nic.in**), the private key is generated on FIPS certified hardware at their place through web interface only after authentication based on user-id and password.

In case the subscriber chooses to generate his/her key pair using his/her own method and submits public key in PKCS#10 format using web interface (**https://nicca.nic.in**) of NICCA after authentication based on user-id and password, he/she retains private key himself/herself.

In both the cases above, the subscriber generates his/her private key himself/herself at their places.

7.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

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

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

7.1.3.1 CA Public Key Delivery to Users

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

7.1.3.2 Key Sizes

NICCA uses RSA public key algorithm.

NICCA (CA and Sub-CA) and End User Private key size is 2048 bits.

7.1.4 Public Key Parameters Generation

Public key parameters are generated by the relevant applications.

7.1.5 Parameter Quality Checking

No Stipulation.

7.1.6 Hardware/Software Key Generation

NICCA key pair is generated by using a hardware security module conforming to FIPS 140-2 level 3or higher standards.

The Subscriber keys for End User Certificate/Digital Signature Certificate are generated on FIPS certified hardware ONLY.

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

The X.509 v3Key Usage and Enhanced Key Usage fields are set according to the requirements stated in section 7 of this CPS.

7.2 Private Key Protection

7.2.1 Standards for Cryptographic Module

A hardware module conforming to FIPS 140-2 level 3or higher standards is used for generation of NICCA keys.

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

NICCA uses 2 out of 4 private key control.

7.2.3 Private Key Escrow

NICCA private keys are presently not escrowed.

7.2.4 Private Key Backup

The Backed up keys are stored in the same manner on hardware Security Module HSM 140-2 Level 3 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.

7.2.5 Private Key Archival

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

7.2.6 Private Key entry into Cryptographic Module

NICCA private key is generated using FIPS 140-2 level 3 hardware security modules.

7.2.7 Method of Activating Private Key

NICCA private key isaccessed by multiple controls.

7.2.8 Method of Deactivating Private Key

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

7.2.9 Method of Destroying Private Key

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.

7.3 Other Aspects of Key Pair Management

7.3.1 Public Key Archival

Public keys may be restored from backup.

7.3.2 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 NICCA Digital Signature Certificate. The Digital Signature Certificate also automatically expires with the expiration of NICCA software license.

7.4 Activation Data

7.4.1 Activation Data Generation and Installation

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

7.4.2 Activation Data Protection

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

7.4.3 Other Aspects of Activation Data

No stipulation

7.5 Computer Security Control

7.5.1 Specific Computer Security Technical Requirements

NICCA computer system satisfies the following requirements:

1. NICCA is run on dedicated computer systems.
2. Only the software needed to perform NICCA tasks is installed on the system.
3. Access to the operating system and NICCA software is allowed only to the authorized NICCA trusted personnel and maintenance personnel from authorised vendor.
4. Physical access to the system is allowed only to the authorized NICCA trusted personnel.
5. All security related events are audited in 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.

7.5.2 Computer Security Rating

No stipulation

7.6 Life Cycle Technical Controls

7.6.1 System Development Controls

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

Production and development environment are totally separated.

7.6.2 Security Management Controls

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

7.6.3 Life Cycle Security Ratings

No Stipulation

7.7 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.

7.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

The Hardware Security Module provides cryptographic functions.

8 CERTIFICATE AND CRL PROFILE

The profile and algorithms for certificates and CRL is strictly in accordance with profiles given in the CCA Interoperability Guidelines for digital signature Certificate version 2.4 December 2009 updated on 14 June 2011" (**http://cca.gov.in**)

9 SPECIFICATION ADMINISTRATION

9.1 SPECIFICATION CHANGE PROCEDURES

All changes in this NICCA CPS shall be brought to the notice of the CCA before being published on NICCA Repository. 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 NICCA CPS shall supersede all previous versions and impose a legal obligation on Subscribers and NICCA. Any changes in CPS shall not contravene any provision of the act, rule and regulation made there under.

9.1.1 ITEMS THAT CAN CHANGE WITHOUT NOTIFICATION

No items can be changed without notification to the CCA.

9.1.2 CHANGES REQUIRING NOTIFICATION

9.1.2.1 List of Items

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

9.1.2.2 Notification Mechanism

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

9.1.2.3 Comment Period

No Stipulation

9.1.2.4 Mechanism to Handle Comments

No Stipulation

9.2 Publication and Notification Policies

9.2.1 Items Not Published in the CPS

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

9.2.2 Distribution of the CPS

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

9.3 CPS Approval Procedures

The draft CPS is presented before NICCA Policy approval committee appointed by 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.

10 DISCLAIMER

NICCA is not responsible for any data loss/damage arising from the use of this Certificate/Token/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.

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.

11 REQUEST FORMS

[1] Digital Signature Certificate (DSC) Request Form (Form Doc-Id : Form-1).

[2] Digital Signature Certificate (DSC) Request Form (Doc-Id : Form-2).

[3] Request for Revocation/Suspension/Activation (Form Doc-Id : Form-3).

12 FLOW CHARTS

[4] Digital Certificate Signature Issuance.

[5] Digital Signature Certificate Revocation/Suspension/Activation

13 REFERENCES

[6] Information Technology (IT) Act 2000.

[7] NICCA Certification Practice Statement Version 4.4

[8] BS25999 is a standard that establishes the process, principles and terminology of business continuity management

~~~
~~~