Tata Consultancy Services Limited

Certifying Authority

Certification Practice Statement

IN SUPPORT OF PUBLIC KEY INFRASTRUCTURE SERVICES

TCS-CA TRUST NETWORK VERSION 1.1

DATE OF PUBLICATION: DECEMBER 2007

PROPOSED EFFECTIVE DATE: DECEMBER 2007

DECCANPARK, 1 – SOFTWARE UNITS LAYOUT, MADHAPUR,
HYDERABAD –500081
ANDHRA PRADESH, INDIA

This document namely the Certification Practice Statement has been drafted based on the **RFC-2527: Internet X.509 Public Key Infrastructure Certificate Policy** and Certification Practices Framework and the guidelines for submission of application for license to operate as a Certifying Authority under the IT Act, 2000, Annexure –1.

Wherever the phrase "Tata Consultancy Services Limited" or the abbreviation "TCS" appears in this document, including within the abbreviation "TCS-CA", it shall be taken to mean "Tata Consultancy Services Limited".

WARNING

DIGITAL CERTIFICATION SERVICES PROVIDED BY TATA CONSULTANCY SERVICES LIMITED ARE SUBJECT TO VARIOUS INDIAN LAWS AND JURISDICTION OF COURTS, TRIBUNALS AND AUTHORITIES IN INDIA.

THIS CERTIFICATION PRACTICE STATEMENT SHALL BE READ WITH ANY STATEMENT WITH SUCH PARTICULARS AS THE CONTROLLER OF CERTIFICATION AUTHORITIES (CCA) MAY SPECIFY BY REGULATION IN EXERCISE OF HIS POWERS UNDER THE INFORMATION TECHNOLOGY ACT, 2000.

WRONG USE OF THE DIGITAL CERTIFICATES OR ITS SERVICES SHALL BE LIABLE TO BE PROCEEDED WITH CONSEQUENCES CIVIL AND CRIMINAL AND SHALL BE SUBJECTED TO PENALTIES AND PUNISHMENT. THE INFORMATION TECHNOLOGY ACT, 2000 AND RULES PROVIDE FOR SPECIFIC DUTIES OF SUBSCRIBERS AS CONTAINED IN CHAPTER VIII OF THE ACT.

DEFINITIONS

The following definitions are to be used while reading the TCS-CA CPS. The definitions are provided in alphabetical order.

(a) "Access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network

(b) "Act" means the Information Technology Act, 2000

(c) "Affixing Digital Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Digital Signature

(d) "Applicant" or "user" means a Digital Signature Certificate Applicant

(e) "Auditor" means any professional or agency appointed by the Certifying Authority and recognized by the Controller of Certifying Authorities for conducting technical audit of operation of Certifying Authority

(f) "CA" refers to the TCS - Certifying Authority licensed by the Controller of Certifying Authorities.

(g) "Compromise" means a violation (or suspected violation) of a security policy, in which an unauthorized disclosure of or loss of control over sensitive information may have occurred

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

(i) "Computer resource" means computer, computer system, computer network, data, computer data base or software

(j) "Controller" means Controller of Certifying Authorities appointed under sub-section (1) of Section 17 of the Act

(k) "CPS" means this Certification Practice Statement.

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

(m) "Devices" are non person entities to whom a Digital Signature Certificate has been issued. The Common Name field in this case will contain either the Domain Name or the IP address associated with the Device. The applicant for a Digital Signature Certificate for a device must be the owner of the Domain Name or the IP address mentioned in the Digital Signature Certificate. Examples of devices include, but are not limited to, Servers, Routers, Laptops and Mobile phones.

(n) "Digital Certificate" means Digital SIGNATURE Certificate issued by the Tata Consultancy Services Limited Certifying Authority .

(o) "Digital Signature" means an electronic method or procedure used in order to authenticate any electronic record by the use of an asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

(p) "Digital Signature Certificate" means Digital Certificate issued by the Tata Consultancy Services Limited Certifying Authority and which may be used for affixing a Digital Signature.

(q) "End Entity" refers to any entity who is the end user of Digital Signature Certificates issued under the TCS-CA Trust Network

(r) "Entity" refers to the users of the Digital Signature Certificate

(s) "Information asset" means all information resources utilized in the course of any organization's business and includes all information, applications (software developed or purchased), and technology (hardware, system software and networks)

(t) "License" means a license granted to Certifying Authorities for the issue of Digital Signature Certificates under the IT Act, 2000

(u) "Licensed Certifying Authority" refers to a Certifying Authority who has been granted a license to issue Digital Signature Certificates

(v) "Key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a Digital Signature created by the private key

(w) "Private key" means that key of a key pair which is used to create a Digital Signature

(x) "Public key" means that key of a key pair which is used to verify a Digital Signature and listed in the Digital Signature Certificate

(y) "Person" shall include an individual or a company or association or body of individuals, whether incorporated or not, or Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments

(z) "Primary Issuing authority" (PIA) means Tata Consultancy Services Limited Certifying Authority (TCS-CA)

(aa) "Subordinate Certifying Authority" (Sub-CA) is a technical CA specially created under TCS-CA Trust network and operated by TCS-CA for a partner who is authorized by TCS-CA to verify the applications and upon successful verification, requesting the TCS-CA to generate a Digital Signature Certificate for the respective Applicants under the TCS-CA Trust Network in accordance with the IT Act, 2000 to its set of affiliated users to form a Closed User Group (CUG). TCS-CA will issue a special Digital Signature Certificate to each Sub-CA. This Digital Signature Certificate shall contain "TCS-CA – Sub-CA for *<name of entity for whom the Sub-CA has been set up>*" whose Private Key shall be under the control of TCS-CA, and TCS-CA shall issue Digital Signature Certificates to subscribers who are duly authorized by the partner, and such Digital Signature Certificates shall contain the name "TCS-CA -- Sub CA for *<name of entity for whom the Sub-CA has been set up>*" .

(bb) "Registration Authority" (RA) is an entity appointed by the TCS-CA under the TCS-CA Trust Network that collects and processes Applicant's/Subscriber's application form as prescribed in the IT Act, 2000. The term RA includes all partners for whom TCS-CA has set up a Sub-CA.

(cc) "Relying Party" means any person seeking to use a Digital Signature Certificate either to verify a Digital signature affixed by the subscriber of that Digital Signature Certificate or to encrypt data which can be decrypted by the subscriber of that digital Certificate.

(dd) "Subscriber" means an applicant in whose name a Digital Signature Certificate has been issued

(ee) "Subscriber identity verification method" means the method used to verify and authenticate the identity of a Subscriber

(ff) "TCS-CA Trust Network" includes the Primary Issuing Authority (TCS-CA), all Partner for whom Sub-CA has been created under TCS-CA, all Registration Authorities (RAs) appointed by TCS-CA and all the Subscribers of the digital signature certification services under TCS-CA Trust Network.

(gg) "TCS-CA Trust Portal" means the TCS-CA website

(hh) "Trusted Person" means any person who has:

- Direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act in respect of a Certifying Authority
- Duties directly involving the issuance, renewal, suspension, revocation of Digital Signature Certificates (including the identification of any person requesting a Digital Signature Certificate from a licensed Certifying Authority), creation of private keys
- Administration of a Certifying Authority's computing facilities

(ii) "Verify" in relation to a Digital Signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether –

- The initial electronic record was affixed with the Digital Signature by the use of private key corresponding to the public key of the Subscriber
- The initial electronic record is retained intact or has been altered since such electronic record was so affixed with the Digital Signature.

Note: Words and expressions used herein and not defined shall have the meaning respectively assigned to them in that context.

ACRONYMS

CA	Certifying Authority
CCA	Controller of Certifying Authorities
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
e-mail	Electronic Mail
FIPS	Federal Information Processing Standard
GMT	Greenwich Mean Time
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
IETF	Internet Engineering Task Force
IT	Information Technology
ITU	International Telecommunications Union
LAN	Local Area Network
MCAO	Manager CA Operations
OID	Object Identifier
PCS	TCS-CA's Public Certification Services
PIA	Primary Issuing Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PRA	Primary Registration Authority
RA	Registration Authority
RFC	Request For Comment
RSA	The Rivest Shamir Adleman Cryptographic Algorithm
S/MIME	Secure Multipurpose Internet Mail Extensions
SPKAC	Netscape signed public key and challenge
SSL	Secure Sockets Layer
SUB-CA	Subordinate Certifying Authority
TCS	Tata Consultancy Services Limited

TCS–CA	Tata Consultancy Services Limited Certifying Authority
URL	Uniform Resource Locator
WAN	Wide Area Network
WWW	World Wide Web
X.509	The ITU-T standard for Certificates and CRLs

IMPORTANT CPS RIGHTS AND OBLIGATIONS

1. This Certification Practice Statement controls the provision and use of Tata Consultancy Services Limited – Certifying Authority's (TCS-CA) digital certification services – including Digital Signature Certificate application, application validation, Digital Signature Certificate issuance, acceptance, use, suspension, activation and revocation of a Digital Signature Certificate.

2. Tata Consultancy Services Limited – Certifying Authority assumes that the applicant will make himself aware of the subscriber obligation, section 2.1.4 of this CPS prior to applying for a Digital Signature Certificate.

3. Tata Consultancy Services Limited – Certifying Authority offers different classes and types of Digital Signature Certificates under the TCS-CA Trust Network. The applicants must decide which class and type of Digital Signature Certificates suit their need.

4. Before submitting a Digital Signature Certificate application, the applicant must, except while requesting for an Encryption Certificate, generate a Digital Signature key pair (Public Key and Private Key) in a secure medium and shall take reasonable care to retain the control of private key corresponding to public key (including Encryption Key pair) and takes all steps to prevent its disclosure to a person not authorized to affix the Digital Signature of the Subscriber.

5. The applicant must accept a Digital Signature Certificate before communicating it to others, or otherwise invoking use of it. By accepting a Digital Signature Certificate, the applicant makes certain important representations as described in obligations of the Subscriber.

For more information or to provide feedback:

- Visit the TCS-CA Trust Portal at **https://www.tcs-ca.tcs.co.in** or
- Contact TCS-CA Administrator at **helpdesk@tcs-ca.tcs.co.in** .

TABLE OF CONTENTS

1 INTRODUCTION

1.1 OVERVIEW

This section provides an overview of the TCS-CA Trust Network Certification Practice Statement (CPS) and its role in the operations of TCS-Certifying Authority and the members of its Trust Network.

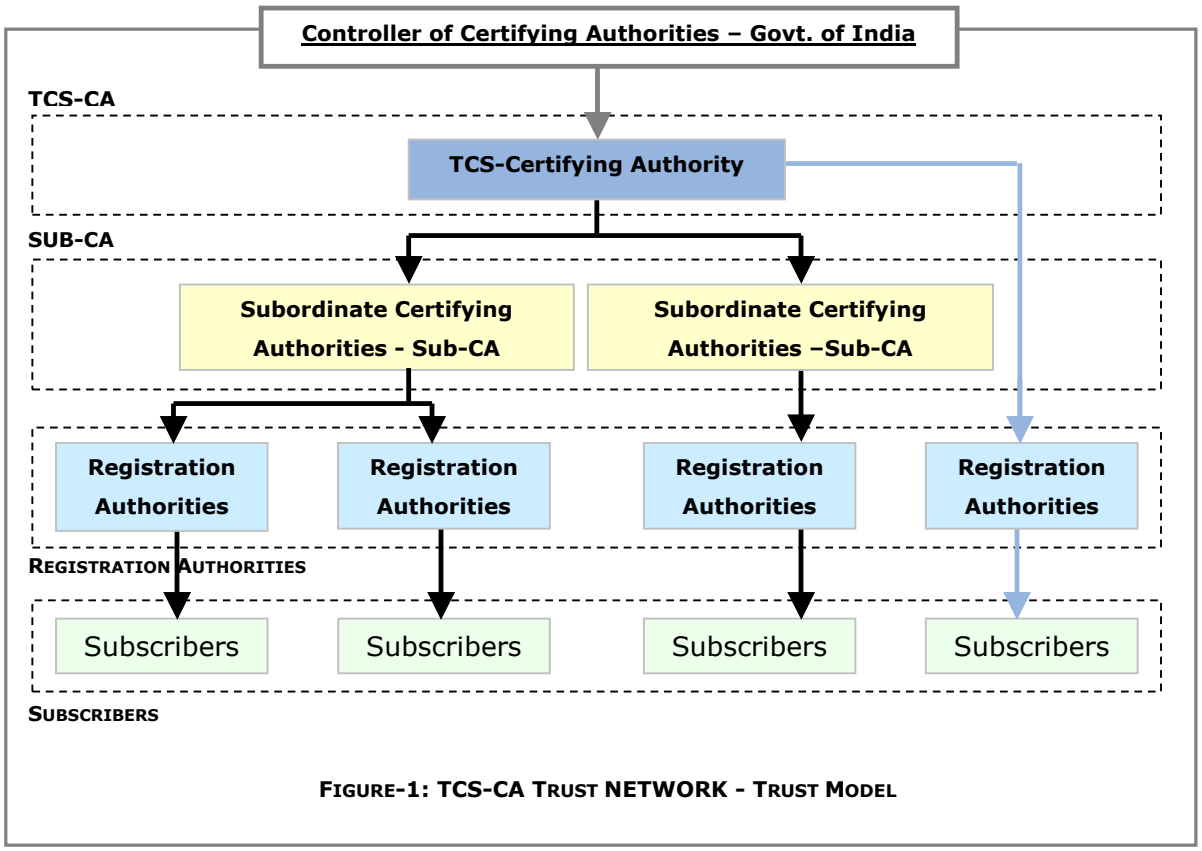

FIGURE-1: TCS-CA TRUST NETWORK - TRUST MODEL

- The **TCS-CA Trust Network** consists of all entities involved in the process of issuing and managing Digital Signature Certificates under the TCS-Certifying Authority. These are TCS-CA, all Partners for whom Sub-CA has been created of TCS-CA and all RAs under TCS-CA

The CPS documents the basis for issuing, managing, using, suspending, activating and revoking of Digital Signature Certificates. The CPS is intended to legally bind all parties that create, use, and validate Digital Signature Certificates within the context of the certification practices.

The CPS is a public document intended to be perused by Partners for whom Sub-CA has been created, RAs, Subscribers, applicants and relying parties. As such the CPS defines the high level practices & policies of TCS-CA digital certification services under the TCS-CA Trust Network. The detailed procedures that support the CPS, are documented in a set of procedure manuals, defined in Appendix-A: TCS-CA Document Master List. These manuals, unless specified explicitly, are confidential to TCS-CA but are open to scrutiny by the CCA office and its approved auditors.

1.2 IDENTIFICATION

This CPS is called the Tata Consultancy Services Limited – Certifying Authority Trust Network Certification Practice Statement.

1.3 COMMUNITY AND APPLICABILITY

This CPS is applicable to the TCS-CA, all Partners for whom Sub-CA has been created of TCS-CA and all RAs under TCS-CA as well as applicants and Subscribers who wish to obtain/ have obtained Digital Signature Certificates including those defined in and by the IT Act, 2000.

1.3.1 Certifying Authority

The TCS-CA will issue a Digital Signature Certificates, which bind a public and private key pair, to a Subscriber.

In addition to the generation of the Digital Signature Certificates, the CA may also suspend, activate or revoke the Digital Signature Certificates. The CA also maintains the CRL for the revoked and suspended Digital Signature Certificates in its repository.

1.3.2 Subordinate Certifying Authority

Subordinate Certifying Authority" (Sub-CA) is a technical CA specially created under TCS-CA Trust network and operated by TCS-CA for a partner who is authorized by TCS-CA to verify the applications and upon successful verification, requesting TCS-CA to generate a Digital Signature Certificate for the respective Applicants under the TCS-CA Trust Network in accordance with the IT Act, 2000 to its set of affiliated users to form a Closed User Group (CUG). TCS-CA will issue a special Digital Signature Certificate for each Sub-CA. This Digital Signature Certificate shall contain "TCS-CA – Sub-CA for *<name of entity for whom the Sub-CA has been set up>*" whose Private Key shall be under the control of TCS-CA, and TCS-CA shall issue

Digital Signature Certificates to subscribers who are duly authorized by the partner, and such Digital Signature Certificates shall contain the name "TCS-CA -- Sub CA for *<name of entity for whom the Sub-CA has been set up>*" in the issuer field.

A partner for whom a Sub-CA has been set up may receive the applications for the Digital Signature Certificate directly from applicants and verifies the details contained in the application. On successful verification, the request is electronically forwarded to the TCS-CA recommending generation of a Digital Signature Certificate for the verified Applicant. TCS-CA shall then issue the Applicant a Digital Signature Certificate signed with the Private Key corresponding to the Sub-CA Digital Signature Certificate created for the partner.

1.3.3 Registration Authorities

A Registration Authority (RA) is an entity appointed by the TCS-CA under the TCS-CA Trust Network that collects and processes Applicant's application form (see Section 12 of this CPS), as prescribed in the IT Act, 2000. The term RA includes all partners for whom TCS-CA has set up a Sub-CA.

An RA receives the applications for the Digital Signature Certificate from the Applicant and verifies the details contained in the application. On successful verification, the request is electronically forwarded to the TCS-CA recommending generation of a Digital Signature Certificate for the verified Applicant.

1.3.4 End Entities

The end entities who make use of the Digital Signature Certificates are:

- **Applicants**
- **Subscribers**
- **Devices**
- **Relying parties**

1.3.5 Applicability

The Digital Signature Certificates issued under the TCS-CA Trust Network are used for lawful purposes as further described in the Digital Signature Certificate usage Sub Section of the Operational Requirement section in this CPS. Use of issued Digital Signature Certificates under the TCS-CA Trust Network for other than above-mentioned usage is expressly prohibited. The CA either by its own judgment, or guided by the advice of a concerned RA, reserves the rights to revoke Digital Signature Certificates of person, entity, or organization for, among other reasons, indulging in illegal use or misuse of Digital Signature Certificates.

1.3.5.1 Prohibited Applications

The Digital Signature Certificates issued under this CPS are not designed, intended or authorized for use or resale as control equipments in hazardous circumstances or for users requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, etc where failure could lead directly to death, personal injury or severe environmental damage.

1.4 CONTACT DETAILS

1.4.1 CPS Administration

This CPS is administered by the Tata Consultancy Services Limited – Certifying Authority. The CPS shall be revised from time to time, as and when needed by TCS-CA, with sufficient notification to the end users by publishing the same in the repository of the TCS-CA Trust Portal.

1.4.2 Contact Information

The Tata Consultancy Services Limited – Certifying Authority can be contacted at the following address:

Tata Consultancy Services Limited - Certifying Authority
deccanpark, 1 – Software Units Layout,
Hyderabad – 500 081
Andhra Pradesh, India
Toll Free number: 1-800-425-2922

For more information or to provide feedback:

- Visit the TCS-CA Trust Portal at **https://www.tcs-ca.tcs.co.in**
- Contact TCS-CA Administrator at **helpdesk@tcs-ca.tcs.co.in**

1.4.3 Publication

Users can obtain the TCS-CA CPS in the following formats:

- In electronic form:
  https://www.tcs-ca.tcs.co.in

- In paper form from:

  Tata Consultancy Services Limited – Certifying Authority

  deccanpark, 1 – Software Units Layout,

  Hyderabad – 500 081

  Andhra Pradesh, India

  Toll Free number: 1-800-425-2922

2 GENERAL PROVISIONS

This section sets forth general provisions and defines and allocates specific responsibilities among various parties participating in the Public Key Infrastructure established by this CPS.

The terms of this CPS are deemed to be effective:

- Upon publication of this CPS in case of RA, Partner for whom Sub-CA has been created, and the TCS-CA
- Upon submission of an application for a Digital Signature Certificate under the TCS-CA Trust Network in case of an Applicant/Subscriber

2.1 OBLIGATIONS

The TCS-CA shall issue Digital Signature Certificates to Applicants within 3 business days after a duly verified Certificate request is received from RA. The Applicant can know the status of the request from the TCS-CA Trust Portal.

A Digital Signature Certificate will be revoked by close of business day for revocations placed online by subscriber from his/her user login and if the request for revocation is received vide email/letter, verification of a revocation request is made and the revocation will be done on the following business day, but action on a revocation request made over a weekend or holiday may be delayed until the following business day of the RA. Revoked Digital Signature Certificates are published in a CRL (Certificate Revocation List), which is issued under the TCS-CA Trust Network and posted to TCS-CA repository for public use.

2.1.1 CA Obligations

The TCS-CA shall be responsible for the following:

- Acting in accordance with policies and procedures designed to safeguard the Digital Signature Certificate management process (including Digital Signature

Certificate issuance, suspension, activation, revocation, and audit trails) and to protect the TCS-CA private key from compromise.

- Issuing Digital Signature Certificates to Applicants that have been verified and validated by RA
- Suspension, activation and revocation of the Digital Signature Certificates based upon advice from RA as per the terms and conditions in the TCS-CA CPS.
- Issuing and publishing the CRL regularly as per the terms and conditions in the TCS-CA CPS.
- Maintaining this CPS with revisions as and when changes are made.
- Creating and maintaining an accurate audit trail of all CA operations under TCS-CA.
- Ensuring that all aspects of TCS-CA digital certification services under the TCS-CA Trust Network, operations and infrastructure related to Certificate issuance are performed in accordance with the requirements, representations and warranties of this CPS.
- TCS-CA shall be responsible for all operations performed by partners appointed as RA, including those for whom Sub-CA has been set up, to the extent agreed under the corresponding Sub-CA and RA agreements entered with the partners under the TCS-CA trust network.
- Submission of Certificate/CRL issued under TCS-CA Trust Network, to the CCA for its National Repository (NRDC).

TCS-CA shall not:

- Be responsible if the Subscriber's password is compromised and a request for Suspension, Revocation or Activation is placed on the Subscriber's behalf.
- Be obliged to inform users of revocation of their Digital Signature Certificates in case of the request being initiated by the Subscribers themselves. In case of request being initiated by TCS-CA, the Subscriber shall be informed of the action being taken.

2.1.2 Obligations of partner for whom Sub-CA has been created

A partner for whom Sub-CA has been created shall be responsible for the following:

- Acting in accordance with policies and procedures designed to safeguard the Digital Signature Certificate management process (including Digital Signature Certificate issuance, suspension, activation, revocation, and audit trails).
- Verifying the applications as per the terms and conditions of the TCS-CA CPS, and upon successful verification, requesting the TCS-CA to generate a Digital Signature Certificate for the respective Applicants
- Receiving and verifying the requests for Digital Signature Certificate suspension, activation and revocation from the Subscribers and upon successful verification, forwarding the request, with its advice, to the TCS-CA.
- Creating and maintaining an accurate audit trail of all operations.
- Ensuring that all aspects of services, operations and infrastructure related to Digital Signature Certificate issuance under the TCS-CA Trust Network are performed in accordance with the requirements, representations and warranties of this CPS.
- Rejecting Digital Signature Certificate applications in the event the Applicant does not indicate acceptance of obligations as per CPS or inaccurate information furnished by the Applicant.
- Additional obligations as set forth in the individual Sub-CA agreements that TCS-CA has entered into with the partner concerned.

The partner for whom Sub-CA has been created shall not:

- Be responsible if the Subscriber's password is compromised and a request for Suspension, Revocation or Activation is placed on the Subscriber's behalf.
- Be obliged to inform users of revocation of their Digital Signature Certificates in case of the request being initiated by the Subscribers themselves. In case of request being initiated by TCS-CA, the Subscriber shall be informed of the action being taken.

2.1.3 RA Obligations

An RA shall be responsible for the following:

- Receiving the prescribed applications for the Digital Signature Certificates from the Applicants.

- Verifying the applications as per the terms and conditions of the TCS-CA CPS, and upon successful verification, recommending the generation of Digital Signature Certificates for the respective Applicants
- Receiving and verifying the requests for Digital Signature Certificate suspension, activation and revocation from the Subscribers and upon successful verification, advising the concerned TCS-CA, whether or not to carry out the request.
- Creating and maintaining an accurate audit trail of all RA operations.
- Rejecting Digital Signature Certificate applications in the event the Applicant does not indicate acceptance of obligations as per CPS or inaccurate information furnished by the Applicant.
- Additional obligations as set forth in the individual RA/Sub-CA agreements

The RA will in certain cases also:

- Notify the Subscribers when their Digital Signature Certificate expires in advance of 30 days.

The RA shall not:

- Be responsible if the Subscriber's password is compromised and a request for Suspension, Revocation or Activation is placed on the Subscriber's behalf.
- Be obliged to inform users of revocation of their Digital Signature Certificates in case of the request being initiated by the Subscribers themselves. In case of request being initiated by RA the Subscriber shall be informed of the action being taken.

2.1.4 Subscriber's Obligations

The Subscriber shall have the following obligations:

- Providing the correct information without any errors, omissions or misrepresentations in the application.
- Generating the key pair (except in case of Encryption Certificate) on a secure medium as specified in the TCS-CA CPS.
- Using the Digital Signature Certificate only for the authorized purposes as specified in this CPS.

- Protecting the private key in a secure medium.
- Demonstrate acceptance of the Digital Signature Certificate which has been issued under the TCS-CA Trust Network when all information contained in the Digital Signature Certificate is as applied for and validated as true.
- Notifying immediately any change in the information included in the Subscriber's Digital Signature Certificate that shall make the information in the Certificate inaccurate or misleading.
- Notifying immediately any suspected or actual compromise of the Subscriber's private key.
- Terminating the use of the Digital Signature Certificate if the information in the Certificate is found to be inaccurate and misleading.
- Additional obligations as mentioned in the Subscriber agreement.

2.1.5 Relying Party Obligations

The Relying party shall be obliged to the following:

- Any relying party seeking to rely upon a Digital Signature Certificate is solely responsible for deciding whether or not to rely upon the said Digital Signature Certificate.
- In the case of verifying a Digital signature, the relying party should check that the Digital Signature Certificate was valid and the Digital Signature Certificate status was not revoked at the time that the Digital Signature in question was affixed.
- In the case of encrypting data for a subscriber, the relying party should check that the Digital Certificate is valid and the Certificate status is not revoked at the time that the encryption is carried out.
- Using the Digital Signature Certificate only for purposes that are specified in this TCS-CA CPS and avoiding unauthorized, illegal uses of the Digital Signature Certificate.
- Verifying the Digital Signature Certificate and its chain of trust before using it for the authorized purposes.
- Verifying the Signature as specified in this TCS-CA CPS before trusting the Digital Signature Certificate.
- May rely on a valid Digital Signature Certificate issued under the TCS-CA Trust Network and under this CPS for the purpose of verifying the Digital Signature only if:

- The relying party acknowledges the obligation under this CPS.
- The relying party acknowledges the limitation in liability of the TCS-CA or RA as well as any warranty disclaimer that may apply.

- Additional obligations as mentioned in the Relying Party agreement.

2.1.6 Repository Obligations

- The TCS-CA repository shall publish the TCS-CA CPS, Digital Signature Certificates, Trust Chain and CRLs issued under the TCS-CA Trust Network in the Repository, updating them whenever changes are made.

2.1.7 Loss Limitations

2.1.7.1 Liability Caps

- In no event will the aggregate liability of the TCS Certifying Authority to all parties (including without limitation a Subscriber, an Applicant or a Relying party) exceed the applicable liability caps for such Digital Signature Certificates, as specified in the TCS-CA CPS. The current liability caps are:

  - Class 1 Digital Signature Certificates - No liability
  - Class 2 Digital Signature Certificates - Rs. 5000 /- (Rupees Five thousand only)
  - Class 3 Digital Signature Certificates - Rs. 10,000 /- (Rupees Ten thousand only)

- In no event shall the TCS-CA or the RA be liable for any indirect, incidental, special, consequential, punitive, reliance, cover or liquidated damages, including but not limited to loss of profits, revenue, data or use, incurred by the other party, and resulting from the services provided under the TCS-CA Trust Network.

2.1.7.2 Other exclusions

The TCS-CA or the RA is not liable for any loss if

- The private key associated with the public key in the TCS-CA or any RA Digital Signature Certificate is compromised.
- The Digital Signature Certificates under the TCS-CA Trust Network are issued as a result of the errors, misrepresentations or omissions by the Subscribers.
- The Digital Signature Certificate used in communications has expired or has been revoked or suspended.
- The Subscriber failed to stop using the Digital Signature Certificate after change in the Digital Signature Certificate status or Digital Signature Certificate information was made.
- The Subscriber breached the TCS-CA CPS or Subscriber's Obligations.
- The Relying Party breached the TCS-CA CPS or Relying Party's Obligations.

2.2 LIABILITIES

The TCS-CA or RA shall not be liable in any way, for any inaccuracy, error, delay or omission in the issuance or validation of any Digital Signature Certificate, or for non-performance including suspension, activation and revocation or the failure to suspend, activate or revoke, due to any cause beyond the TCS-CA or RA's reasonable control.

The TCS-CA or the RA shall have no liability to a Subscriber, arising from or relating to issuance, administration or use of a Digital Signature Certificate under the TCS-CA Trust Network that is issued or continued in force in reliance upon or as a result of any false or misleading information provided by the Subscriber or any material omission in any information provided by the Subscriber in connection with their application for Digital Signature Certificate under the TCS-CA Trust Network or otherwise.

2.2.1 CA Liabilities

2.2.1.1 Warranties

TCS-CA warrants

- To provide the Digital Signature Certification services such as TCS-CA Repository.
- To provide the PKI architecture for operating as CA as specified in this TCS-CA CPS.
- That the RAs established by TCS-CA shall perform the validation of the Digital Signature Certificate management as per the CPS.
- That the RAs appointed by TCS-CA or by any Partner for whom Sub-CA has been created shall perform the validation of the Digital Signature Certificate application as per the CPS.
- The issuance of Digital Signature Certificates to the validated Applicants as specified in this TCS-CA CPS.
- A Digital Signature Certificate will be revoked by close of business day for revocations placed online by subscriber from his/her user login and if the request

for revocation is received vide email/letter, verification of a revocation request is made and the revocation will be done on the following business day, but action on a revocation request made over a weekend or holiday may be delayed until the following business day of the RA. To activate the Subscriber's Digital Signature Certificate within 1 week of receipt of valid request from the RA to activate a particular Digital Signature Certificate of a Subscriber.

- To publish the user accepted Digital Signature Certificates in the TCS-CA Repository.
- To put the revoked/suspended Digital Signature Certificates in the Repository.
- To generate a TCS-CA CRL with suspended, activated and revoked Digital Signature Certificates and publish the updated CRL to the TCS-CA repository as specified in Section 4.8 of this CPS.

2.2.1.2 Limitations on warranties

TCS-CA has made all reasonable attempts to ensure that the software has been designed, developed and tested in accordance with best practices followed in the industry. However,

- TCS-CA disclaims all other warranties except as explicitly stated in this TCS-CA CPS.
- TCS-CA provides limited warranty as per this CPS to the reliability of the technique used in generation and storage of the private key of TCS-CA.

2.2.2 Liabilities of partner for whom Sub-CA has been created

2.2.2.1 Warranties

The partner for whom Sub-CA has been created warrants that it will

- Forward the verified Applicant's request for issuing a Digital Signature Certificate to the TCS-CA.
- Send a request to the TCS-CA to suspend, activate or revoke a Digital Signature Certificate.

- Activate the Subscriber's Suspended Digital Signature Certificate within 1 week of receipt of valid request from the RA to activate a particular Digital Signature Certificate of a Subscriber.

2.2.2.2 Limitations on warranties

The partner for whom Sub-CA has been created has made all reasonable attempts to ensure that the software has been designed, developed and tested in accordance with best practices followed in the industry, if applicable. However,

- Partner for whom Sub-CA has been created disclaims all other warranties except as explicitly stated in this TCS-CA CPS.
- Partner for whom Sub-CA has been created provides limited warranty as per this CPS to the reliability of the technique used in generation and storage of the private key.

2.2.3 RA Liabilities

The following responsibilities and liabilities of the TCS-CA or RA are discharged by the RA on behalf of the TCS-CA and in accordance with the separate "RA Agreement" entered into with the TCS-CA. Among other duties and responsibilities specified in the "RA Agreement", the TCS-CA expects the RA to fulfill the following:

- Provide an opportunity to an Applicant to submit a request for Digital Signature Certificates.
- Perform verification of the details in the application given by the Applicant for obtaining a Digital Signature Certificate.
- Forward verified Applicant's request for issuing a Digital Signature Certificate to the TCS-CA.
- Send a request to the TCS-CA to suspend, activate or revoke a Digital Signature Certificate.
- The warranties, disclaimers of warranty, and limitations of liability between the TCS-CA and the RAs are set forth and governed by the RA/Sub-CA agreements between them.

2.3 FINANCIAL RESPONSIBILITY

The TCS-CA or RA does not make any representation and does not give any warranties on the financial transactions which the Subscribers and the relying parties perform using the Digital Signature Certificate obtained under the TCS-CA Trust Network. The Subscribers and the relying parties shall be responsible for any losses, damages or any consequences due to such transactions.

2.3.1 Indemnification by the Subscriber

By accepting a Digital Signature Certificate, the Subscriber agrees to fully indemnify and hold the TCS-CA and/or the RAs, harmless at all times from any acts or omissions resulting in liability, any loss or damage and any suits and expenses of any kind, that the TCS-CA and/or the RA may incur, that are caused by the use or publication of a Digital Signature Certificate, and that arises from

- Error, misrepresentation or omission made by the Subscriber while applying for Digital Signature Certificate under the TCS-CA Trust Network.
- Modification to the information contained in the Digital Signature Certificate by the Subscriber.
- Using the Digital Signature Certificate for the purposes other than permitted for the corresponding class of the Certificate.
- Failure in protecting the Subscriber's private key corresponding to the public key in the Digital Signature Certificate leading to a compromise of the Subscriber's private key.

2.3.2 Indemnification by the Relying Parties

The relying party shall indemnify and hold the TCS-CA and RAs, harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind that the TCS-CA and the RA may incur, that are caused by the use or publication of a Digital Signature Certificate and that arises from:

- Lack of proper validation of the Digital Signature Certificates done by the relying parties before using the Certificates.
- Relying on Digital Signature Certificates that have expired or revoked and are no longer valid.

- Using Digital Signature Certificates for purposes other than those permitted for the corresponding classes of Certificates.

2.3.3 Fiduciary Relationships

This TCS-CA CPS, the Subscriber agreement, the Sub-CA/RA do not constitute fiduciary, partner, agent, trustee, or legal representative among the parties involved in the TCS-CA Digital Signature Certification Services under the TCS-CA Trust Network.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Governing Law

The laws of the Government of India, the Information Technology Act and the Information Technology rules framed by the Government of India and the rules and regulations specified by the Controller of Certifying Authorities, Ministry of Communications and Information Technology, Department of Information Technology, Government of India shall govern the construction, validity, enforceability and performance of the TCS-CA Trust Network Certification Practice Statement.

2.4.2 Severability, Survival, Merger, Notice

To the extent permitted by applicable law, Subscriber Agreements, Agreements and Relying Party Agreements under the TCS-CA Trust Network shall contain severability, survival, merger, and notice clauses.

A severability clause in an agreement prevents any determination of the invalidity or enforceability of a clause in the agreement from impairing the remainder of the agreement. A survival clause specifies the provisions of an agreement that continue in effect despite the termination or expiration of the agreement. A merger clause states that all understandings concerning the subject matter of an agreement are incorporated in the agreement. A notice clause in an agreement sets forth how the parties are to provide notices to each other.

2.4.2.1 Severability

If any provision of this CPS is, for any reason and to any extent, found to be invalid or unenforceable, the remainder of this CPS shall be interpreted so as best to reasonably effect the intent of its parties.

It is expressly understood and agreed that each and every provision of this CPS that provides for a limitation of liability, disclaimer or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

2.4.2.2 Survival

The obligations and restrictions contained within CPS (Audit, Confidential Information, Obligations of the TCS-CA and the RA under the TCS-CA Trust Network, and Limitations upon Such Obligations) shall survive the termination of this CPS.

2.4.2.3 Merger

Should TCS-CA or RA merge with another entity, the obligations and restrictions (Audit, Confidential Information, Obligations of the TCS-CA and the RA, and Limitations upon Such Obligations) shall be borne by the new entity thus created by the merger.

2.4.2.4 Notice

Whenever any person hereto desires or is required to give any notice, demand, or request with respect to this CPS, such communication shall be made either using Digitally signed messages consistent with the requirements of this CPS or in writing and duly signed. Communications in writing must be delivered by a courier service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

To TCS-CA:	Tata Consultancy Services Limited - Certifying Authority **deccan**park, 1 – Software Units Layout, Hyderabad – 500 081 Andhra Pradesh, India

By TCS-CA:	To the most recent address of record on file with TCS-CA.

2.4.3 Dispute Resolution Procedures

As specified in the IT Act prescribed by the Ministry of Communications and Information Technology, Department of Information Technology, Government of India, all the disputes among TCS-CA, the Subscribers and the relying parties shall be referred to the CCA for arbitration or resolution.

Disputes between TCS-CA and any one of its Partner for whom Sub-CA has been created and/or RAs in the TCS-CA Trust Network shall be resolved pursuant to provisions in the applicable agreement between the parties.

Additionally, to the extent permitted by applicable law, the Subscriber Agreements and Relying Party Agreements under the TCS-CA Trust Network shall contain a dispute resolution clause.

2.5 FEES

2.5.1 Digital Signature Certificate Issuance Fees

The current fees for Digital Signature Certificate issuance under the TCS-CA Trust Network are as follows:

2.5.1.1 For Digital Signature Certificates other than Server Certificates

For details of fees for Digital Signature Certificates other than Server certificates please visit our website www.tcs-ca.tcs.co.in .
The prices are subject to change and any such change shall be published on the TCS-CA Trust Portal immediately.

2.5.1.2 For Server Certificates

For details of fees for Digital Certificates other than Server certificates please visit our website www.tcs-ca.tcs.co.in .
The prices are subject to change and any such change shall be published on the TCS-CA Trust Portal immediately.

2.5.2 Digital Signature Certificate Access Fees

No fee is charged for Digital Signature Certificate access.

This is subject to change and any such change shall be published at the TCS-CA Trust Portal immediately.

2.5.3 Revocation or Status Information Access Fees

No fee is charged for Digital Signature Certificate revocation or status information access.

This is subject to change and any such change shall be published on the TCS-CA Trust Portal immediately.

2.5.4 Fees for Other Services such as Policy Information

No fee is charged for other services like online access to policy information such as this Certification Practice Statement. A fee of Rs. 2,000/- (Rupees Two Thousand only) shall be charged for a printed version of Certification Practice Statement.

This is subject to change and any such change shall be published at the TCS-CA Trust Portal immediately.

2.5.5 Refund Policy

The TCS-CA Trust Network does not provide any refund of the fees paid for the Digital Signature Certificates or services provided.

The TCS-CA or RA may refuse to issue a Digital Signature Certificate to any person, at its sole discretion, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. Upon a refusal to issue a Digital Signature Certificate, the TCS-CA or RA shall refund to any Digital Signature Certificate Applicant any paid Digital Signature Certificate enrolment fee, unless the Digital Signature Certificate Applicant submitted fraudulent or falsified information to the TCS-CA or RA. In such a case the fee shall not be refunded.

2.6 PUBLICATION AND REPOSITORY

TCS-CA shall maintain the repository to store information relevant to the operations of the TCS-CA Public Key Infrastructure Services under the TCS-CA Trust Network. This shall include the digital signature certificate trust chain of TCS-CA. All the information and modifications are published in the repository to provide access to the updated information. This information is subject to changes and any such change shall be published in the TCS-CA repository as detailed in other relevant sections of this CPS.

2.7 PUBLICATION OF TCS-CA INFORMATION

The following information is published in the TCS-CA repository

- The TCS-CA Trust Network Certification Practice Statement.
- The Digital Signature Certificates issued under the TCS-CA Trust Network on acceptance by the respective subscribers.
- The Digital Signature Certificates and public keys corresponding to the respective private keys of the TCS-CA, Partner for whom Sub-CA has been created and ,RAs
- The CRL for the Digital Signature Certificates revoked or suspended by the TCS-CA. The CRL shall be updated frequently as mentioned in this CPS and updated in the Repository.

2.7.1 Frequency of Publication

The TCS-CA CPS is published as per the policy set forth in the Section 8 of the TCS-CA CPS.

2.7.2 Access Controls

The TCS-CA CPS that is published at the TCS-CA Trust Portal is accessible to the Certifying Authority, all Partners for whom Sub-CA has been created, all Registration Authorities, Subscribers under the TCS-CA Trust Network, Applicants, and Relying Parties.

The TCS-CA CPS can be modified by TCS-CA with the approval of the CCA as defined in Section 8 of this CPS.

2.7.3 Repositories

The TCS-CA repositories are maintained by TCS-CA and are accessible to authorized personnel. The TCS-CA repositories are updated periodically as specified in this TCS-CA CPS with relevant information sent to the CCA as per the IT Act, 2000. The TCS-CA repositories are the source for the most current CRL and other information regarding Digital Signature Certificates issued under the TCS-CA Trust Network.

2.8 COMPLIANCE AUDIT

The TCS-CA and RAs under the TCS-CA Trust Network shall implement and preserve an audit trail of all material events, such as key generation and Digital Signature Certificate application, validation, suspension, and revocation and other audit records for the relevant time period as specified in Section 4.10.3.

The TCS-CA shall be audited for compliance with the procedures specified in the TCS-CA CPS as well as the provisions of the IT Act, 2000, its Rules, Regulations and Guidelines.

The Partner for whom Sub-CA has been created and the RAs shall be audited by TCS-CA for compliance with the procedures specified in the TCS-CA CPS.

2.8.1 Frequency of Entity Compliance Audit

The TCS-CA Trust Network shall be audited for compliance with the procedures specified in the TCS-CA CPS. The frequency of the audit shall be done annually as specified in the IT Act, 2000 as well as the provisions of the IT Act, 2000, its Rules, Regulations and Guidelines by:

- The empanelled external auditor who is recognized by the Controller of Certifying Authorities for the TCS-CA and
- TCS-CA for the Partner for whom Sub-CA has been created and the RAs under the TCS-CA Trust Network, as applicable.

In addition, a periodic internal audit shall also be conducted, with a frequency not less than once in 6 months, to ensure compliance with documented processes, recommend revision of these processes if deemed necessary for any reason, and to assure top management of the smooth and efficient functioning of TCS-CA Trust Network.

2.8.2 Topics Covered by Audit

The auditor shall examine all procedures and operations of the TCS-CA performing the Certification Services for compliance with the IT Act, 2000 Rules, Regulations, Guidelines and practices specified in this CPS and prepare audit reports.
TCS-CA shall conduct half yearly internal audit of the security policy, physical security, planning of its operations and the repository. The annual audit shall include, *inter alia*:

- Security policy and planning
- Physical security
- Technology evaluation
- Certifying Authority's services administration
- Relevant TCS-CA CPS
- Compliance with the relevant TCS-CA CPS
- Contracts/Agreements
- Regulations prescribed by the controller
- Policy requirements of Certifying Authority Rules, 2000
- Changes/Additions in physical controls such as site location, access, etc.
- Re-deployment of personnel from an approved role/task to a new one
- Appropriate security clearances for outgoing employees such as deletion of keys and revocation of access privileges

The audited party shall follow approved procedures to ensure that its activities are recorded and made available during audits.

2.8.3 Identity/Qualifications of Auditor

The empanelled external auditor, who is recognized by the Controller of Certifying Authorities, shall perform the audit.

TCS top management shall decide the composition of the internal audit team, when an audit for TCS-CA becomes due.

2.8.4 Auditor's Relationship to Audited Party

The auditing firm involved in the preparing the audit reports shall be independent of the party being audited and shall not be a software or hardware vendor which is, or has been providing services or supplying equipment to the party being audited. The auditing firm and the party being audited shall not have any current or planned financial, legal or other relationship, other than that of an auditor and the audited party.

2.8.5 Actions taken as a Result of Deficiency

On receipt of the audit findings, the audited parties shall take preventive and corrective actions to correct the deficiency within reasonable and agreed upon timeframes.

2.8.6 Communication of Results

After commencement of the operations by the CA, CA shall communicate the results of the periodic audits by the empanelled auditors concerning the state of practices and procedures in the audited party, to the CCA within 4 weeks of completion of audit.

2.9 CONFIDENTIALITY

All information collected, generated, transmitted, and maintained by the TCS-CA and/or RA is considered confidential, except for information that

- Is posted to TCS-CA's website/ Trust Portal
- Is in the possession of Subscriber, except information which has been received under an obligation of confidentiality agreed to by the TCS-CA and/or RA in a written agreement, or
- Is or becomes publicly available.

The TCS-CA and the RAs under the TCS-CA Trust Network and PKI Services shall take reasonable care in protecting the information from being disclosed or used for purposes other than specified in this TCS-CA CPS.

Access to confidential information by operational staff of the TCS-CA shall be on a need-to-know and a need-to-use basis. Paper-based records, documents and backup data containing confidential information shall be kept safely and securely, and away from other (non-confidential) data.

The confidential information shall not be taken out of the country except where a properly constitutional warrant or other legally enforceable document is produced to the Controller and only after the CCA permits TCS-CA to do so.

The TCS-CA and the RAs under the TCS-CA Trust Network and PKI Services shall not disclose the information provided by the Applicant/Subscriber, unless otherwise specified elsewhere within this Section 2.9 of the CPS.

2.9.1 Types of Information to be Kept Confidential

The following information shall be considered confidential and may not be disclosed except as specified in this TCS-CA CPS.

- CA application records, whether approved or disapproved.
- All transaction records between parties.
- Contingency planning and disaster recovery plans.
- Security measures controlling the operations of the TCS-CA and and the RAs
- All information provided by the Applicant/Subscriber, that is not part of the respective Digital Signature Certificate or the repository or any other publicly accessible information.
- Audit trail records of the TCS-CA and RAs operations.
- All Audit reports.
- Transactional data related to Subscribers' activities on the TCS-CA Trust Portal.
- Data in transit between the Subscriber and servers under the TCS-CA Trust Network (this is achieved by using an SSL-enabled web server supporting HTTPS transactions).

However, data on the usage of the Digital Signature Certificates which do not relate to the TCS-CA and RA activities cannot be protected because such usage happens outside the TCS-CA Trust Network system, for example between a customer and a relying party.

2.9.2 Types of Information not Considered Confidential

The following information shall not be considered confidential except as specified in this TCS-CA CPS.

- Information contained in the Digital Signature Certificate.
- Information contained in the CRL.
- Information contained in the TCS-CA CPS.

2.9.3 Disclosure of Suspension/Revocation Information

TCS-CA shall publish the Digital Signature Certificate revocation/suspension details of all the Digital Signature Certificates revoked/suspended under the TCS-CA Trust Network. The Digital Signature Certificates revoked/suspended after verification of revocation/suspension request by the RA will be added to the TCS-CA and/or the Partner for whom Sub-CA has been created CRL that shall be published and updated at the TCS-CA Trust Portal. Revocation of Digital Signature Certificates shall be only for due cause. The reasons for the revocation shall be disclosed only to the Subscriber or to the agencies having the power to compel the disclosure.

2.9.4 Release to Law Enforcement Officials

The TCS-CA and the RAs under the TCS-CA Trust Network and Digital Signature Certification Services shall release the confidential information to law enforcement officials in compliance to an order from a Court or Tribunal or any Government or public authority having the power to compel the disclosure.

2.9.5 Release as Part of Civil Discovery

The TCS-CA and the RAs operating may disclose information that is normally considered to be confidential during any judicial, arbitration, litigation or administrative proceedings. The TCS-CA and the RAs shall make reasonable efforts to protect those information using the court of law by restricting the disclosure of the information to the extent reasonably required by any such judicial, arbitration, litigation or administrative proceedings.

2.9.6 Disclosure upon Owner's Request

The TCS-CA and the RAs shall disclose the information provided by the Applicant/ Subscriber to whom the TCS-CA and/or RA is obliged to keep such information confidential upon the request from such Applicant/ Subscriber to do so.

2.10 INTELLECTUAL PROPERTY RIGHTS

2.10.1 Subscribers

The TCS-CA and the RAs shall comply with Applicant's/Subscriber's information protection as per the IT Act, 2000. The information supplied by the Applicant/Subscriber is the property of the respective Applicant/Subscriber. All Applicants/Subscribers shall grant to the TCS-CA and the RAs a non-exclusive, world-wide, paid-up, royalty-free license to use, copy, modify, publish and distribute such information subject to Applicant/Subscriber's information protection as per the IT Act, 2000.

2.10.2 Tata Consultancy Services Limited – Certifying Authority

TCS-CA shall grant to the Subscribers and the relying parties a non-exclusive, non-transferable license to use, copy and distribute the Digital Signature Certificates issued under the TCS-CA Trust Network provided that:

- The Digital Signature Certificates are used as specified in this TCS-CA CPS, Subscriber agreement.
- The Digital Signature Certificates are reproduced fully and accurately.
- The Digital Signature Certificates are not published in the publicly available databases, Repositories and the directories without the express written permission of TCS-CA.

TCS-CA grants permission to reproduce the TCS-CA CPS provided,

- The copyrights notice being retained in all the copies of the TCS-CA CPS.
- The TCS-CA CPS is reproduced fully and accurately.

2.11 DIGITAL SIGNATURE CERTIFICATE CLASSES

TCS-CA Trust Network supports three distinct Digital Signature Certificate classes as defined in the TCS-CA CPS. Each class provides for a different level of verification and hence a designated level of trust. The following subsections describe each Certificate class.

TCS-CA does not endorse or recommend the usage of Digital Signature Certificates of any particular class, issued under the TCS-CA Trust Network, for any particular application or purpose. TCS-CA wishes to reaffirm that it is up to a relying party and/or application service provider to decide which particular class of Digital Signature Certificate is acceptable for any given application.

2.11.1 Class 1 Digital Signature Certificates

Description: Class 1 Digital Signature Certificates are issued to individuals, business and government organizations. Class 1 Digital Signature Certificates confirm that a user's name (or alias) and e-mail address form an unambiguous subject name within the TCS-CA repository. Class 1 Digital Signature Certificates are sent electronically to Subscribers and added to their set of available Certificates. They can be used for Web browsing and personal e-mail, to enhance the security of these environments.

Assurance level: Class 1 Digital Signature Certificates do not facilitate the authentication of the identity of the Subscriber. The only verification is a simple check of the non-ambiguity of the common name and email id combination within the TCS-CA repository, plus a limited verification of the e-mail address.

These Digital Signature Certificates provide the lowest level of assurance of all Digital Signature Certificates under the TCS-CA Trust Network. They are not intended for commercial use where proof of identity is required and shall not be relied upon for such uses. TCS-CA does not make any representation and does not give any warranties regarding the identity of the subscriber or any consequences, which the Subscribers and the relying parties may face or potentially face using the Class 1 Digital Signature Certificate obtained from the TCS-CA Trust Network.

2.11.2 Class 2 Digital Signature Certificates

Description: Class 2 Digital Signature Certificates are issued on recommendation by non TCS-RAs to individuals, representatives of business and government organizations. Non TCS-RAs assume the responsibility of verifying the accuracy of the information submitted by an applicant. In the case of a Class 2 Digital Signature Certificates, the verification of the details supplied with the request for a Digital Signature Certificate is carried out by the RA, as applicable.

From a functional standpoint there is no difference between a Class 2 Digital Signature Certificate and a Class 3 Digital Signature Certificate. The only difference is that in the case of a Class 2 Digital Signature Certificate the verification process used prior to issuing a Certificate is carried out by a non TCS-RA

2.11.3 Class 3 Digital Signature Certificates

Description: Class 3 Digital Signature Certificates are issued to individuals, representatives of business and government organizations.

- **To individuals** – Class 3 Digital Signature Certificates provide important assurances of the identity of individual Subscribers by requiring their personal (physical, if required) appearance before an RA. Personal details such as Name, PAN, Address, Passport details will be verified by the RA and after confirmation of facts it will recommend the application to TCS-CA for the issuance of a Digital Signature Certificate. The private key corresponding to the public key contained in a Class 3 Digital Signature Certificate must be generated and stored in a trustworthy manner according to applicable requirements.

- **To organizations** – Class 3 Digital Signature Certificates can provide assurances of the existence and name of various public and private sector organizations (such as government agencies and corporations).

Class 3 Digital Signature Certificates are used by TCS-CA Subscribers for electronic commerce applications/transactions such as electronic banking, electronic data interchange (EDI), and membership-based online services.

Assurance level: Individual Class 3 Digital Signature Certificate processes use various procedures to obtain evidence of the identity of individual and organization Subscribers. These validation procedures provide stronger assurances of an Applicant's identity than Class 2 Digital Signature Certificates.

2.12 SINGLE KEY PAIR

The TCS-CA and the RAs under the TCS-CA Trust Network implement the Single Key pair concept in Digital Signature Certificates issued in accordance with the IT Act.

2.13 DUAL KEY PAIR

The TCS-CA and the RAs under the TCS-CA Trust Network implement the Dual Key pair concept in Digital Signature Certificates issued in accordance with the IT Act. A Subscriber wishing to use encryption must obtain an encryption Certificate in order to do so. In such cases the Subscribers will have two distinct private/public key pairs. One private/public key pair is solely used for encrypting electronic data and the other private/public key pair shall be used for signing electronic data.

2.13.1 Encryption Key Pair

The sender uses the Subscriber's public key, available in the Digital Certificate of the Subscriber, to encrypt data to be sent to the Subscriber. The Subscriber decrypts the encrypted data using his private key that resides in his browser, token, smart card etc., as the case may be.

A copy of the private/public key pair of the Subscriber shall be retained with the safe custody of the TCS-CA. The TCS-CA shall generate the private/public key pair of the Subscriber on receiving the verified request from the corresponding RA and send the Digital Certificate and key pair through a secure channel to the Subscriber.

The generation of the encryption key pair shall be in conformity with the Indian Telegraph Act and all other relevant parts of the Indian legal system.

2.13.2 Signing Key Pair

The Subscriber uses the signing key pair for digitally signing all electronic data that the Subscriber wishes to authenticate. The Subscriber generates the signing private/public key pair on a trustworthy medium and assumes the responsibility for safeguarding the private key. The Subscriber applies to the RA by submitting a request and obtains a Digital Signature Certificate from the TCS-CA as specified in this TCS-CA CPS to confirm the accuracy of the Subscriber's public key. The Subscriber may enclose a copy of this Digital Signature Certificate with all communication. The recipient/relying party shall use the public key in the Certificate to verify the Signature of the Subscriber as specified in the TCS-CA CPS.

3 IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

The initial registration process by the Applicant includes the submission of the online application for issuing Digital Signature Certificate along with the supporting documents by the Applicant and the applicable verification by the RA of the information submitted by the applicant.

3.2 DIGITAL SIGNATURE CERTIFICATE CLASSES AND RAS

TCS-CA issues 3 classes of Digital Signature Certificates (see Section 2.11). A Digital Signature Certificate has to be obtained by applying to a RA, as applicable. There are two kinds of RAs: TCS-RA and non-TCS-RA.

A TCS-RA is an RA that is part of TCS, the parent organization of TCS-CA. A TCS-RA shall only ordinarily process Class 1 and Class 3 Digital Signature Certificates.

A non-TCS-RA under the TCS-CA/Partner for whom Sub-CA has been created is an RA of an organization that has an agreement with TCS-CA to facilitate its employees or other affiliates obtaining Digital Signature Certificates in a more streamlined manner. A non-TCS-RA under the TCS-CA/Partner for whom Sub-CA has been created can only issue Class 2 Digital Signature Certificates.

3.3 OBTAINING CLASS 1 DIGITAL SIGNATURE CERTIFICATES

A Class 1 Digital Signature Certificate application can only be verified by a TCS-RA.

- The Applicant logs in to the TCS-CA Trust Portal to self-register and generates the Digital Signature Certificate request (and key pair) preferably in a secure medium.
- User fills the online request form.
- RA verifies the non-ambiguity of the common name and email Id combination mentioned in the online request form and the request is forwarded to CA to issue a Digital Signature Certificate.
- Limited email verification is achieved by sending the authentication pin to the email id mentioned in the online request form and it is this email id which forms the email id field in the certificate.
- CA issues the Digital Signature Certificate. This can only be downloaded by presenting the authentication pin

Non-TCS RAs cannot verify applications for Class 1 Digital Signature Certificates.

3.4 OBTAINING CLASS 2 DIGITAL SIGNATURE CERTIFICATES

Class 2 Digital Signature Certificate applications shall only be ordinarily verified by non TCS-RAs

A RA organization shall have policies governing who is eligible to be recommended for getting Digital Signature Certificates. For example, such a policy could say that senior managers and above are eligible to obtain Digital Signature Certificates. It need not be restricted to employees – as long as the rules are clear and the verification of someone's eligibility is unambiguous, any affiliated entity could apply for a Digital Signature Certificate. The policy would also govern approved usage of Digital Signature Certificates so obtained.

TCS-CA would have an Agreement with such partners (the "Sub-CA/RA Agreement")

When an Applicant wishes to obtain a Digital Signature Certificate:

- The Applicant would approach the RA with his/her details
- The RA would verify (using the policies described earlier) eligibility and authenticate the applicant details, and create a user-id on the system
- The Applicant registers and generates the Digital Signature Certificate request (key pair) in a secured manner
- The RA operator/administrator at the non-TCS RA concerned shall then verify the details submitted
- If verified successfully the RA Administrator would recommend the Digital Signature Certificate request for generation
- TCS-CA issues the Digital Signature Certificate based upon the request approved by RA

The details given in the application form (see Section 12) are verified against supplied documentary evidence, and depend on whether the Applicant is an individual, organization, etc.

In certain cases based on a need felt by TCS-CA/RA, the procedures may include validation based on a comparison of information submitted by the Digital Signature Certificate Applicant against information in business records or trusted third party databases or the database of a TCS-CA approved identity-proofing service. TCS-CA reserves the sole right to approve such databases or record being used for this validation.

TCS RAs shall not ordinarily verify applications for Class 2 Digital Signature Certificates.

3.5 OBTAINING CLASS 3 DIGITAL SIGNATURE CERTIFICATES

A Class 3 Digital Signature Certificate application can only be verified by a TCS-RA.

- The Applicant logs in to the TCS-CA Trust Portal to self-register and generates the Digital Signature Certificate request (and key pair) preferably in a secure medium
- The Applicant submits all supporting documents to the RA.

3.5.1 Individual Applicant

Once the application has been filled out, the individual Applicant needs to be present (physical presence, if required) at RA with at least one of the following original documents:

- Passport
- Voter's ID
- Bank Account Details
- Driver's license
- Ration Card
- Any Other
- **(OR)** domain registration Certificate in case of server Certificate.

RA shall verify all the details that are marked as "mandatory" by the IT Act, 2000. (See Section 12 of the CPS).

3.5.2 Company Applicant

- The representative of a "Company" Applicant needs to meet (physical presence, if required) with RA official with the proof of ownership of the name and other details (as in Section 3.6.7).
- The Applicant needs to submit at least one of the following:
    - Passport
    - Voter's ID card
    - Income Tax PAN Card
    - Identity Card – Attested by Authorized signatory of the company
    - Driver's License
    - Ration Card
    - **(OR)** domain registration Certificate in case of server Certificate.
    - In case a "Server Certificate" is being applied for, proof of Domain name registration will also be required.

3.5.3 Government Applicant

- The representative of a "Government" Applicant needs to be present (physical presence, if required) at RA official with the proof of ownership of the name and other details. The Applicant needs to submit the following
    - Name of the Organization
    - Administrative Ministry/ Department.
    - Address
    - In case a "server Certificate" is being applied for, proof of Domain name registration will also be required.
    - The Applicant needs to submit at least one of the following:
        - Passport
        - Voter's ID card
        - Income Tax PAN Card
        - Government Identity Card – Attested by Authorized signatory in the Government organization.
        - Driver's License
        - Ration Card
        - **(OR)** domain registration Certificate in case of server Certificate.
        - Letter of Authority from Head of Office or JS (Admn.) for Govt Sector / Superior Authority for Banking Sector of Applicant

- Based on the above details submitted the RA forwards the request to CA.
- CA issues a Digital Signature Certificate based on RA recommendation.

Notes

- If the Applicant/Subscriber requires an Encryption Certificate, then (a) the Applicant must have previously applied for and been given a "Signing Certificate" which is currently valid, and (b) the Applicant/Subscriber must submit the same details without the public key this time. This is because for an Encryption Certificate, the key pair is generated by TCS-CA and not by the Applicant.
- For Classes 2 and 3, If any of the mandatory information (as specified in Section 12 of this CPS) is not verifiable, this information is deemed to be missing and the application will be rejected.

- TCS-CA reserves the right to decide which specific forms of identification would be acceptable for validation. In the absence of a government-issued identification, TCS-CA may prescribe alternate methods of validation like trusted third party databases or the database of a TCS-CA approved identity-proofing service or other alternatives.

Non-TCS RAs cannot verify applications for Class 3 Digital Signature Certificates.

3.6 NAMES

3.6.1 Types of Names

The names in the Digital Signature Certificates issued under the TCS-CA Trust Network shall comply with the X.500 naming conventions. These Digital Signature Certificates shall use Distinguished Names (DN) to provide the identities to Subscribers, the TCS-CA and the Partner for whom Sub-CA has been created under the TCS-CA Trust Network. The Digital Signature Certificates contain the following types of names.

- Common Name (CN), which is the unique name of the Subscriber.
  (In case of Server Certificates, the Common Name (CN) shall be the fully qualified hostname or path used in the DNS of the World Wide Web server on which the Applicant is intending to install the Web Server Certificate)
- Email address of the Subscriber.
- Organization (O).
- Organizational Unit (OU), which is used to distinguish various organizational groups within the same organization.
- City or Locality (L).
- State or Province (SP), which is an identifier of the state or the province to which the Subscriber belongs.
- Country(C), which is the identifier for the country to which the Subscriber belongs.

3.6.2 Need for Names to be Meaningful

Names used shall identify the person or object to which they are assigned in a meaningful way. This will be automatically ensured because all the details provided (such as person's name, organization's name, etc) are verified.

3.6.3 Rules for Interpreting Various Name Forms

The names shall be interpreted as specified in the section 3.6.1 of this TCS-CA CPS. Other terms, numbers, characters and letters may be appended to existing names to ensure the uniqueness of each name.

3.6.4 Uniqueness of Names

The Distinguished names form the basis for the uniqueness of each assigned name but the same Applicant/Subscriber can have multiple Digital Signature Certificates with the same DNs for different Digital Signature Certificate purposes as specified in the CPS.

The distinguished names should be able to uniquely identify the Subscriber in public Repository in which it is published. Additionally all the Digital Signature Certificates under the TCS-CA Trust Network shall be assigned a unique serial number, which will enable identification, suspension, activation and revocation of the Digital Signature Certificates when required.

3.6.5 Name Claim Dispute Resolution Procedure

The naming convention specified in Section 3.6 is strictly enforced. The TCS-CA and the RA shall resolve any dispute in accordance with this naming convention as specified by the TCS-CA CPS.

3.6.6 Method to Prove Possession of Private Key

The TCS-CA or RA, as applicable, shall have proof that the Applicant/Subscriber possesses the private key corresponding to the public key sought to be certified, and that the private key is usable, by using PKCS#10/SPKAC as the format for obtaining this information from the Applicant.

The RA does the verification to prove the possession of the Applicant/Subscriber's private key with the request submitted by the Applicant/Subscriber as specified by the CPS.

3.6.7 Authentication of Organization Identity

The RAs shall be responsible for verifying the identity of the organization. The RA operating under the TCS-CA Trust Network shall perform appropriate verification of an organization's entity based on the information given in the application form in order for TCS-CA or the RA to establish the bona fides of the organization.

For the TCS-CA or the RA to establish the bona fides of the organization, the organization submitting the application shall submit proof of ownership of the name, such as:

- Company Registration
- Society Registration
- Memorandum of Understanding
- Article of Association
- Documents pertaining to Shops & Establishments Act
- Bank details for a Current Account
- Partnership Deed / Agreement etc

In addition, proof that the person representing the organization is duly authorized to do so, is also required.

3.6.8 Authentication of Individual Identity

The RA operating under the TCS-CA Trust Network shall perform appropriate verification of an individual entity based on the information provided in the application form. The RA shall perform the verification depending on the Digital Signature Certificate classes' type as specified in the TCS-CA CPS. This verification shall take the form of checking the validity and authenticity of details such as passport, PAN card, etc. For class 3 applications, a physical visit of the applicant to the RA may be required.

TCS-CA reserves the right to decide which specific forms of identification would be acceptable for validation. In the absence of a government-issued identification, TCS-CA may prescribe alternate methods of validation by the RA.

3.7 ROUTINE REKEY

The TCS-CA shall not renew the Subscriber's Digital Signature Certificates after the expiration of its Digital Signature Certificate under the TCS-CA Trust Network but requires the corresponding Subscriber to apply for a new Digital Signature Certificate after generating a new private-public key pair preferably on a trustworthy medium and complete the initial registration process once again as specified in the section 3.1 of this TCS-CA CPS.

The corresponding RA may put reasonable efforts to inform the Subscriber in advance about the expiration of the Subscriber's Digital Signature Certificate.

The Subscriber may retain the use of the old encryption key pair for the purpose of decrypting data encrypted with the encryption private-public key pair.

3.8 REKEY AFTER REVOCATION

The TCS-CA shall not renew the Digital Signature Certificates that have been revoked for any Subscriber under the TCS-CA Trust Network. The Subscriber, who further wants to use the Digital Signature Certification Services under the TCS-CA Trust Network, has to apply for a new Digital Signature Certificate after generating a new private-public key pair on a secure medium and complete the initial registration process once again as specified in the section 3.1 of this TCS-CA CPS.

3.9 DIGITAL SIGNATURE CERTIFICATE REPLACEMENT

TCS-CA shall replace the Digital Signature Certificates that the subscriber is unable to download or whose private key is unable to export from the browser free of charge provided the subscriber reports such problem with in the period allowed for free replacement. The Subscriber who wants a replacement has to first initiate revocation of the digital signature certificate and apply for a replacement Digital

Signature Certificate after generating a new private-public key pair on a secure medium and complete the initial registration process once again by submitting the certificate enrollment form.

The digital signature certificate replacement option is available with in 21 days of issuance of digital signature certificate. This time period is subject to change and any such changes shall be published on the TCS-CA Trust Portal from time to time.

4 OPERATIONAL REQUIREMENTS

4.1 DIGITAL SIGNATURE CERTIFICATE APPLICATION

To obtain the Digital Signature Certificate from the TCS-CA Trust Network, the Applicant has to follow the initial registration process specified in the Section 3.1 of this TCS-CA CPS. The RAs operating under the TCS-CA of TCS-CA Trust Network shall perform verification of the information provided by the Applicant to establish their identity.

4.2 DIGITAL SIGNATURE CERTIFICATE ISSUANCE

Upon successful completion of the applicant identification and authentication process in accordance with this CPS, the TCS-CA shall generate the Digital Signature Certificate. No interim Digital Signature Certificate shall be issued.

4.3 DIGITAL SIGNATURE CERTIFICATE ACCEPTANCE

The Digital Signature Certificate of the Subscriber will be considered as accepted by the Subscriber when the corresponding Subscriber downloads the Digital Signature Certificate.

4.4 DIGITAL SIGNATURE CERTIFICATE EXPIRY

Every Digital Signature Certificate shall have an expiry date, after which the Digital Signature Certificate is deemed to be no longer valid and shall be archived. The owner of the Digital Signature Certificate shall not use the Certificate for signing purpose after the expiry. In order to be able to digitally sign, the Subscriber has to re-apply for a fresh Digital Signature Certificate.

4.5 DIGITAL SIGNATURE CERTIFICATE REPLACEMENT

To obtain the replacement Digital Signature Certificate from the TCS-CA Trust Network, the Applicant has to follow the process specified in the Section 3.9 of this TCS-CA CPS. The RAs operating under the TCS-CA of TCS-CA Trust Network shall perform verification of the information provided by the Applicant to establish their identity and recommend to TCS-CA to issue him/her a replacement digital signature certificate.

4.6 DIGITAL SIGNATURE CERTIFICATE REVOCATION

Revocation is the process of making the Applicant's Digital Signature Certificate invalid permanently based on conditions as specified in this CPS.

The RA which has processed the application in respect of any Digital Signature Certificate, has the right to recommend the revocation of such Digital Signature Certificate based on conditions specified in this CPS. The revoked Digital Signature Certificates are added to the TCS-CA and the corresponding CRL to be published and shall not be used again by the Subscriber.

It is the Subscriber's obligation to notify the RA with a request to revoke a Subscriber's Digital Signature Certificate on conditions as specified in this CPS. Upon receipt of such a request, the RA verifies to confirm the revocation request. This verified request is subsequently transmitted to the TCS-CA as applicable, where the revocation request is processed. The RA may also initiate a revocation request without a request from the Subscriber or Participant if the situation warrants it. The TCS-CA itself may also initiate a revocation request without a request from a Subscriber, RA if the situation warrants it.

The RA shall also request for the revocation of the Subscriber's Digital Signature Certificate, if the RA becomes aware of the occurrence of any event that would require the revocation of the corresponding Subscriber's Digital Signature Certificate as specified in this CPS.

4.6.1 Circumstances for Revocation

The Digital Signature Certificate can be revoked under the TCS-CA Trust Network in the following circumstances:

- Compromise of the private key of the TCS-CA or a Partner for whom Sub-CA has been created
- Compromise of the private key of an RA
- Violation of the any terms of the TCS-CA CPS or Subscriber agreement by the Subscribers
- Later changes in the information contained in the Digital Signature Certificate issued by the TCS-CA
- A determination that the Digital Signature Certificate was not issued in accordance with the requirements of the TCS-CA CPS or the Subscriber's Agreement
- Any other reason/circumstances that may reasonably be expected to affect the integrity, security, or trustworthiness of Digital Signature Certificate
- The private key of the Subscriber is found to be compromised
- Instructions from appropriate government authorities, court of law, or law enforcement agencies.

4.6.2 Who can Request Revocation

The Subscriber shall request for Digital Signature Certificate revocation when the Subscriber's private key is compromised or he has reason to believe that the private key may have been compromised or if there is a change in the Digital Signature Certificate's information or circumstances that might result in the information provided in the Digital Signature Certificate to become inaccurate, invalid or misleading. The subscriber may voluntarily request for his certificate to be revoked for any other reason.

The RA who has recommended the issuance of Digital Signature Certificate shall request for Digital Signature Certificate revocation when there is evidence leading to the conclusion that the Subscriber's private key is compromised or that the private key may have been compromised or if there is a change in the Digital Signature Certificate's information or circumstances that might result in the information provided in the Digital Signature Certificate to become inaccurate, invalid or

misleading. The RA may also request revocation if there is evidence that the subscriber is in violation of the terms of the TCS-CA CPS or Subscriber agreement or the subscriber has provided incorrect information in his application.

TCS-CA will evaluate a revocation request and promptly act to revoke the Digital Signature Certificate. In case TCS-CA is in doubt about the genuineness of a revocation request, it reserves the right to conduct further enquiries and take steps including but not limited to suspending the certificate before making a final determination on whether or not to revoke the Digital Signature Certificate. TCS-CA may also revoke a Digital Signature Certificate if instructed in writing by appropriate government authorities, court of law, or law enforcement agencies.

4.6.3 Procedure for Revocation Request

4.6.3.1 Request from the Subscriber

The procedure for the Subscriber to request the revocation of Digital Signature Certificate is as follows:

- The Subscriber generates the request for the Digital Signature Certificate revocation and sends the details along with the reason for revocation
- The RA verifies the details sent by the Subscriber and checks the validity of the reason for revocation (see below). If valid the RA will forward the request to the TCS-CA for revocation of the Digital Signature Certificate
- After receiving the request for revocation signed by the RA, the TCS-CA verifies the request and then revokes the Subscriber's Digital Signature Certificate. The TCS-CA then updates the corresponding CRL with the list of all revoked Digital Signature Certificates and publishes to the Repository.
- The Subscriber can check the status of the revocation request on the TCS-CA Trust Portal.

The validity of the request will be checked as follows:

- For requests from the Subscriber signed using the private key, no further verification is done.

- For requests submitted via the TCS-CA Trust Portal using the user's own user-id and password, no further verification is done.
- For written requests which are signed and accompanied by police complaint, no further verification is done
- For written requests which are signed and accompanied by copy of attested identity proof with the same signature, no further verification is done

For requests submitted over the phone, other details (passport number, PAN number, date of birth, and address) may be verified before executing the revocation request.

4.6.3.2 Request from government/courts/law enforcement

For revocation requests originating from entities such as the government/court/law enforcement agency, verification is based on the nature of documentation submitted in support of the request and will be according to applicable laws.

4.6.3.3 Request from the RA

- RA prepares the Subscriber's details and signs with the RA's private key and forwards to the TCS-CA
- RA sends evidence based on which revocation is being requested to TCS-CA, under signed covering letter
- After receiving the request for revocation signed by the RA, the TCS-CA verifies the request and then revokes the Subscriber's Digital Signature Certificate. In certain circumstances TCS-CA may wait for evidence under signed covering letter. TCS-CA then updates the CRL with the list of all revoked Digital Signature Certificates and publishes to the Repository.

4.6.4 Revocation Request Grace Period

If the private key of the Subscriber is compromised, the Subscriber shall request for the revocation immediately. In other cases request for the revocation shall be made as soon as reasonably practicable. (Ref: TCS-CA-05, Certifying Authority Operations Manual).

4.7 DIGITAL SIGNATURE CERTIFICATE SUSPENSION

(Ref: TCS-CA-05, Certifying Authority Operations Manual).
Suspension is the process of making the Subscriber's Digital Signature Certificate to be invalid temporarily based on conditions as specified in this CPS.

The TCS-CA either on its own or on the recommendation of a concerned RA shall reserve the right to suspend the Digital Signature Certificates of its Subscribers. Wherever reasonably possible this will be done with reasonable notice to the affected Subscribers. By suspension the Digital Signature Certificate usage shall be made invalid temporarily. All suspended Digital Signature Certificates shall be listed in the CRL of the TCS-CA and published to the Repository of the TCS-CA. The TCS-CA shall reserve the right to reactivate the Digital Signature Certificate when the validity of the Digital Signature Certificate has been confirmed.

4.7.1 Circumstances for Suspension

The TCS-CA, by itself or on the recommendation of the RA or on the request of a subscriber may suspend a Digital Signature Certificate in the following circumstances:

- Non-payment of applicable Digital Signature Certificate fees
- Any circumstance which leads TCS-CA to believe that the trust of the TCS-CA trust network may be jeopardized

4.7.2 Who can request Suspension

The RA or the Subscriber may request for suspension

The RA or the Subscriber may only request for the suspension of the Digital Signature Certificate if there is reason to believe that circumstances exists that require the Digital Signature certificate to be suspended

4.7.3 Procedure for Suspension Request

The Subscribers and the RAs shall request for the Digital Signature Certificate suspension using the same procedures as for the Digital Signature Certificate revocation specified in Section 4.6.3 of this TCS-CA CPS.

4.7.4 Revocation of Suspended digital signature certificates

The TCS-CA, reserve the right to revoke the suspended Digital Signature Certificates of its Subscribers, if a request for activation of suspended Digital Signature Certificate is not received within 15 days of the date of suspension.

4.8 ACTIVATION OF SUSPENDED DIGITAL SIGNATURE CERTIFICATES

Activation is the process of making the Applicant/Subscriber's Suspended Digital Signature Certificate to be valid for use based on conditions as specified in this CPS.

The suspended Digital Signature Certificates shall be re-activated upon approval by the TCS-CA or when the same party that had the Digital Signature Certificate suspended initiates the request. This should be done within a reasonable time after the request for suspension was received. The TCS-CA shall remove the re-activated Digital Signature Certificates from the corresponding CRL listing and a new CRL will be generated and published to the repository.

4.8.1 Who can request Activation

A subscriber can always initiate a request for activation of his suspended Digital Signature Certificate, RAs may only initiate the request for activation for those Digital Signature Certificate for which they had initiated the suspension. A Digital Signature Certificate shall be activated only if the TCS-CA is satisfied that the reason for suspension is no longer valid.

4.9 CRL ISSUANCE FREQUENCY

The TCS-CA shall update and issue the CRL (including certificates issued for any Partner for whom Sub-CA has been created whenever Digital Signature Certificates under their respective user groups are revoked or suspended or on the first working day of each month or 30 days after the last update or as and when necessary, whichever occurs first. The CRL issued shall be published to the Repository immediately.

4.9.1 CRL Checking Requirements

A relying party shall use the Digital Signature Certificates issued under the TCS-CA Trust Network only after checking the same with the latest CRL of the corresponding

Digital Signature Certificate issuer available at the Repository. The TCS-CA or the RA shall not be liable to any damages/loss caused by the Digital Signature Certificates or CRLs.

4.9.2 Revocation/Status Checking Availability

The repository is made available to the Subscribers and general public via the TCS-CA Trust Portal. The repository contains all information of the Subscribers Digital Signature Certificates relating to their validity, suspension, activation and revocation through CRL. The relying party must check the Certificate details online before they trust the Digital Signature Certificates. TCS-CA or the RA shall not be held responsible for any loss/damage caused by Digital Signature Certificates issued under the TCS-CA Trust Network that are used by the relying party.

4.10 SECURITY AUDIT PROCEDURES

(Ref TCS-CA-27, System Security Audit Procedures Manual)
The TCS-CA shall maintain audit logs, which will be maintained and updated in real time. These logs will be backed up to physical media (Digital tape, CD or appropriate other storage media). The audit logs will contain the history of the operational activities of the TCS-CA and will be kept in accordance with the applicable record retention policy. Internal and external auditors shall perform periodic review of the TCS-CA s operating practices, procedures and policies.

All the significant security events are time stamped and recorded as audit logs in audit trail files. These audit trail files are archived periodically.

All audit procedures for the TCS-CA Trust Network operation shall be in compliance with the specifications in the IT Act prescribed by the Ministry of Communications and Information Technology, Department of Information Technology, Government of India.

4.10.1 Types of events recorded

Adequate audit trails shall be captured of all sensitive events and pattern analysis made to analyse any misuse as mentioned in this sub-section:

4.10.1.1 Certificate Life Cycle Management

- Requests for generation, revocation, suspension and activation of Certificates
- Both successful and unsuccessful processing of the requests
- Generated Certificates and CRLs

4.10.1.2 Key Life Cycle Management

- Key Generation, backup, archival, recovery and destruction

4.10.1.3 System Security Events

- System start-up and shutdown
- Application start-up and shutdown
- Attempts to create, remove, set passwords or change the system privileges of the Application
- Changes to TCS-CA key or any of its details
- Changes to Certificate policies
- Unauthorized attempts at network access to the TCS-CA system
- Unauthorized attempts to system files.

4.10.1.4 Other Events

- Creation of users to both system and secure area.
- Activation, Deactivation of users.
- Operations facility visitors' entry and exit.
- Operations facility users entry and exit.
- Trusted Personnel changes
- System configuration changes and maintenance
- Records of the destruction of the media relevant to the CA operations.

4.10.1.5 Log entries include the following details

- Event Date and time
- User and the type of user of the event
- Type of the event

4.10.2 Frequency of audit logs processing or auditing

The audit logs are processed and audited as per TCS-CA policies as defined in the CPS with minimal frequency of at least once in two weeks. Further additional audit log processing shall be carried out if any event is found to be affecting the security credentials of the TCS-CA system.

4.10.3 Period for which Audit Logs are retained

Audit logs shall be retained for at least twelve months and archived as specified in this TCS-CA CPS.

4.10.4 Protection of Audit Logs

Audit logs can be viewed, modified or deleted only by the designated administrators of the system. Unauthorized access to the audit logs are restricted by physical and logical access control systems and such access shall be logged.

4.10.5 Audit Log Back-up Procedures

Backup of the audit files are performed weekly and archived in a secure location with access limited to a few trusted personnel only.

4.10.6 Audit collection system (internal and external)

The TCS-CA system shall have all entries and exit logged and also all operational procedures will be logged for archival.

4.10.7 Notification to event-causing subject

The Audit logs will be enabled to provide information of any unauthorized access to the TCS-CA system or premises. In case of any such event the proper personnel must be informed immediately and other actions taken as per the TCS-CA Security Audit Procedures Manual.

4.10.8 Vulnerability assessments

Vulnerability assessments shall be performed, reviewed and revised on a daily, weekly and monthly basis based on the type of events logged by the authorized personnel

4.11 RECORDS ARCHIVAL

The TCS-CA and the RAs shall archive all the operational records in accordance to the standards specified in the IT Act prescribed by the Ministry of Communications and Information Technology, Department of Information Technology, Government of India.

4.11.1 Types of events recorded

4.11.1.1 Digital Signature Certificate Life Cycle Management

The TCS-CA shall archive records of activities, not limited to, Digital Signature Certificate generation, revocation, suspension and activation of all their Certificates and also Subscriber Certificates.

These records include:

- The details of the Subscriber
- The requests verified and forwarded by the corresponding RA
- Identity of the RA personnel processing the request
- Audit Logs which are retained for time specified in the CPS
- All Digital Signature Certificates generated by the TCS-CA under the TCS-CA Trust Network shall be retained in TCS-CA records for at least seven years.
- Notices for suspension
- Information of suspended, revoked and expired Certificates.

4.11.2 Backup of records

(Ref: Gold Book: System-related Procedures)
A copy of all records of the operations of the TCS-CA shall be retained at three different locations within the country including the TCS-CA premises stored in a secure place with restricted access. The TCS-CA shall verify the integrity of the backups at least once in every six months or any time period as affixed in this CPS.

4.12 KEY CHANGEOVER

The TCS-CA, Partner for whom Sub-CA has been created, RAs and Subscriber keys shall be changed periodically as stipulated by the IT Act and the Key change shall be processed as per Key Generation specified in this CPS.

The TCS-CA shall provide reasonable notice to the Subscriber's relying parties of any change to a new key pair used by the TCS-CA to sign Digital Signature Certificates under the TCS-CA Trust Network. There will be no key change of the Subscriber's Certificate unless in the case of a compromise.

The Subscribers of TCS-CA Trust Network shall be issued Digital Signature Certificate for a specified period of time. Before or after the expiration of the Certificate, the Subscribers shall generate a new private-public key-pair and submit the public key along with the new application to the corresponding TCS-CA or RA for generating a new Certificate preferable before the existing Certificate expires.

The period of maximum validity of the Certificates shall be as mentioned below unless otherwise mentioned in this CPS:

- TCS-CA Certifying Authority's keys and associated Certificates – five years
- The keys of the partner for whom Sub-CA has been created and associate Certificates – up to a maximum of 5 years not exceeding the expiry period of TCS-CA Digital Signature Certificate
- Subscriber Digital Signature Certificate key – maximum of five years depending on the type and class of Certificate

4.13 KEY COMPROMISE OF TCS-CA OR PARTNER FOR WHOM SUB-CA HAS BEEN CREATED

The TCS-CA and the Partner for whom Sub-CA has been created under the TCS-CA Trust Network shall maintain a backup of all the critical information and the Authority's public keys shall be archived permanently. The compromise of the TCS-CA or Partner for whom Sub-CA has been created private key shall be informed to all the applicable Subscribers as soon as practicable and shall also be published to the TCS-CA Trust Portal.

In case of the Subscriber's private key being compromised, the TCS-CA on the recommendation of the concerned RA shall immediately revoke the affected keys and associated Digital Signature Certificates.

In case of Key compromise of the Partner for whom Sub-CA has been created, all Certificates issued by the Partner for whom Sub-CA has been created under the TCS-CA Trust Network shall be revoked and a CRL shall be generated. The CRL is posted on the TCS-CA Repository and a communication shall be sent to TCS-CA notifying the event, including the new public key for signing by TCS-CA. All customers whose Certificates are still valid will be notified via email, and upon request, will be provided new Certificates signed with the new private key on request. There will be no extra charge for this. However, the agreement between TCS-CA (the TCS-CA) and the Partner for whom Sub-CA has been created in question shall govern whether any costs shall be recovered in such cases and the extent of such costs.

In case of TCS-CA Key compromise, all Certificates issued by TCS-CA shall be revoked and a CRL shall be generated. The CRL is posted on the TCS-CA Trust Portal and a communication shall be sent to the CCA notifying the event, including the new public key for signing by the CCA. All customers whose Certificates are still valid will be notified via email, and upon request, will be provided new Certificates signed with the new TCS-CA private key on request. There will be no extra charge for this.

4.14 KEY DESTRUCTION/CHANGEOVER OF TCS-CA OR PARTNER FOR WHOM SUB-CA HAS BEEN CREATED

The TCS-CA or the Partner for whom Sub-CA has been created under the TCS-CA Trust Network shall follow the procedures for private key destruction procedure as laid out in the "TCS-CA Key Management Procedure Manual". This shall be done under the following circumstances: (a) Key Compromise, (b) Private Key Certificate expiry, and (c) Termination of services.

In the case of Key compromise, see Section 4.13 for activities to be performed before such key destruction.

In the case of expiry of the TCS-CA or the Partner for whom Sub-CA has been created Certificate, a new private and public key pair are generated and submitted to the TCS-CA (in case of Partner for whom Sub-CA has been created under the TCS-CA Trust Network) or the CCA (in case of TCS-CA) for certification.

For termination of services, please see the Section 4.15 for activities to be performed before key destruction.

4.15 TERMINATION OF SERVICES

The TCS-CA and the Partner for whom Sub-CA has been created shall reserve the right to terminate its operations at any time with reasonable notice as stated in Section 4.15.1 below to all affected parties. The TCS-CA and the Partner for whom Sub-CA has been created shall take the necessary steps to destroy all copies of the private keys necessary for encryption and notify the details of such activity to TCS-CA (in case of Partner for whom Sub-CA has been created under the TCS-CA Trust Network) or the CCA (in case of TCS-CA) as specified by the IT Act.

4.15.1 Requirements prior to Cessation

The following obligations shall be followed by Partner for whom Sub-CA has been created to reduce the impact of termination of service by providing for timely notice, transfer of responsibilities to succeeding entities, maintenance of records, etc.
Before ceasing the operations TCS-CA or Partner for whom Sub-CA has been created shall:

- Notify TCS-CA (in case of Partner for whom Sub-CA has been created closing the services) or the CCA (in case of TCS-CA closing the services) of its intention to cease acting as a Partner for whom Sub-CA has been created or TCS-CA respectively. Such notice shall be made at least ninety (90) days before ceasing to act as TCS-CA or the Partner for whom Sub-CA has been created or ninety days before the date of expiry of license. TCS-CA (in case of Partner for whom Sub-CA has been created closing the services) or the CCA (in case of TCS-CA closing the services) may require additional statements in order to verify compliance with this provision.
- Provide a sixty (60) day notice to the Subscriber of each unrevoked or unexpired Certificate of its intention to cease acting as a TCS-CA or the Partner for whom Sub-CA has been created.
- Revoke all Certificates that remain unrevoked or unexpired at the end of the sixty (60) day notice period, whether or not the Subscribers have requested revocation. This is to enable the Subscribers to find alternate means of certification and thereby prevent undue disruption to their business.
- Give notice of the revocation to each affected Subscriber.
- Make a reasonable effort to ensure that discontinuing its certification services will cause minimal disruption to its Subscribers and to persons duly needing to verify Digital Signatures by reference to the public keys contained in outstanding Certificates.
- Make reasonable arrangements for preserving its records for the stipulated time as specified in this CPS.

4.16 CERTIFICATE USAGE

4.16.1 Encryption

Senders can use Digital Signature Certificates issued by the TCS-CA under the TCS-CA Trust Network to send electronic data to Recipient(s). The data, which is being sent, shall be encrypted by the recipient's public key listed in the corresponding Digital Signature Certificate of the encryption key pair. On receiving the encrypted data, the recipient shall decrypt the message with the private key corresponding to the public key listed in the Digital Signature Certificate used to encrypt the data.

4.16.2 Signing

The Subscriber can use the Digital Signature Certificate issued under the TCS-CA Trust Network to sign the data to be sent. The Subscriber shall sign the data with the private key of the signing key-pair and enclose the Digital Signature Certificate containing the sender's public key. The recipient shall use the sender's public key listed in the Digital Signature Certificate to verify the Signature.

4.16.3 SSL Server

The Subscriber can use the Digital Signature Certificate issued by the TCS-CA under the TCS-CA Trust Network for use in Secure Sockets Layer (SSL) between the Web servers and customers' and users' Web browsers.

4.16.4 SSL Client

The Subscriber can use the Digital Signature Certificate issued by the TCS-CA under the TCS-CA Trust Network for use in Secure Sockets Layer (SSL) communication between the browser and the Web Servers.

4.16.5 Object Signing

The Subscriber can use the Digital Signature Certificate issued by the TCS-CA under the TCS-CA Trust Network for Object Signing. The objects can be but are not limited to Java applets, Java Scripts, plug-ins.

Note: The use of the above Certificates is subject to the terms and conditions as specified in this CPS and the Subscriber agreement.

5 PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

The system components and operation of the TCS-CA shall be contained within a physically protected environment to deter, detect and prevent unauthorized use of, access to, or disclosure of sensitive information. The physical security standards are modeled as per the physical and operational security guidelines mentioned in the Information Technology Act, 2000 Rules (Schedule II).

5.1.2 Physical Access

The operation site shall be actively monitored with redundant power and notification methods. Sensitive areas within the facility, such as power and network connection shall also be controlled within the protected facility.

The Operation site has multiple tiers of security enforced through Photo ID badges, proximity cards and Biometric access devices. The trusted persons escort all visitors and every visitor shall sign the visitors' log.

The facility shall be continually staffed (24x7), either by trusted persons or by an on-site guard service during non-business hours.

An access log shall be maintained at the operational site and inspected periodically.

5.1.3 Power and Air Conditioning

The operation site shall be supplied with uninterrupted power supply and air conditioning sufficient to create a reliable operating environment.

All critical systems shall have backup power capable of supporting the critical systems until manual power shutdowns can occur.

5.1.4 Water Exposure

All precautions to protect critical systems on operation premises from water damages by using raised floors and water detector systems shall be taken.

5.1.5 Fire Prevention and Protection

The operation site shall have installed automatic fire detectors and extinguishers compliant with standard requirements specified by the fire brigade to prevent and protect the facility from fire.

5.1.6 Media Storage

All media relevant to the operation shall be protected in a secure place with access restricted to authorized personnel as per the guidelines in the Gold Book – System Procedures.

5.1.7 Waste Disposal

Unused, unwanted documents and materials shall be scrutinized before being destroyed or released for disposal.

5.1.8 Off-site backup

All critical data shall be incrementally backed up and the backup copies stored at an offsite location. The data shall be properly secured based on the classification of data, which is defined by the Certifying Authority in the security policy.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

Employees who shall have access to or control operations that may materially affect the issuance, use, suspension, activation or revocation of Digital Signature Certificates, including access to restricted operation of the TCS-CA Repository, are considered as serving in trusted positions. Such personnel include but are not limited

to, system administration personnel, designated consultant, and executives who shall be designated to oversee the TCS-CA infrastructure.

All the employees whose duties include any of the following must acquire and periodically re-qualify for "trusted" status:

- Access to the Operation site
- Access to the Certificate generation machine
- Access to critical system
- Access to the Cryptographic signing units
- Holding combinations of keys or access to the safe deposit boxes containing critical data
- Access to the company or Subscriber sensitive material
- Oversight of infrastructure
- Granting of physical and/or logical access

5.2.2 Number of persons required

TCS-CA shall maintain at least 2 CA administrators, 2 RA Administrators and 2 System Administrators Separate individuals shall be identified for each of these roles. TCS-CA may deploy additional persons as needed for satisfying operational and administrative needs.

5.2.3 Identification and Authentication for each Role

- All personnel performing trusted roles in the TCS-CA Trust Network facility shall have their identities and authorization verified before they are empowered to perform the appropriate trusted role.
- Class 3 TCS-CA Digital Signature Certificates would be issued only to users of type Certifying Authority (CA), Partner for whom Sub-CA has been created Administrator (Sub-CAA), RA Administrator (RAA), RA Operator (RAO), CA Administrator (CAA) and CA Operator (CAO) for performing respective operations under the TCS-CA Trust Network. No personnel belonging to other trusted roles would be issued a Digital Signature Certificate for conducting related operations.
- Each of these Certificates and accounts shall
    - Be restricted to the actions and uses authorized for that trusted role

- Not be shared with anyone
- Be directly attributed to the personnel performing that trusted role

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience and Clearance Requirements

The persons being considered for trusted roles shall possess the required background, qualifications and experience necessary to perform the roles ably and satisfactorily.

The Certifying Authority shall grant the trusted status to the person after he/she has acquired the required skills and qualification to perform the trusted role.

5.3.2 Background Check Procedures

The TCS-CA or RA shall perform background checking for all the personnel before deploying them in trusted roles. These checks include

- Check of qualifications relevant to the trusted role responsibilities.
- Check of prior employment
- Check or passport/ration card/driver's license details

The personnel shall be rejected for the trusted role if any of the above checks reveals misrepresentation or indicates that the concerned individual is not suitable for the corresponding trusted role.

5.3.3 Training Requirements

The TCS-CA or RA shall provide adequate training to the personnel selected for each trusted role to perform their job responsibilities ably and satisfactorily.

This includes:

- Comprehensive training with respect to the duties to be performed.
- Awareness of the relevant aspects of Information Technology Security Policy and Security Guidelines framed for carrying out TCS-CA or RA operations.
- Training in disaster recovery and business continuity procedures formed by the TCS-CA or RA as applicable.
- Training in the PKI software used to perform the operations.

The training method may vary from on-job training, classroom based training, self-study, and Computer Based Training (CBT). The training program shall be revised as and when necessary to improve the performance of its personnel.

5.3.4 Retraining Frequency and Requirements

The TCS-CA or RA shall provide its personnel ongoing training to update their skills and knowledge to perform their job responsibilities ably and satisfactorily.

Refresher training for the personnel in all the trusted roles shall be given by the TCS-CA or RA as and when required.

The training plans for the personnel in all the trusted roles shall be reviewed annually.

5.3.5 Sanctions for Unauthorized Actions

The Partner for whom Sub-CA has been created shall take appropriate disciplinary actions against personnel for unauthorized actions or other violations of the policies and procedures of Operations.

5.3.6 Documentation Supplied to Personnel

All the personnel involved in the PKI services under the TCS-CA Trust Network shall be required to read the TCS-CA CPS and Security Policy documents.

Adequate training materials and relevant documents shall be provided to all the personnel in trusted roles to perform their job responsibilities ably and satisfactorily.

5.3.7 Breach of Security

In the event of breach of security being discovered, the matter should be immediately escalated to at least two of the following - CA, CA Head, CA Administrator. Immediate corrective action shall be taken and impact analysis to determine the extent of breach of security shall be carried out. Appropriate action to plug the breach shall be taken.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

The TCS-CA's and the Partner for whom Sub-CA has been created private-public key pairs shall be generated by TCS-CA confidentially using the standards specified in the IT Act, 2000. The key generation shall be conducted in a secure and trustworthy environment. The Certificate and key generation shall be documented and witnessed for authentication purpose. Each such key pair will be 2048 bits long and will be generated on a secure medium.

Subscribers shall be required to use private key/public key pairs that are 1024 bits long, generated on a secure medium.

The TCS-CA and the Partner for whom Sub-CA has been created shall generate encryption private-public RSA key pairs that are 1024 bits long for Subscribers.

6.1.2 Private Key Delivery to Entity

The TCS-CA shall generate the private key of the encryption key pair for the Subscriber, and the private key shall be delivered to the Subscriber as a PKCS #12 file. The TCS-CA shall validate the Subscriber by verifying his/her/its Signature produced by his/her/its signing private key before delivering the encryption private key.

6.1.3 Public Key Delivery to Certificate Issuer

The public key to be included in the Digital Signature Certificate issued under the TCS-CA Trust Network shall be given to the RA with the filled pro forma as specified in the IT Act, 2000 as a request for Certificate generation. The RA shall verify the details and deliver the public key along with the Applicant's details with RA's Signature to the TCS-CA recommending the generation of the Digital Signature Certificate. The Certification process ensures that the Subscriber's public key is not

changed during transit and that the sender possesses the private key corresponding to the transferred public key.

The public key for the Encryption Certificate shall be generated by the TCS-CA

6.1.4 CA Public Key Delivery to Users

The Digital Signature Certificate of the TCS-CA or the Partner for whom Sub-CA has been created shall be obtained from the TCS-CA repository.

6.1.5 Key Sizes

The key length of the TCS-CA and the Sub-CAs shall be equivalent to 2048-bit RSA key pair.

Subscribers shall be required to use private key/public key pairs that are 1024 bits long.

6.1.6 Time Stamp

All servers used in the TCS-CA Trust Network set-up use the NTP suite of programs to keep themselves synchronized with timeservers around the world. The protocol and the technique used, along with the frequency of synchronization and the margins of error, are described in RFC 1305, and in the NTP software home pages at http://www.ntp.org/. The error margins of the Time Stamping clock shall not be more than 1 in 10^9.

6.2 PRIVATE KEY PROTECTION AND BACKUP

A signing private key is generated at the Subscriber end and neither the TCS-CA nor RA gets to see this key at any time. Hence this section applies only to encryption private keys.

The generation of the encryption key pair shall be in conformity with the Indian Telegraph Act and all other relevant parts of the Indian legal system. A copy of the

Dual Key Pair (Encryption) of the Subscriber shall be retained with the safe custody of the TCS-CA.

The purpose of this archival is to satisfy legal requirements, such as summons or requests for a Subscriber's private key from a law enforcement agency. There are no key recovery services provided or implied, and Subscribers should exercise care not to lose their private keys after they have downloaded them.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The Subscriber public key shall be retained and archived by the TCS-CA for the Certificate life-cycle management.

6.3.2 Usage Periods for the Public and Private Keys

The Certificate is valid for the period specified in the Certificate profile and can neither be extended nor renewed thereafter. After expiry of the existing Certificate, the Subscriber must apply for and obtain a new Certificate, including submitting details for verification as before.

6.4 ACTIVATION DATA

All key management activities like Certificate generation, suspension, activation or revocation and CRL generation shall use the private key stored in FIPS 140-1 Level 3 compliant storage, which is activated using tokens.

6.5 COMPUTER SECURITY CONTROLS

The design of the TCS-CA digital signature certification services and the Certificate generation system provides reasonable assurance that the system software and the data files used to issue, suspend, activate and revoke Digital Signature Certificates shall be secured from unauthorized access. The access to the production systems is strictly limited to those individuals who shall be assigned for that work. No Remote access shall be permitted to Certificate Generation Module. Remote access for other

management functions shall be restricted to authorized users who authenticate themselves to the system. The systems shall be monitored regularly and action shall be taken in event that any correction is required.

The TCS-CA digital signature certification services and corresponding system utilizes a wide variety of hardware and software to perform various functions in a secure and timely manner. For reasons of security, the details are not being provided in this CPS. (Ref: TCS-CA-07, TCS-CA Information Technology and Security Policy Manual and TCS-CA-05 Certifying Authority Operations Manual)

6.6 LIFE CYCLE TECHNICAL CONTROLS

The technical controls and the security procedures described in this TCS-CA CPS shall be reviewed on a yearly basis. The operational procedures may be modified to maintain and enhance the system security.

6.7 NETWORK SECURITY CONTROLS

Network devices and Firewall systems shall be utilized to enhance the security of the systems in the TCS-CA Trust Network.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

The TCS-CA or RA under the TCS-CA Trust Network shall utilize hardware cryptographic modules to perform all Digital signing operations that are rated FIPS 140-1 level 3 of security.

6.9 BREACH OF SECURITY

In the event that a breach of security is discovered, the matter shall be immediately escalated to at least two of the following - CA, CA Head, CA Administrator. Immediate corrective action shall be taken and impact analysis to determine the extent of breach of security shall be carried out. Appropriate action to plug the breach shall be taken.

7 CERTIFICATE AND CRL PROFILE

7.1 CERTIFICATE PROFILE

Digital Signature Certificates issued by the TCS-CA or RA under the TCS-CA Trust Network under this CPS shall contain public keys used for authenticating the sender of the electronic message and verifying the integrity of such messages.

The Certificate created shall conform to International Telecommunication Union X.509 version 3 standard. At a minimum, Certificates produced under this CPS shall contain the field and indicated prescribed values or constraints described below in this section.

7.1.1 Base Certificate

The Base Certificate consists of the following fields:

Version	Version 3 (value 2)
Serial Number	Unique as per the Issuer Distinguished Name
Issuer DN	Issuer Distinguished Name
Subject DN	Entity Distinguished Name
Validity	Certificate Validity Period
Subject Public Key	Public key and identity of the algorithm with which the Key is used.
Signature Algorithm	The algorithm identifier for the algorithm used by the TCS-CA or a Partner for whom Sub-CA has been created.

7.1.2 Name Forms

The following shall be the minimum content rules for the subject Name field of the Certificate issued under this CPS:

Depending on additional technical customizations there may exist character set restrictions, which precludes inclusion of certain additional characters.

- Common Name
- E-mail
- Organization
- Organization Unit
- Locality
- State
- Country

In addition to this, an additional "Organization Unit" field will be added, whose value will give the class of Certificate issued (Class 1, 2, or 3).

7.1.3 Usage of Extensions

The following shall be the minimum use of extensions for the Digital Signature Certificates issued by the TCS-CA as per this CPS

7.1.3.1 Basic Constraints

Certifying Authority

TCS-CA (TCS-CA) and Partner for whom Sub-CA has been created Certificate shall have the Basic constraints CA field set to TRUE.

The critical field of these extensions shall be set to TRUE.

End Entity

The end-entity Certificates shall contain the Basic constraints extension with CA field set to FALSE. DER encoding rules establish that fields intended to be set to their default value will be absent in resulting encoding. Therefore, this field may be absent in Basic constraints extension of the End-entity Certificates, thereby indicating the default FALSE value of this field.

The criticality of this extension shall be set to TRUE.

7.1.4 Key Usage

The following shall be the minimum extensions required for the specific usage for the Digital Signature Certificates issued by the TCS-CA as per this CPS.

7.1.4.1 Sub-CA Certificates

Sub-CA Certificates shall contain a key usage extension with Key Cert Sign, CRL Sign and Digital Signature.
The criticality field of this extension shall be set to TRUE.

7.1.4.2 End Entity

All the End Entity shall contain the following extension set as per the type of the Certificate.

Signing Certificate
This type of Certificate shall contain the key usage extension with Digital Signature and Non-Repudiation.

Encryption Certificate
This type of Certificate shall contain the key usage extension with Key Encipherment and the extended key usage will have email protection.

SSL Server Certificate
This type of Certificate will contain the key usage extension with Key Encipherment and the extended key usage will have Server Authentication.

Object Signing Certificate
This type of Certificate will contain the key usage extension with Non-Repudiation, Digital Signature and the extended key usage will have code signing

7.2 CRL PROFILE

Certificate Revocation List issued by the TCS-CA shall contain the list of the Revoked and Suspended Certificates.

The CRL created shall conform to International Telecommunication Union version 2 standard. At a minimum, Certificates produced under this CPS shall contain the field and indicated prescribed values or value constraints described below in this section.

The Base CRL consists of the following Fields

Version	2 (value 1)
Issuer DN	Issuer Distinguished Name
Signature	The algorithm identifier for the algorithm used by the certifying Authority for signing of the CRL.
Last Update	This field contains the issue date of this CRL
Next Update	This field indicates the date by which the next CRL will be issued.
Revoked Certificates	This field contains the list of revoked/suspended Certificate serial numbers, the reason for revocation/suspension and the date on which the revocation has occurred.
Signature Value	This Field contains a Digital Signature computed on the ASN1.1 DER encoded CRL
Extension	Authority Key Identifier

8 SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

The details in the TCS-CA CPS may be changed periodically with the approval of the CCA. The updated CPS shall be published as specified in the Section 8.2 of this CPS. The version number and the date of publication shall be updated with the updated TCS-CA CPS.

8.2 PUBLICATION AND NOTIFICATION POLICIES

The TCS-CA CPS shall be published on the TCS-CA Trust Portal. The changes shall be archived/notified on the TCS-CA Trust Portal.

8.3 CPS APPROVAL PROCEDURES

Proposed changes to the CPS are divided into two classes. Simple changes (such as minor clarifications, spelling/grammatical errors, minor typographic errors) shall be noted as and when the error is found. On the first of each month, all such errors (if any) are collected and the whole set treated as one proposed change.

Large changes, such as material changes in policy, procedures, financial information (such as fees or liability caps), and any other changes are treated as proposed changes.

The TCS-CA management must approve the proposed changes. A Change Control Board consisting of the head of the TCS-CA entity, one member from the operational staff of TCS-CA, and one senior officer of TCS shall approve or reject these changes.

These changes are informed to the CCA and upon approval by CCA are adopted as the new CPS and updated on the TCS-CA Trust Portal.

9 CERTIFICATE PROFILE

TCS - CA Certificate Profile

Version Number *(version 3)*
Serial Number
Signature Algorithm : *(Algorithm Identifier)*
Issuer
Validity
Not Before :
Not After :
Subject
Subject Public Key Info
Extensions : (*X509v3 Extensions*)
{
Basic Constraints
(*CA : TRUE/FALSE*)

Subject Key Identifier
Key Usage
{
Digital Signature
Non Repudiation
Key Encipherment
Data Encipherment
Key Agreement
Key Cert Sign
CRLSign
Encipher Only
Decipher Only
}

Extended Key Usage
{
Extended Key Usage Syntax
Key Purpose Id
{
Server Authentication
Client Authentication
Code Signing
Email Protection
Time Stamping
}
}

Signature Algorithm : *(Algorithm Identifier)*
Signature Value

FIGURE-3: TCS-CA CERTIFICATE PROFILE

10 CRL PROFILE

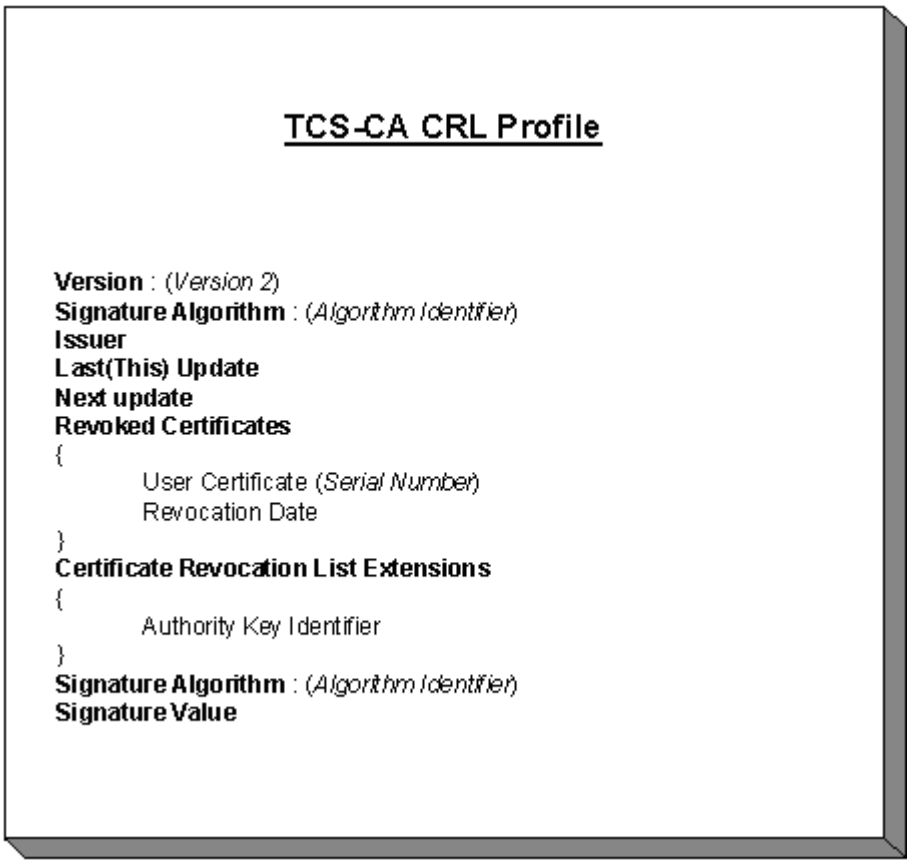

FIGURE-4: TCS-CA CRL PROFILE

11 TCS-CA SUBSCRIBER AGREEMENT

TATA CONSULTANCY SERVICES - CERTIFYING AUTHORITY
[DIGITAL SIGNATURE CERTIFICATION SERVICES]

YOU MUST READ AND AGREE TO THIS SUBSCRIBER AGREEMENT BEFORE APPLYING FOR, ACCEPTING, OR USING A DIGITAL SIGNATURE CERTIFICATE.

THIS SUBSCRIBER AGREEMENT will become effective on the date you submit the Certificate application to the designated RA /TCS-CA as applicable. By submitting the Certificate Application Form, you are requesting the TCS-CA to issue a Digital Signature Certificate to you and are expressing your agreement to the terms of this Subscriber Agreement.

TATA CONSULTANCY SERVICES Digital Signature Certification Services are governed by TATA CONSULTANCY SERVICES - CERTIFYING AUTHORITY Trust Network Certification Practice Statement (the "TCS-CA CPS") as amended from time to time, which is incorporated by reference into this Subscriber Agreement. The TCS-CA CPS is published on TATA CONSULTANCY SERVICES - CERTIFYING AUTHORITY repository at http://www.tcs-ca.tcs.co.in and is available in E-mail from: helpdesk@tcs-ca.tcs.co.in. Amendments to the TCS-CA CPS are also posted in TATA CONSULTANCY SERVICES - CERTIFYING AUTHORITY repository at http://www.tcs-ca.tcs.co.in.

YOU AGREE TO USE THE DIGITAL SIGNATURE CERTIFICATE AND ANY RELATED TCS-CA PKI SERVICES ONLY IN ACCORDANCE WITH THE CPS AND APPLICABLE LAWS, RULES AND REGULATIONS.

YOU CERTIFY THAT THE INFORMATION PROVIDED BY YOU IS ACCURATE, CURRENT AND COMPLETE. YOU CONSENT TO THIRD PARTY, INDEPENDENT VERIFICATION OF THE PROVIDED INFORMATION. SHOULD THERE BE ANY MATERIAL CHANGES IN THE INFORMATION PROVIDED IN YOUR APPLICATION AFTER A DIGITAL SIGNATURE CERTIFICATE HAS BEEN ISSUED TO YOU, THE CERTIFICATE WILL BE RENDERED INVALID AND YOU WILL HAVE TO APPLY FOR A NEW CERTIFICATE. YOU SHALL NOT

SEND ANY DATA IN ENCRYPTED FORMAT THAT MAY DIRECTLY OR INDIRECTLY COMPROMISE THE NATION'S SECURITY AND INTEREST. YOU AGREE AND ACKNOWLEDGE THAT TCS-CA HAS AUTHORITY AND POWER TO REVOKE THE DIGITAL SIGNATURE CERTIFICATE ISSUED TO YOU IF AT ANY POINT IT IS DETERMENT THAT THE INFORMATION PROVIDED IS INCOMPLETE OR INCORRECT

YOU SHALL SUBMIT YOUR PRIVATE KEY (S) TO TCS-CA OR CCA ON THEIR DIRECTION OF ANY COMPETENT AUTHORITY UNDER VARIOUS LAWS AND ACTS INCLUDING THE IT ACT 2000, BECAUSE OF A DISPUTE ARISING DUE TO THE ISSUE OF A DIGITAL SIGNATURE CERTIFICATE ISSUED BY TCS-CA AND USED FOR ENCRYPTION OF ANY MATERIAL .

AS STATED IN THE TCS-CA CPS, TATA CONSULTANCY SERVICES - CERTIFYING AUTHORITY OR DESIGNATED PARTNER FOR WHOM SUB-CA HAS BEEN CREATED OR REGISTRATION AUTHORITY (i.e. TCS-CA/RA) PROVIDES LIMITED WARRANTIES, DISCLAIMS ALL OTHER WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, LIMITS LIABILITY, AND EXCLUDES ALL LIABILITY FOR INCIDENTAL, CONSEQUENTIAL, AND PUNITIVE DAMAGES AS STATED IN THE TCS-CA CPS. SEE THE TCS-CA CPS FOR IMPORTANT DETAILS.

YOU DEMONSTRATE YOUR KNOWLEDGE AND ACCEPTANCE OF THE TERMS OF THIS SUBSCRIBER AGREEMENT AND THE TCS-CA CPS AND THE DOCUMENTS REFERRED TO IN THE TCS-CA CPS BY EITHER (I) SUBMITTING AN APPLICATION FOR A DIGITAL SIGNATURE CERTIFICATE TO TATA CONSULTANCY SERVICES - CERTIFYING AUTHORITY OR DESIGNATED PARTNER FOR WHOM SUB-CA HAS BEEN CREATED OR REGISTRATION AUTHORITY, OR (II) USING THE DIGITAL SIGNATURE CERTIFICATE.

PLEASE NOTE THAT THE SCOPE OF THIS AGREEMENT IS LIMITED TO THE ISSUE OF DIGITAL SIGNATURE CERTIFICATE AND WILL NOT APPLY IN ANY MANNER TO THE CONTRACTUAL TERMS AND CONDITIONS THAT MAYBE ENTERED INTO BETWEEN YOU AS SUBSCRIBER AND THE RELYING PARTY. ALL CLAIMS, CONTRACTUAL OR OTHERWISE, RESULTING FROM OR CONNECTED TO THE DEALINGS OR TRANSACTIONS SHALL BE ENTIRELY BETWEEN YOU AND THE RELYING PARTY.

12 DIGITAL SIGNATURE CERTIFICATE APPLICATION FORM

12.1 FORM FOR A COMPANY TYPE OF CERTIFICATE

TATA CONSULTANCY SERVICES LIMITED – CERTIFYING AUTHORITY

REQUEST FORM FOR CLASS-2/3 CERTIFICATE

Affix recent Passport size Photograph of the Applicant
Please sign across the Photograph

USER TYPE - COMPANY

Instructions:

1. Please fill the form in BLOCK LETTERS
2. Items marked with * are mandatory.
3. For the items marked with #, details for at least one are mandatory

COMPANY'S DETAILS TO BE FILLED IN BY THE APPLICANT: *

COMPANY REGISTRATION NO. *

Date of Incorporation/Agreement/ Partnership (DD/MM/YYYY) *

		/				/			

PARTICULARS OF BUSINESS

A. Corporate / Branch / Registered Office

Name

Flat/Door/Block No.

Name of Premises/ Building/Village

Road/Street/Lane/
Post Office

Area/Locality/Taluka
/Sub-Division

Town/City/District

State/Union Territory

Pin

Telephone No.

Fax

Web Page URL, if any

Nature of Business

Company Income Tax
PAN No.

PERSONAL DETAILS OF THE AUTHORISED APPLICANT * (Mandatory)

FULL NAME *
Last Name/Surname

First Name

Middle Name

ADDRESS

Flat/Door/Block No.

Name of Premises/
Building/Village

Area/Locality/Taluka

Road/Street/Post Office
Sub-Division

Town/City/District

State/Union Territory

Pin

Telephone No.

Fax

Mobile Phone No.

Nationality

Visa details, in case of Foreign Nationals

Details for at least one is mandatory

PASSPORT DETAILS #

Passport No.

Passport Issuing Authority

Passport Expiry Date

VOTER'S IDENTITY CARD NO. #

INCOME TAX PAN NO. #

E-MAIL ADDRESS * (Mandatory)

TYPE OF DIGITAL SIGNATURE CERTIFICATE REQUIRED * (Please tick one)

Signing Certificate (Single Key pair) ☐

(This can be used for signing and/or encryption)

Encryption certificate (Dual Key Pair) ☐

(This can be used only for encryption)

Signing certificate (Dual Key pair) ☐

(This can be used only for signing)

Date

Signature of the Applicant

To be filled by TCS - RA Office

The above details have been verified and found to be correct.

Signature of RA Office

Name:

Date:

Seal:

DOCUMENT CHECKLIST FOR <u>COMPANY</u> TYPE OF CERTIFICATE

The following is a list of the supporting documents that you need to submit along with the Certificate Request Form.

NOTE:

- *NOTARIZATION TO BE DONE BY PUBLIC NOTARY/practicing CA / CS*
  Or
- *ATTESTATION TO BE DONE BY GAZZETTED OFFICER.*

Sr. No.	Required Documents	Document submitted	Documents verified by RA
1	**<u>Certificate of Incorporation</u>** **Public & Private Limited Companies (any one NOTARIZED copy required)** • Certificate true copy of the Certificate of incorporation / Business commencement from either the company secretary / a Director of the company • Certified true copy of the Memorandum and Articles of Association from either the Company secretary / a Directory of the company • Copy of the latest Annual report.		
	Partnership Firms (any one required) • Certificate true copy of the partnership deed from either a Class I Gazette officer / Notary / Chartered Accountant. • Copy of One of the following: - o Latest Annual Report o Latest Balance sheet o Latest Income Tax Return		
	Proprietorship Firms (any one required) • Copy of the Latest bank statement certified by the bank manager of the bank where the account is held.		

	• Copy of One of the following: -
	  ○ Latest Balance sheet
	  ○ Latest Income Tax Return		

2	**<u>Subscriber Verification Documents</u> (any one attested copy required)** • Passport • Voter's ID • PAN card • Identity Card – Attested by Authorized signatory of the company with photograph. • Driver's license • Ration Card		
3	**<u>Proof of Address</u> (any one attested copy required)** • Passport • Ration card • Driver's license • Latest Telephone bill • Latest Electricity bill • LIC receipt • Authorization Letter on the company's letterhead attested by company's authorized person.		
4	Company PAN No. **(Required)**		
5	Certificate Enrollment Form (downloaded from www.tcs-ca.tcs.co.in) + Letter of Authority **(Required)**		

Declaration

I hereby agree that I have read and understood the following instructions carefully and ensure proper usage of the Digital Signature Certificate.

1. The certificate should be downloaded onto the same machine/device from where the request was initiated.
2. After placing an online request for a certificate, the following activities should not be carried out until the certificate is successfully downloaded:
   - √ Formatting of the machine
   - √ Reinstallation or upgrade of the internet browser on the machine from which the certificate request was initiated
3. At the time of registration, a valid email ID that is accessed regularly should be provided.
4. Certificate revocation is permanent and irreversible. If my certificate is revoked, I will have to reapply for a fresh certificate. The same will be approved only after the payment of necessary applicable charges.
5. The security level in the Internet Browser should be set to 'Medium' and all scripting should be enabled.
6. The 'Certificate Trust Chain' has to be downloaded for using my certificate. (Link: **http://www.tcs-ca.tcs.co.in/index.jsp?link=html/chaindownload.html**)
7. It is my responsibility to remember the passwords that are used while generating/exporting the certificates/keys.
8. Requirements with respect to Operating System and Internet Browser are as follows:
   - √ Operating System
     a. Supported Versions - Windows 2000/XP
     b. Recommended Versions - Windows 2000/XP
   - √ Internet Browser
     a. Supported Versions - IE 5.5 and above
     b. Recommended Versions - IE 6.0 and above

Date

Signature of the Applicant

Annexure-A: Letter of Authority

I, _____, in the capacity of the _____ of _____, authorize _____, whose signature is attested below to carry out all the necessary formalities on behalf of _____ for the application of a Class-3 Digital Signature Certificate with the validity period of ___ year(s).

_____

Signature and Designation
of Authorizing Person

_____

Signature and Designation
of the Applicant

_____

Signature and Designation
of the Authorizing Person

12.2 Form for an Individual type of Certificate Government / Banking Sector

TATA CONSULTANCY SERVICES LIMITED – CERTIFYING AUTHORITY

REQUEST FORM FOR CLASS-2/3 CERTIFICATE

USER TYPE – GOVERNMENT/BANKING SECTOR

Affix recent passport-size photograph of the applicant. Applicant to sign across the photograph.

Instructions:

4. Please fill the form in BLOCK LETTERS
5. Items marked with * are mandatory.
6. For the items marked with # (Details for at least one are mandatory)

DETAILS TO BE FILLED IN BY THE APPLICANT: *

FULL NAME *

Last Name/Surname

First Name

Middle Name

Designation:

GENDER * (Tick as applicable)

Male ☐ Female ☐

ORGANISATION/OFFICE DETAILS *

Organization Name

Office Address

Pin Code

Administrative Ministry/
Department

Government of India/
State Government

Telephone No. --
Area Code Telephone No.

Fax No. --
Area Code Fax No.

Details of at least one are mandatory #

EMPLOYEE IDENTIFICATION NO.#

PASSPORT NO. #

VOTER'S IDENTITY CARD NO. #

INCOME TAX PAN NO. #

E-MAIL ADDRESS * (Mandatory - a valid and active email ID that is accessed frequently)

Date

Signature of the Applicant

Instructions

1. All subscribers are advised to read Certificate Practice Statement of CA.
2. The certificate shall be downloaded onto the same computer / Hardware device (USB token, Smart Card etc.) by login as same computer user account from where the request was initiated.
3. After placing an online request for a certificate, the following activities **shall not** be carried out until the certificate is successfully downloaded:
   - Formatting of the computer
   - Deletion of computer user account used to logon when the request was initiated
   - Reinstallation or upgrade of the Internet browser on the computer from which the certificate request was initiated.
4. If you lose your key pair, you shall inform the RA Administrator immediately and apply for the revocation of your certificate.
5. Application form must be submitted in person.
6. Incomplete/Inconsistent application is liable to be rejected.

Declaration

I hereby confirm that I have read and understood the above instructions and will follow the above instructions for obtaining and using the Digital Signature Certificate.

Date:

Place: **Signature of the Applicant**

For Head of Office or JS (Admn.) for Govt Sector / Superior Authority for Banking

Sector of Applicant

LETTER OF AUTHORITY

This is to certify that Mr. /Ms. _____has provided correct information in the "Application form for issue of Digital Signature Certificate for subscriber of Government and Banking Sector" to the best of my knowledge and belief. I hereby authorize him/her, on behalf of my organization to apply for obtaining Digital Signature Certificate from CA for the purpose specified above.

Date:

Place:

Name of Officer with Designation:

(Signature of Officer with stamp of Org./Office)

Office Email:

TO BE FILLED BY RA OFFICE

The above details have been verified and found to be correct.

Signature of RA Office

Name:

Date:

12.3 Form for an Individual type of Certificate

TATA CONSULTANCY SERVICES LIMITED – CERTIFYING AUTHORITY

REQUEST FORM FOR CLASS-2/3 CERTIFICATE

User Type – Individual

Affix recent passport-size photograph of the applicant. Applicant to sign across the photograph.

Instructions:

7. Please fill the form in BLOCK LETTERS
8. Items marked with * are mandatory.
9. For the items marked with # (Details for at least one are mandatory)

DETAILS TO BE FILLED IN BY THE APPLICANT: *

FULL NAME *

Last Name/Surname

First Name

Middle Name

GENDER *(Tick as applicable)

Male ☐ Female ☐

Residential Address *

Pin Code

Mobile Phone No.

Telephone No. --

Area Code Telephone No.

Office Address *

Pin Code

Details of at least one are mandatory #

PASSPORT NO. #

VOTER'S IDENTITY CARD NO. #

INCOME TAX PAN NO. #

E-MAIL ADDRESS * (Mandatory - a valid and active email ID that is accessed frequently)

The information provided above in the Request Form for procuring a DSC from TCS-CA is true and correct to the best of my knowledge.

Date Signature of the Applicant

CHECKLIST FOR <u>INDIVIDUAL</u> TYPE OF CERTIFICATE

The following is a list of the supporting documents that you need to submit along with the Certificate Request Form.

<u>NOTE</u> :

- *NOTARIZATION TO BE DONE BY PUBLIC NOTARY/practicing CA / CS*
  or
- *ATTESTATION TO BE DONE BY GAZZETTED OFFICER.*

Sr. No.	Required Documents (Photo copies)	Document submitted	Documents verified by RA
1	**<u>Applicant Verification Documents</u> (any one attested copy required)** • Passport • Voter's ID • Bank Account Details • Driver's license • Ration Card • Any Other		
2	Online Certificate Enrollment Form with Request Number **+** Letter of Authority *(Available for printing on completion of Online Enrollment)* **(Required)**		

Instructions

1. All subscribers are advised to read Certificate Practice Statement of CA.
2. The certificate shall be downloaded onto the same computer / Hardware device (USB token, Smart Card etc.) by login as same computer user account from where the request was initiated.
3. After placing an online request for a certificate, the following activities **shall not** be carried out until the certificate is successfully downloaded:
   - Formatting of the computer
   - Deletion of computer user account used to logon when the request was initiated
   - Reinstallation or upgrade of the Internet browser on the computer from which the certificate request was initiated.
4. If you lose your key pair, you shall inform the RA Administrator immediately and apply for the revocation of your certificate.
5. Application form must be submitted in person.
6. Incomplete/Inconsistent application is liable to be rejected.

Declaration

I hereby confirm that I have read and understood the above instructions and will follow the above instructions for obtaining and using the Digital Signature Certificate.

Date:

Place: **Signature of the Applicant**

TO BE FILLED BY RA OFFICE

The above details have been verified and found to be correct.

Signature of RA Office

Name:

Date:

12.4 Form for an Individual type of CERTIFICATE (Foreign directors)

TATA CONSULTANCY SERVICES LIMITED – CERTIFYING AUTHORITY

REQUEST FORM FOR CLASS-2/3 CERTIFICATE FOR FOREIGN DIRECTORS.

USER TYPE – INDIVIDUAL

Affix recent passport-size photograph of the applicant. Applicant to sign across the photograph.

Instructions:

10. Please fill the form in BLOCK LETTERS
11. Items marked with * are mandatory.
12. For the items marked with # (Details for at least one are mandatory)

DETAILS TO BE FILLED IN BY THE APPLICANT: *

FULL NAME *

Last Name/Surname

First Name

Middle Name

GENDER * (Tick as applicable)

Male ☐ Female ☐

DATE OF BIRTH: ☐☐ ☐☐ ☐☐☐☐

(DD) (MM) (YYYY)

Residential Address *

Pin Code

Country

Telephone No. -

Code Telephone No.

E-MAIL ADDRESS * (Mandatory - a valid and active email ID that is accessed frequently)

The information provided above in the Request Form for procuring a DSC from TCS-CA is true and correct to the best of my knowledge.

Date Signature of the Applicant

Annexure-A: Letter of Authority

This is to certify that. Mr./Ms./Mrs ……. with the residence at……
……
……
……
……
(Residential Address) is maintaining a bank account (A/c NO…….) with our bank……(Bank Name) and operating that account in the normal course of its business/activities. His/Her signature as appearing below is duly attested (as per the records available with bank).

Signature of Authorized Signatory

Name: …….

Designation:……..

Date:

Signature of Branch Manager.

Name: …….

Designation:……..

(**Bank Seal)**

Annexure-B: Letter of Authority

To,
Tata Consultancy Services – Certifying Authority
Tata Consultancy Services Limited
Hyderabad

This is to certify that Mr. / Ms. _____
(Director's name) is a bonafide Director of
_____ (organization name)

Details of Attesting Authority (Company secretary)

Name _____

Profession _____

Professional Membership No _____

Date _____

Place _____

Signature with Stamp/Seal

CHECKLIST FOR <u>INDIVIDUAL</u> TYPE OF CERTIFICATE

The following is a list of the supporting documents that you need to submit along with the Certificate Request Form.

<u>NOTE</u>: NOTARIZATION *TO BE DONE BY NOTARY PUBLIC OF RESPECTIVE COUNTRY.*

Sr. No.	Required Documents (Photo copies)	Document submitted	Documents verified by RA
1(a)	**<u>IN CASE OF FOREIGN DIRECTOR/FOREIGN CITIZEN RESIDING IN INDIA</u> (**Any one or more copies duly NOTARIZED BY **<u>NOTARY PUBLIC</u>** of the respective country, where the Director is resident of**)** **<u>Photo Identification Proof</u>:** • Passport with VISA details • Driving License • Social Security Number • Citizen Card • PAN or Equivalent Tax Card of the respective country, where the Director is Citizen of. **<u>Residence Proof:</u>** • Lease agreement/Property Documents • Telephone Bill • Electricity Bill • Driving License.		

1(b)	**IN CASE OF INDIAN CITIZEN/INDIAN DIRECTOR RESIDING IN ABROAD (**Any one or more copies duly NOTARIZED BY **NOTARY PUBLIC** of the respective country, where the Director is resident of**)** **Photo Identification Proof:** • Passport with VISA details • Driving License • Social Security Number • Citizen Card **Residence Proof:** • Passport copy • Driving License • Electricity Bill • Telephone Bill		
1(C)	**IN CASE OF FOREIGN DIRECTOR/FOREIGN CITIZEN RESIDING IN ABROAD** copies duly NOTARIZED BY **NOTARY PUBLIC** of the respective country, where the Director is resident of**)** **Photo Identification Proof:** (Any One copy) • Passport with VISA details • Driving License • Citizen Card **Residence Proof:** (Any one copy) • Passport with VISA details • Driving License • Electricity Bill • Telephone Bill		
2	Online Certificate Enrollment Form with Request Number.		
3	Annexure-A Letter of Authority duly attested by the Banker where the Director holds valid bank account.		

	(OR) Annexure-B Letter of Authority duly attested by the Company secretary where Director doesn't have bank account.		

Instructions

7. All subscribers are advised to read Certificate Practice Statement of CA.
8. The certificate shall be downloaded onto the same computer / Hardware device (USB token, Smart Card etc.) by login as same computer user account from where the request was initiated.
9. After placing an online request for a certificate, the following activities **shall not** be carried out until the certificate is successfully downloaded:
   - Formatting of the computer
   - Deletion of computer user account used to logon when the request was initiated
   - Reinstallation or upgrade of the Internet browser on the computer from which the certificate request was initiated.
10. If you lose your key pair, you shall inform the RA Administrator immediately and apply for the revocation of your certificate.
11. Application form must be submitted in person.
12. Incomplete/Inconsistent application is liable to be rejected.

Declaration

I hereby confirm that I have read and understood the above instructions and will follow the above instructions for obtaining and using the Digital Signature Certificate.

Date:

Place: **Signature of the Applicant**

TO BE FILLED BY RA OFFICE

The above details have been verified and found to be correct.

Signature of RA Office

Name:

Date:

13 TCS-CA RELYING PARTY AGREEMENT

TATA CONSULTANCY SERVICES - CERTIFYING AUTHORITY
[DIGITAL SIGNATURE CERTIFICATION SERVICES]

THIS IS AN AGREEMENT BETWEEN YOU, THE RELYING PARTY (OR VERIFIER) AND TATA CONSULTANCY SERVICES - CERTIFYING AUTHORITY.

YOU MUST READ THIS AGREEMENT BEFORE VALIDATING OR VERIFYING A DIGITAL SIGNATURE CERTIFICATE OR OTHERWISE ACCESSING OR USING TATA CONSULTANCY SERVICES - CERTIFYING AUTHORITY (TCS-CA) DATABASE OF CERTIFICATE REVOCATIONS AND OTHER INFORMATION IN THE REPOSITORY OF TCS-CA.

THIS RELYING PARTY AGREEMENT (this "Agreement") PROVIDES, AMONG OTHER THINGS, LIMITED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, MERCHANTABLE QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, LIMITS LIABILITY, AND EXCLUDES ALL LIABILITY FOR INCIDENTAL, CONSEQUENTIAL, AND PUNITIVE DAMAGES. YOU MUST ALSO CAREFULLY READ THE TCS-CA TRUST NETWORK CERTIFICATION PRACTICE STATEMENT (CPS) POSTED AT THE TCS-CA WEB SITE (https://www.tcs-ca.tcs.co.in/) AS AMENDED FROM TIME TO TIME, WHICH IS INCORPORATED BY REFERENCE INTO THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THE RELYING PARTY AGREEMENT, YOU ARE NOT AUTHORIZED TO USE THE TCS-CA REPOSITORY.

Agreement

This Relying Party Agreement becomes effective when you submit a query to search for Certificate or to verify a digital signature created with a private key corresponding to a public key contained in a Certificate, or when you other wise use or rely upon any information or service provided by the Tata Consultancy Services Limited - Certifying Authority.

Definitions

Unless otherwise noted herein, defined terms in this agreement shall have the meaning given to them in the then current CPS.

Certification Practice Statement

You acknowledge and agree that your use of the TCS-CA repository and reliance on any Certificate shall be governed by TCS-CA Trust Network Certification Practice Statement as amended from time to time, which is incorporated by reference into this agreement. The CPS is published on the TCS-CA Trust Portal.

Certificate Validation

You acknowledge that you have access to sufficient information to ensure that you can make an informed decision as to the extent to which you will choose to rely on the information in the Certificate.

You are responsible for deciding whether or not to rely on the information in a Certificate.

You are solely responsible for exercising due diligence and responsible judgment before relying on the Certificates and digital signatures. A Certificate is not a grant from any issuing authority or any right or privileges, except as specifically provided in the CPS.

You assume all risks if you rely on an unverifiable digital signature and are not entitled to any presumptions that the digital signature is effective as a signature of the Subscriber.

You may rely upon a digital signature binding the Subscriber if

1. the digital signature was created during the operational period of valid Certificate and it can be verified by cross checking a validated Certificate chain and

2. such reliance is responsible under the circumstances. If the circumstances indicate a need for additional assurance, you may obtain such assurance for such reliance to be reasonable.

Additionally, you should consider the classes and types of Certificates. The final decision concerning whether or not to rely on the verified digital signature is exclusively yours.

You acknowledge and accept that in providing the services as contained in the CPS, neither TCS-CA, Partner for whom Sub-CA has been created (Sub-CA) or Registration Authorities (RAs) shall become a party to any of the dealings or transactions entered into between yourself and the Subscriber and that the services shall be limited to certifying the digital signature of the Subscriber in accordance with the TCS-CA CPS. All claims, of contractual nature or otherwise, resulting from or connected to the dealings or transactions shall be entirely between you and the Subscriber and you shall not hold TCS-CA or any Partner for whom Sub-CA has been created or Registration Authorities or any of their employees and representatives liable.

Disclaimer and Limitations on Obligations of Partner for whom Sub-CA has been created and TCS

EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, PARTNER FOR WHOM SUB-CA HAS BEEN CREATED AND REGISTRATION AUTHORITIES AND TCS-CA DISCLAIM ALL WARRANTIES, CONDITIONS AND OBLIGATIONS OF EVERY TYPE, INCLUDING ANY WARRANTY OR CONDITION OF MERCHANTABILITY, MERCHANTABLE QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY OF THE ACCURACY OF THE INFORMATION PROVIDED, AND IN FUTURE DISCLAIM ANY AND ALL LIABILITY FOR NEGLIGENCE, FAILURE TO WARN, OR LACK OF REASONABLE CARE.

Exclusion of Certain Elements of Damage

IN NO EVENT SHALL ANY PARTNER FOR WHOM SUB-CA HAS BEEN CREATED OR REGISTRATION AUTHORITIES OR TCS-CA BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS

OF DATA, OR OTHER INDIRECT, CONSEQUENTIAL, PUNITIVE DAMAGES, WHETHER OR NOT REASONABLY FORESEEABLE, ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE, NON-PERFORMANCE OR UNAVAILABILITY OF THE CERTIFICATES, DIGITAL SIGNATURES, OR ANY OTHER TRANSACTION OR SERVICES OFFERED OR CONTEMPLATED HEREIN, EVEN IF SUCH REGISTRATION AUTHORITIES , PARTNER FOR WHOM SUB-CA HAS BEEN CREATED OR TCS OR BOTH HAVE BEEN ADVISED OF SUCH DAMAGES.

Damages and Loss Limitations

IN NO EVENT WILL THE AGGREGATE LIABILITY OF ANY REGISTRATION AUTHORITY, PARTNER FOR WHOM SUB-CA HAS BEEN CREATED AND TCS, TO ALL PARTIES (INCLUDING YOU) EXCEED THE APPLICABLE LIABILITY CAP FOR SUCH CERTIFICATE SET FORTH IN THE TABLE BELOW

THE COMBINED AGGREGATE LIABILITY OF ALL REGISTRATION AUTHORITIES , PARTNER FOR WHOM SUB-CA HAS BEEN CREATED AND TCS TO ANY AND ALL PERSONS CONCERNING A SPECIFIC CERTIFICATE SHALL BE LIMITED TO AN AMOUNT NOT TO EXCEED THE FOLLOWING, FOR THE AGGREGATE OF ALL DIGITAL SIGNATURES AND TRANSACTIONS RELATED TO SUCH CERTIFICATES.

Liability Caps

CLASS-1 - No liability
CLASS-2 - INR 5000 (Rupees Five thousand only)
CLASS-3 - INR 10000 (Rupees Ten thousand only)

Private Key Protection

You are hereby notified of the possibility of theft or other form of compromise of a private key corresponding to a public key contained in a Certificate which, may or may not be detected and of the possibility of use of a stolen or compromised key to forge a digital signature to a document.

It is the duty of every Subscriber to exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorized to affect a digital signature of the Subscriber.

Governing Laws

All applicable laws and regulations of India shall govern the enforceability, construction, interpretation and validity of this agreement.

Dispute Resolution

As specified in the IT Act, 2000 prescribed by the Ministry of Communications and Information Technology, Department of Information Technology. Government of India, all disputes between TCS-CA/ PARTNER FOR WHOM SUB-CA HAS BEEN CREATED /RA, the Subscriber and the relying party shall be referred to the Controller of Certifying Authorities for arbitration or resolution.

YOU DEMONSTRATE YOUR KNOWLEDGE AND ACCEPTANCE OF THE TERMS OF THIS AGREEMENT BY SUBMITTING A QUERY TO SEARCH FOR, OR TO VERIFY THE REVOCATION STATUS OF A DIGITAL SIGNATURE CERTIFICATE OR BY OTHER WISE USING OR RELYING UPON ANY INFORMATION OR SERVICES PROVIDED BY THE TCS-CA REPOSITORY OR WEBSITE RELATING TO A CERTIFICATE. IF YOU DO NOT AGREE WITH ANY OF THE TERMS OF THIS AGREEMENT, PLEASE DO NOT SUBMIT A QUERY.

GLOSSARY

ACCEPT (A DIGITAL CERTIFICATE / A DIGITAL SIGNATURE CERTIFICATE)

To demonstrate approval of a Digital Certificate by a Digital Certificate Applicant while knowing or having notice of its informational contents.

ACCESS

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

ACCESS CONTROL

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

ADDRESSEE

A person who is intended by the originator to receive the electronic record but does not include any intermediary.

AFFIRM / AFFIRMATION

To state or indicate by conduct that data is correct or information is true.

AFFIXING DIGITAL SIGNATURE

With its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Digital Signature;

ALIAS

A pseudonym.

APPLICANT (SEE CA APPLICANT; CERTIFICATE APPLICANT)

APPLICATION SOFTWARE

A software that is specific to the solution of an application problem. It is the software coded by or for an end user that performs a service or relates to the user's work.

APPLICATION SYSTEM

A family of products designed to offer solutions for commercial data processing, office and communications environments, as well as to provide simple, consistent programmer and end user interfaces for businesses of all sizes.

ARCHIVE

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

ASSURANCES

Statements or conduct intended to convey a general intention, supported by a good-faith effort, to provide and maintain a specified service. "Assurances" does not necessarily imply a guarantee that the services will be performed fully and satisfactorily. Assurances are distinct from insurance, promises, guarantees, and warranties, unless otherwise expressly indicated.

ASYMMETRIC CRYPTO SYSTEM

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

AUDIT

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

AUDIT TRAIL

A chronological record of system activities providing documentary evidence of processing that enables management staff to reconstruct, review, and examine the sequence of states and activities surrounding or leading to each event in the path of a transaction from its inception to output of fi9nal results.

AUTHENTICATED RECORD

A signed document with appropriate assurances of authentication or a message with a Digital Signature verified by a relying party. However, for suspension and revocation request purposes, the Digital Signature contained in such notification message must have been created by the private key corresponding to the public key contained in the Digital Signature Certificate.

AUTHENTICATION

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

AUTHORITY REVOCATION LIST (ARL)

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

AUTHORIZATION

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

AVAILABILITY

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

BACKUP

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

BINDING

An affirmation by a Certifying Authority of the relationship between a named entity and its public key.

CERTIFICATE

A Digital Signature Certificate issued by Certifying Authority.

CERTIFICATE CHAIN

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

CERTIFICATE EXPIRATION

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

CERTIFICATE EXTENSION

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

CERTIFICATE ISSUANCE

The actions performed by a Certifying Authority in creating a Digital Signature Certificate and notifying the Digital Signature Certificate Applicant (anticipated to become a Subscriber) listed in the Digital Signature Certificate of its contents.

CERTIFICATE MANAGEMENT [MANAGEMENT OF DIGITAL SIGNATURE CERTIFICATE]

Certificate management includes, but is not limited to, storage, distribution, dissemination, accounting, publication, compromise, recovery, revocation, suspension and administration of Digital Signature Certificates. A Certifying Authority designates issued and accepted Digital Signature Certificates as valid by publication.

CERTIFICATE POLICY

A specialized form of administrative policy tuned to electronic transactions performed during Digital Signature Certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of Digital Signature Certificates. Indirectly, a Certificate policy can also govern the transactions conducted using a communications system protected by a Certificate-based security system. By controlling critical Certificate extensions, such policies and associated enforcement

technology can support provision of the security services required by particular applications.

CERTIFICATE REVOCATION (SEE REVOKE A CERTIFICATE)

CERTIFICATE REVOCATION LIST (CRL)

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

CERTIFICATE SERIAL NUMBER

A value that unambiguously identifies a Digital Signature Certificate generated by a Certifying Authority.

CERTIFICATE SIGNING REQUEST (CSR)

A machine-readable form of a Digital Signature Certificate application.

CERTIFICATE SUSPENSION (SEE SUSPEND A CERTIFICATE)

CERTIFICATION / CERTIFY

The process of issuing a Digital Signature Certificate by a Certifying Authority.

CERTIFYING AUTHORITY (CA)

A person who has been granted a license to issue a Digital Signature Certificate under section 24 of Information Technology Act, 2000.

CERTIFYING AUTHORITY SOFTWARE

The cryptographic software required for managing the keys of end entities.

CERTIFYING AUTHORITY SYSTEM

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

CERTIFICATION PRACTICE STATEMENT (CPS)

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

CHALLENGE PHRASE

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

CERTIFICATE CLASS

A Digital Signature Certificate of a specified level of trust.

CLIENT APPLICATION

An application that runs on a personal computer or workstation and relies on a server to perform some operation.

COMMON KEY

Some systems of cryptographic hardware require arming through a secret-sharing process and require that the last of these shares remain physically attached to the hardware in order for it to stay armed. In this case, "common key" refers to this last share. It is not assumed to be secret as it is not continually in an individual's possession.

COMMUNICATION/NETWORK SYSTEM

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

COMPROMISE

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

COMPUTER

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

COMPUTER CENTRE (SEE DATA CENTRE)

COMPUTER DATA BASE

Means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network.

COMPUTER NETWORK

Interconnection of one or more computers through:

i. The use of satellite, microwave, terrestrial line or other communication media; and
ii. Terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.

COMPUTER PERIPHERAL

Means equipment that works in conjunction with a computer but is not a part of the main computer itself, such as printer, magnetic tape reader, etc.

COMPUTER RESOURCE

Means computer, computer system, computer network, data, computer database or software.

COMPUTER SYSTEM

A device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in

conjunction with external files, which contain computer programs, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions.

COMPUTER VIRUS (SEE VIRUS)

CONFIDENTIALITY

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

CONFIRM

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

CONFIRMATION OF DIGITAL SIGNATURE CERTIFICATE CHAIN

The process of validating a Digital Signature Certificate chain and subsequently validating an end-user Subscriber Digital Signature Certificate.

CONTINGENCY PLANS

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

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

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

CONTROLS

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

CORRESPOND

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

CRITICAL INFORMATION

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

CROSS-CERTIFICATE

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

CRYPTOGRAPHIC ALGORITHM

A clearly specified mathematical process for computation; a set of rules that produce a prescribed result.

CRYPTOGRAPHY (*See also* **PUBLIC KEY CRYPTOGRAPHY)**

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

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

DAMAGE

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

DATA

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

DATA BASE (SEE COMPUTER DATABASE)

DATA CENTRE (AS ALSO COMPUTER CENTRE)

The facility covering the computer room, media library, network area, server area, programming and administration areas, other storage and support areas used to carry out the computer processing functions. Usually refers to the computer room and media library.

DATA CONFIDENTIALITY (SEE CONFIDENTIALITY)

DATA INTEGRITY

A condition in which data has not been altered or destroyed in an unauthorized manner. (*See also* THREAT; COMPROMISE)

DATA SECURITY

The practice of protecting data from accidental or malicious modification, destruction, or disclosure.

DEMO CERTIFICATE

A Digital Signature Certificate issued by a Certifying Authority to be used exclusively for demonstration and presentation purposes and not for any secure or confidential communications. Demo Digital Signature Certificates may be used by authorized persons only.

DIGITAL SIGNATURE CERTIFICATE

Means a Digital Signature Certificate issued under sub-section *(4)* of section 35 of the Information Technology Act, 2000.

DIGITAL SIGNATURE CERTIFICATE APPLICANT

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

DIGITAL SIGNATURE CERTIFICATE APPLICATION

A request from a Digital Signature Certificate Applicant (or authorized agent) to a Certifying Authority for the issuance of a Digital Signature Certificate. (*See also* CERTIFICATE APPLICANT; CERTIFICATE SIGNING REQUEST)

DIGITAL SIGNATURE

Means authentication of any electronic record by a Subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of the Information Technology Act, 2000.

DIGITAL SIGNATURE CERTIFICATE

Means a Digital Signature Certificate issued under sub-section *(4)* of section 35 of the Information Technology Act, 2000.

DISTINGUISHED NAME

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

DOCUMENT

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

ELECTRONIC FORM

With reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated microfiche or similar device.

ELECTRONIC MAIL ("E-MAIL")

Messages sent, received or forwarded in Digital form via a computer-based communication mechanism.

ELECTRONIC RECORD

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

ENCRYPTION

The process of transforming plaintext data into an unintelligible form (cipher text) such that the original data either cannot be recovered (one-way encryption) or

cannot be recovered without using an inverse decryption process (two-way encryption).

EXTENSIONS

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

FIREWALL/DOUBLE FIREWALL

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

FILE TRANSFER PROTOCOL (FTP)

The application protocol that offers file system access from the Internet suite of protocols.

FUNCTION

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

GATEWAY

Hardware or software that is used to translate protocols between two or more systems.

GENERATE A KEY PAIR

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

HARD COPY

A copy of computer output that is printed on paper in a visually readable form; e.g. printed reports, listing, and documents.

HASH (HASH FUNCTION)

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

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

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

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

HIGH-SECURITY ZONE

An area, to which access is controlled through an entry point and limited to authorized, appropriately screened personnel and properly escorted visitors. High-Security Zones should be accessible only from Security Zones, and are separated from Security Zones and Operations Zones by a perimeter. High-Security Zones are monitored 24 hours a day a week by security staff, other personnel or electronic means.

IDENTIFICATION / IDENTIFY

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

IDENTITY

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

INFORMATION

Includes data, text, images, sound, voice, codes, computer programs, software and databases or microfilm or computer generated microfiche.

INFORMATION ASSETS

Means all information resources utilized in the course of any organization's business and includes all information, application software (developed or purchased), and technology (hardware, system software and networks).

INTERMEDIARY

With respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.

INFORMATION TECHNOLOGY SECURITY

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

INFORMATION TECHNOLOGY SECURITY POLICY

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

KEY

A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, Signature generation, or Signature verification).

KEY GENERATION

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

KEY MANAGEMENT

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

KEY PAIR

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

LICENCE

Means a license granted to a Certifying Authority.

LOCAL AREA NETWORK (LAN)

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

MANAGEMENT OF DIGITAL SIGNATURE CERTIFICATE [SEE CERTIFICATE MANAGEMENT]

MEDIA

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

MESSAGE

A Digital representation of information; a computer-based record. A subset of RECORD. (*See also* RECORD)

NAME

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

NETWORK

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

NETWORK ADMINISTRATOR

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

NODE

In a network, a point at which one or more functional units connect channels or data circuits.

NOMINATED WEBSITE

A website designated by the Certifying Authority for display of information such as fee schedule, Certification Practice Statement, Certificate Policy etc.

NON-REPUDIATION

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

NOTARY

A natural person authorized by an executive governmental agency to perform notarial services such as taking acknowledgements, administering oaths or affirmations, witnessing or attesting Signatures, and noting protests of negotiable instruments.

ON-LINE

Communications that provide a real-time connection.

OPERATIONS ZONE

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

OPERATIONAL CERTIFICATE

A Digital Signature Certificate which is within its operational period at the present date and time or at a different specified date and time, depending on the context.

OPERATIONAL MANAGEMENT

Refers to all business/service unit management (i.e. the user management) as well as Information Technology management.

OPERATIONAL FIELD

The period starting with the date and time a Digital Signature Certificate is issued (or on a later date and time if stated in the Digital Signature Certificate) and ending with the date and time on which the Digital Signature Certificate expires or is suspended or revoked.

ORGANIZATION

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

ORIGINATOR

A person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.

PASSWORD (PASS PHRASE; PIN NUMBER)

Confidential authentication information usually composed of a string of characters used to provide access to a computer resource.

PC CARD (SEE ALSO SMART CARD)

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

PERSON

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

PERSONAL PRESENCE

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

PKI (PUBLIC KEY INFRASTRUCTURE) / PKI SERVER

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

PKI HIERARCHY

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

PLEDGE (SEE SOFTWARE PUBLISHER'S PLEDGE)

POLICY

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

Introduction

Definitions

Policy Statement identifying the need for "something" (e.g. data security)

Scope

People playing a role and their responsibilities

Statement of Enforcement, including responsibility

PRIVATE KEY

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

PROCEDURE

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

PROGRAM

A detailed and explicit set of instructions for accomplishing some purpose, the set being expressed in some language suitable for input to a computer, or in machine language.

PROXY SERVER

A server that sits between a client application such as a web browser and a real server. It intercepts all requests to the real server to see if it can fulfill the request itself. If not, it forwards the request to the real server.

PUBLIC ACCESS ZONE

Generally surrounds or forms part of a government facility. Examples include the grounds surrounding a building, and public corridors and elevator lobbies in multiple-occupancy buildings. Boundary designators such as signs and direct or remote surveillance may be used to discourage unauthorized activity.

PUBLIC KEY

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

PUBLIC KEY CERTIFICATE (*See* CERTIFICATE)

PUBLIC KEY CRYPTOGRAPHY (*See* CRYPTOGRAPHY)

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

PUBLIC KEY INFRASTRUCTURE (PKI)

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

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

RECIPIENT (of a **DIGITAL SIGNATURE)**

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

RECORD

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

RE-ENROLLMENT (*See also* **RENEWAL)**

RELYING PARTY

A recipient who acts in reliance on a Certificate and Digital Signature.

RENEWAL

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

REPOSITORY

A database of Digital Signature Certificates and other relevant information accessible on-line.

REPUDIATION (*See also* **NONREPUDIATION)**

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

REVOKE A CERTIFICATE

The process of permanently ending the operational period of a Digital Signature Certificate from a specified time forward.

RISK

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

RISK ANALYSIS

The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards.

RISK ASSESSMENT

An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events.

RISK MANAGEMENT

The total process of identifying, controlling, and eliminating or MINIMISING uncertain events that may affect information technology system resources.

RSA

A public key cryptographic system invented by Rivest, Shamir & Adelman.

SECRET SHARE

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

SECRET SHARE HOLDER

An authorized holder of a physical token containing a secret share.

SECURE CHANNEL

A cryptographically enhanced communications path that protects messages against perceived security threats.

SECURE SYSTEM

Means computer hardware, software, and procedure that—

(a) Are reasonably secure from unauthorized access and misuse;

(b) Provide a reasonable level of reliability and correct operation;

(c) Are reasonably suited to performing the intended functions; and

(d) Adhere to generally accepted security procedures.

SECURITY PROCEDURE

Means the security procedure prescribed under section 16 of the Information Technology Act, 2000.

SECURITY

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

SECURITY POLICY

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

SECURITY SERVICES

Services provided by a set of security frameworks and performed by means of certain security mechanisms. Such services include, but are not limited to, access control, data confidentiality, and data integrity.

SECURITY ZONE

An area to which access is limited to authorized personnel and to authorized and properly escorted visitors. Security Zones should preferably be accessible from an Operations Zone, and through a specific entry point. A Security Zone need not be separated from an Operations Zone by a secure perimeter. A Security Zone should be monitored 24 hours a day and 7-week by security staff, other personnel or electronic means.

SERIAL NUMBER (*See* CERTIFICATE SERIAL NUMBER)

SERVER

A computer system that responds to requests from client systems.

SIGN

To create a Digital Signature for a message, or to affix a Signature to a document, depending upon the context.

SIGNATURE (*See* DIGITAL SIGNATURE)

SIGNER

A person who creates a Digital Signature for a message or a Signature for a document.

SMART CARD

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

S/MIME

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

SUBJECT (OF A CERTIFICATE)

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

SUBJECT NAME

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

SUBSCRIBER

A person in whose name the Digital Signature Certificate is issued.

SUBSCRIBER AGREEMENT

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

SUBSCRIBER INFORMATION

Information supplied to a Certifying Authority as part of a Digital Signature Certificate application. (*See also* CERTIFICATE APPLICATION)

SUSPEND A CERTIFICATE

A temporary "hold" placed on the effectiveness of the operational period of a Digital Signature Certificate without permanently revoking the Digital Signature Certificate. A Digital Signature Certificate suspension is invoked by, *e.g.,* a CRL entry with a reason code. (*See also* REVOKE A CERTIFICATE)

SYSTEM ADMINISTRATOR

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

SYSTEM SECURITY

A system function that restricts the use of objects to certain users.

SYSTEM SOFTWARE

Application-independent software that supports the running of application software. It is a software that is part of or made available with a computer system and that determines how application programs are run; for example, an operating system.

TEST CERTIFICATE

A Digital Signature Certificate issued by a Certifying Authority for the limited purpose of internal technical testing. Only authorized persons can use Test Certificates.

THREAT

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

TIME-OUT

A security feature that logs off a user if any entry is not made at the terminal within a specified period of time.

TIME STAMP

A notation that indicates (at least) the correct date and time of an action, and identity of the person or device that created the time stamp

TOKEN

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

TRANSACTION

A computer-based transfer of business information, which consists of specific processes to facilitate communication over global networks.

TRUST

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

TRUSTED POSITION

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

TRUSTED THIRD PARTY

In general, an independent, unbiased third party that contributes to the ultimate security and trustworthiness of computer-based information transfers. A trusted third party does not connote the existence of a trustor-trustee or other fiduciary relationship. (*Cf.,* TRUST)

TRUSTWORTHY SYSTEM

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

TYPE (OF CERTIFICATE)

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

UNAMBIGUOUS NAME (*See* DISTINGUISHED NAME)

UNIFORM RESOURCE LOCATOR (URL)

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

USER

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

VALID CERTIFICATE

A Digital Signature Certificate issued by a Certifying Authority and accepted by the Subscriber listed in it.

VALIDATE A CERTIFICATE (*i.e.,* of an END-USER SUBSCRIBER CERTIFICATE)

The process performed by a recipient or relying party to confirm that an end-user Subscriber Digital Signature Certificate is valid and was operational at the date and time a pertinent Digital Signature was created.

VALIDATION (OF CERTIFICATE APPLICATION)

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

VALIDATION (OF SOFTWARE) (*See* SOFTWARE VALIDATION)

VERIFY (A DIGITAL SIGNATURE)

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

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

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

VIRUS

Means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource.

VULNERABILITY

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

WEB BROWSER

A software application used to locate and display web pages.

WORLD WIDE WEB (WWW)

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

WRITING

Information in a record that is accessible and usable for subsequent reference.

X.509

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

APPENDIX – A

TCS-CA Document Master List

The following are the documents available for Tata Consultancy Services Limited Certifying Authority Operations and Public Key Infrastructure.

Document Number	Document Name
TCS-CA-02	Technical Specification
TCS-CA-04	Certifying Authority Manual
TCS-CA-05	Certifying Authority Operations Manual
TCS-CA-07	Computer Security Policy Manual
TCS-CA-08	Cross Certification Arrangement Procedures Manual
TCS-CA-09	Disaster Recovery and Business Continuity Plan
TCS-CA-12	Employee Services Termination Trace
TCS-CA-13	H/W and S/W Inventory Master List
TCS-CA-16	Induction Manual
TCS-CA-17	Induction Trace
TCS-CA-18	Key Management Procedures Manual
TCS-CA-23	RA Operations Manual
TCS-CA-24	Security Architecture
TCS-CA-25	Responsibilities of Security Personnel
TCS-CA-26	Subscriber Confidentiality Procedures Manual
TCS-CA-27	System Security Audit Procedures Manual
	Gold Book: System-related Procedures
	Green Book: Operations
	Orange Book: Security

CONTACT

For clarifications related to the TCS-CA Trust Network Certification Practice Statement, email our Help Desk.

✉ **helpdesk@tcs-ca.tcs.co.in**

To learn more about Digital Certificates, PKI Products and Services, visit the Tata Consultancy Services – Certifying Authority Trust Portal.

💻 **https://www.tcs-ca.tcs.co.in**

TATA CONSULTANCY SERVICES