Certification Practice Statement of CSL-CA

Document Version Control

Document version no:	1.0.2	**Total number of pages :**	69
Document Status :	☒ Draft	☐ Final Version	
Drafter :	Sakil Md Tarikul Islam	Computer Services Ltd CA	

Diffusion list :	☒ External	☒ Internal CSL	
		Sakil Md Tarikul Islam Momluk Sabir Ahmed	CSL CA CSL CA

Document history:				
Date	Version	Drafter	Comments	Verified by
2010/09/26	1.0.1	Jihan Bushra Jaman	Creation of the document	Momluk Sabir Ahmed
2020/11/15	1.0.2	Sakil Islam	Creation of the document	Momluk Sabir Ahmed

Table Of Contents

Section 1

1 Section 1: Introduction

1.1 Overview

This document is the Certification Practice Statement (CPS) of the Computer Services CA. The CPS states the practices that Computer Services CA employs in providing certification services as per the Information and Technology Act 2006 (amended in 2013) and Information Technology (Certificate Authority) Rules 2010 of the Bangladesh Government. This document also details security processes to be followed by subscribers, relying parties, and the system architecture. This document presents reliable information to subscribers and to the reliable parties. CSL-CA certificates are trustworthy and lawfully valid as per the above Act. The use of certificates issued by CSL-CA shall be consistent with all applicable laws, rules and regulations. Any other types of usage are prohibited.

Computer Services CA offers the following services:

- Receiving Certificate requests
- Verification of the individuals and organizations based on the class of certificate request
- Certificate generation
- Certificate signing
- Certificate issue
- Certificate publication
- Certificate revocation
- Certificate suspension and activation of suspended certificates

It is assumed that the reader is generally familiar with Digital Signature Certificate (DSC), Digital Signature, Public Key Infrastructure (PKI) and networking

1.2 Document Name and Identification

Document Name – CSL-CA CPS

Document Version – 1.0.2

OID – 2.16.50.1.9

This document is published at www. ca.computerservicesltd.com

PKI Participants

1.2.1 Certification Authority

CSL-CA is licensed certificate authority in Bangladesh that derives its trust from root CA of Bangladesh. CSL-CA PKI involves the following participants:

1.2.2 Registration Authorities

Registration Authority (RA) of CSL-CA – CSL-CA certificates will be issued to entities and subscribers in multiple regions, number of registration authorities will be set up to carry out the verification, process the certificate applications and certificate revocation requests.

1.2.3 Subscribers

CSL-CA subscribers are the persons or entities that have obtained the certificates after due verification of their identity by CSL-CA or its RAs.

1.2.4 Relying Parties

Relying parties of CSL-CA are those who use the certificates issued by CSL-CA to verify the identity of the subscribers when they perform secure electronic communication. The relying parties may or may not be the subscribers

1.3 Certificate Usage

1.3.1 Appropriate Uses

There are three classes of the certificates issued by CSL_CA and their usage shall be as below:

Class 1 Certificate	Shall be used for signing or encrypting the personal emails
Class 2 Certificate	Besides the usage mentioned for Class 1 Certificates, these certificates shall be used for digitally signing file/form/transaction, client authentication
Class 3 Certificate	Besides the usage mentioned for Class 2 Certificates, these certificates shall be used for server authentication or similar services, code signing, time-stamping service and high value transactions

1.3.2 Prohibited Certificate Use

It is prohibited to use the above certificate to sign other certificates. It is also prohibited use the certificates for the purposes other than those specified in section 1.3.1

1.4 Policy Administration

Details of administering the document are found in this subsection

1.4.1 Document Administration

This CPS document is administrated by CSL-CA .

Email: admin@ca.computerservicesltd.com

Phone: +88 02 9890719

Fax: +88 02 9891132

1.4.2 Contact person

Contact Person Name: Momluk Sabir Ahmed

Email: sabir@computerservicesltd.com

Phone: + 88 01678090022

Fax: + 88 02 9891132

1.4.3 CPS Approvals

This document is approved by

- CSL-CA Policy approval committee
- CSL-CA legal department
- However this document is final after endorsement by Controller of Certifying Authorities, Bangladesh.

Document Maintenance

This document is maintained by CSL-CA. Any questions regarding CSL-CA services may be sent to: admin@ca.computerservicesltd.com

1.4.4 CPS Approval Procedures

The CPS is initially approved by CSL-CA Policy approval committee and CSL-Legal department. After that it submitted to CCA for their approval

1.5 Acronyms

CA Certification Authority
CMA Certificate Management Authority
CP Certificate Policy
CPS Certification Practice Statement
CRL Certificate Revocation List
CA Certification Authority
CMA Certificate Management Authority
CP Certificate Policy
CPS Certification Practice Statement
CRL Certificate Revocation List
CSA Certificate Status Authority
CSOR Computer Security Objects Registry
DES Data Encryption Standard
DN Distinguished Name
DSA Digital Signature Algorithm
DSS Digital Signature Standard
ECA External Certification Authority
EPMA ECA Policy Management Authority
FBCA Federal Bridge Certification Authority
FIPS Federal Information Processing Standard
HSM Hardware Security Module
PKI Public Key Infrastructure
I&A Identification and Authentication
ID Identity (also, a credential asserting an identity)
ISO International Organization for Standards
KRP Key Recovery Policy
KRPS Key Recovery Practice Statement
LDAP Lightweight Directory Access Protocol
OCSP Online Certificate Status Protocol
OID Object Identifier
PIN Personal Identification Number
PKCS Public Key Certificate Standard
RA Registration Authority
RFC Request For Comment
RSA Rivest, Shamir, Adelman (encryption and digital signature algorithm)
S/MIME Secure Multipurpose Internet Mail Extensions
SSL Secure Socket Layer
TSA Time Stamping Application

Section 2:

2 Section 2: Publication and Repository Responsibilities

CSL-CA repository include latest version of CSL-CA CPS, Certificates, CRLs. The repository of certificates and CRLs will be hosted in an LDAP directory

2.1 Repositories:

CSL-CA maintains a repository of certificates it issues and a Certificate Revocation List (CRL) for the certificates it revoked or suspended. CSL-CA publishes and issues certificates in the CSL-CA repository. Revocation data on issued digital certificates is published at a location of the CRL distribution point specified in the certificate. All the certificate information is published in a dedicated CSL-CA LDAP directory server. The LDAP directory server is publicly available. The repository is available at CSL-CA website www.ca.computerservicesltd.com

2.2 Publication of certificate information

. The latest version of CPS shall be published in the repository

. A copy of the digital certificate is published in the LDAP repository as soon as a certificate is issued.

. The CRLs shall be published and updated in the CSL-CA repository.

2.3 Time and Frequency of publication

. The latest version of CPS shall be published in the repository within reasonable time upon its approval as mentioned in section 1.4.4.

. A copy of the digital certificate is published in the repository as soon as a certificate is issued.

. The CRLs shall be published and updated in the CSL-CA repository once every business working day

2.4 Access Controls on Repositories

. The information in the repository consisting of CSL-CA CPS, certificate policy definitions, issued digital certificates and CRLs are publicly accessible without any restriction. This information is read only. CSL-CA reserves the right to make the modifications to CSL-CA CPS subject to necessary approvals.

. Subscribers, relying parties or others accessing the CSL-CA repository and other published resources are deemed to have agreed with the provisions of this CPS and any other conditions of usage that CSL-CA may make available.

SECTION 3

3 Section 3: NOTIFICATION AND AUTHENTICATION

3.1 Naming

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

3.1.1 Types of names

Each subscriber will be represented by a clearly distinguishable and unique X.509 V3 Distinguished Name (DN) in the certificate subject name field.

The DN shall be in the form of printable string or such other form but will not be blank

3.1.2 Need for names to be meaningful

3.1.2.1 ***The "Subject Name" field in the digital certificate must be associated with the name of the Subscriber***

3.1.2.2 In the case of individuals the Common Name (CN) attribute of the DN contains the legal name as presented in the government issued photo-identification

3.1.2.3 For server certificates the Common Name attribute of the DN contains the fully qualified name of the server.

3.1.2.4 The DN may also include organization position or role

3.1.2.5 If the certificate refers to a role or position, the certificate may also contain the identity of the person who holds that role or position.

3.1.3 Anonymity or pseudonymity of subscribers

CSL-CA does not issue anonymous or pseudonymous certificates

3.1.4 Rules for Interpreting Various Name Forms

The Distinguished Name (DN) will include the following details:

- Common Name (CN) = Common name that is unique for every subscriber
- Organization (O) = Organization Name (entity name as registered)
- Organizational Unit (OU) = Organizational units distinguished within an organization

- Locality (L) = Town/City of the subscriber
- State or Province (SP) = State or province to which the subscriber belongs
- Email (E) = Email address of the certificate holder
- Phone Number (Phone) = Contact number of the certificate holder
- The attributes in the distinguished name (DN) CN, O, C,E are mandatory.

3.1.5 Uniqueness of names

DN must be unique for all subscribers of CSL-CA. CSL-CA adopts the unique identifier so that subscribers with identical names can be supported.

3.1.6 Recognition, authentication, and role of trademarks

The use of trademarks will be reserved to registered trademark holders. Proper documentary proof of such ownership must be produced to CSL-CA.

3.2 Initial identity validation

The process of identification of a subscriber will differ based on the class of certificate that the subscriber is applying for and may include the following:
Verification of email, postal address, face to face authentication and verification of stipulated documents. An application for a certificate must be made personally by an individual or by duly authorized representative of the subscriber.

3.2.1 Method to prove possession of private key

Subscriber generates his/her own key pair and submits the public key in PKCS#10 format to CSL-CA, which establishes that the subscriber possesses the corresponding private key

3.2.2 Authentication of organization identity

An Identification in the form of authority letter from employer organization will be required for organization identity. The authentication process is dependent on class of digital certificate being issued and the process will differ accordingly.

3.2.3 Authentication of individual identity

The authentication process is dependent on class of certificate being issued. The authentication process may include face to face identity verification. The acceptable documentation for face to face identity verification of the subscriber shall include:

- Name,
- Photograph,
- Signature,
- Postal address proof like phone bill or utility bill
- National ID or passport
- Additional document may be asked by CSL-CA or its RA

3.2.4 Non-verified subscriber information

Unverified information shall not be included in the certificates

3.2.5 Validation of authority

Certificates that contain explicit or implicit organizational affiliation shall be issued only after ascertaining the applicant has the authorization to act on behalf of the organization in the asserted capacity.

For certificates issued at the request of a Subscriber's agent, both the agent and the Subscriber shall jointly and severally indemnify and hold harmless CSL-CA, and its parent companies, subsidiaries, directors, officers, employees, agents, and contractors. The Subscriber shall control and be responsible for the data that an agent of the Subscriber supplies CSL-CA. The Subscriber must promptly notify CSL-CA of any misrepresentations and omissions made by an agent of the Subscriber. The duty of this article is continuous.

3.2.6 Criteria for interoperation

Certificates shall be issued in accordance with CCA interoperability guidelines.

3.2.7 Identification and authentication for re-key requests

CSL-CA Certification Services support Certificate renewal in the mode of rekey. Subscribers may request Certificate renewal provided that:

- Content of Certificate information as contained in the registration records has not been changed.
- The request is made before the expiry of their current certificates.
- Their current certificates have not been revoked.
- They are not listed in the compromised user.
- Their keys are not included as the compromised keys

For continuity of the certificate, the subscriber has to obtain a new certificate to maintain the continuity of the certificate before it expires

3.2.8 Identification and authentication for routine re-key

Subscribers will need to re-apply after the expiration of existing certificate. Subscribers shall generate a new private-public key pair on a trustworthy medium and complete the initial registration process again.

CSL-CA or its RA may put reasonable efforts to inform the subscriber in advance about the expiration of the certificate.

3.2.9 Identification and authentication for re-key after revocation

Once a digital certificate has been revoked, for whatever reason, the subscriber will be required to begin the request process afresh if they require a new digital certificate.

3.3 Identification and authentication for revocation request

(Refer to procedure for revocation Request)

Section 4

4 Section 4: CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

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

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

Certificate applications must be submitted by the individual who is the subject of the certificate or by persons who are duly authorized to request a certificate on behalf of the applicant.

4.1.2 Enrollment process and responsibilities

CSL CA makes the provision for both online/offline enrollment of the subscribers for issuing the digital certificates. The enrollment process requires submission of the duly filled application form along with the supporting documents. The procedure depends on the class of certificate requested. For detailed description please see Appendix-A

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

A Certificate applicant must complete an application in the prescribed format obtained from the CSL. The application form has to be filled in by the Applicant. The applicant is required to send only one copy to CSL. However the applicant is advised to retain a copy of the same which shall be required while filling up of online information for key pair generation.

CSL CA validate that:

- The certificate applicant/subscriber has agreed to terms and conditions
- The applicant/subscriber is the persons identified in the request
- Veracity of the information listed in the application

Please see appendix-A for detailed issuance/distribution procedure

4.2.2 Approval or rejection of certificate applications

After successful completion of all required validations of the certificate application, CSL-CA will approve the application for digital certificate. If the information in the certificate application is not confirmed, the application will be rejected. CSL-CA reserves the right to reject an application for a certificate if CSL-CA assesses that it diminishes the trust of the CSL-CA brand, without incurring any liability, responsibility for any loss or expense arising out of such refusal. CSL-CA reserves the right not to disclose reasons for such refusal.

The applicants whose applications have been rejected may reapply subsequently.

4.2.3 Time to process certificate applications

CSL-CA makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame. The time frame is greatly dependent on the applicant providing the necessary details and documentation in a timely manner. Upon the receipt of the necessary details and documentation, CSL CA aims to confirm submitted application data and to complete the validation process and issue or reject a certificate application within ten (10) working days.

Occasionally, events outside of the control of CSL CA may delay the issuance process. However, CSL CA will make every reasonable effort to meet its issuance times and to make applicants aware of any factors that may affect issuance times.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Please see Appendix A for a detailed account of the issuance/distribution procedure for each class of digital certificate.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Please see Appendix A for a detailed account of the issuance/distribution procedure for each class of digital certificate.

4.4 Certificate acceptance

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

4.4.1 Conduct constituting certificate acceptance

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

The subscriber is responsible for installing the issued certificate on the subscriber‟s computer or hardware security module according to the subscriber's system specifications. A subscriber is deemed to have accepted a certificate upon downloading the certificate
In the event of any actual or suspected loss, disclosure or other Compromise of the Subscriber‟s Private Key the Subscriber will request that the Certificate be revoked and recreated. Any revocation will be done in accordance with this CPS.

4.4.2 Publication of the certificate by the CA

CSL-CA publishes the certificate in its repository upon delivering it to the subscriber

4.4.3 Notification of certificate issuance by the CA to other entities

Respective RA who handled the communication with the subscriber will be notified of the certificate issuance

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

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

4.5.2 Relying party public key and certificate usage

Relying party may rely on a Certificate that references this CPS only if the Certificate is used and relied upon for usage in applications mentioned.

It is the sole duty of relying party to verify the purpose for which a certificate is used and these purposes should be in line with the purpose for which certificate is issued.

- The reliance is reasonable and in good faith in light of all the circumstances known to the relying party at the time of the reliance.
- The Certificate is used exclusively for purposes mentioned in the Certificate.
- The purpose for which the Certificate is used is appropriate under this CPS.
- The Certificate is being used within its operational period.
- The relying party checked the status of the Certificate by using the CRL published in the repositories prior to reliance, or a check of the Certificate‟s status would have indicated that the Certificate was valid.

4.6 Certificate renewal

The subscribers of the CSL-CA shall be issued a certificate by CSL-CA for a specific period of time. Before or after expiration of the certificate the subscribers will generate new public-private key pair and submit the public key along with new application to CSL-CA for renewal.

4.6.1 Circumstance for certificate renewal

The certificate can be requested one month before expiry of the certificate

4.6.2 Who may request renewal

Any existing subscriber of CSL-CA can request the renewal of certificate

4.6.3 Processing certificate renewal requests

Subscribers need to submit the application and supporting documents for renewal of the certificate. The requests will be processed as mentioned in Section 4.2

4.6.4 Notification of new certificate issuance to subscriber

Subscribers will be intimated by mail or through RAs about the issuance of the new certificate

4.6.5 Conduct constituting acceptance of a renewal certificate

Refer to section 4.4.1

4.6.6 Publication of the renewal certificate by the CA

Refer to section 4.4.2

4.6.7 Notification of certificate issuance by the CA to other entities

Refer to section 4.4.3

4.7 Certificate re-key

The validity period associated with a digital certificate will be dependent on the digital certificate class in question. The CSL-CA will provide a facility to renew digital certificates that are just about to expire.
The frequency at which digital certificates are reissued/ rolled over is dependent on the class of digital certificates in question.

4.7.1 Circumstance for certificate re-key

Subscribers must regenerate their key pair in the following circumstances:

- Expiration of their certificate signed by the CSL CA;
- Revocation of their certificate by the CSL CA;

4.7.2 Who may request certification of a new public key

Prior to the expiration of an existing Subscriber‟s Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. CSL-CA requires that the Subscriber generate a new key pair to replace the expiring key pair.

Subscribers may request Certificate renewal provided that:

- Content of Certificate information as contained in the registration records has not been changed.
- The request is made before the expiry of their current certificates.

- Their current certificates have not been revoked.
- They are not listed in the compromised user.
- Their keys are not included as the compromised keys.

4.7.3 Processing certificate re-keying requests

Expiration warnings will be sent to subscribers before it is re-key time.

- Re-key after certificate expiration uses completely the same authentication procedure as that for the new certificate.
- At least once every 3 years the subscriber must go through the same authentication procedure as the one described for a new certificate.
- In case the request for a new certificate is due to revocation of certificate the subscriber must follow the same procedure as the one described in for a new one.

4.7.4 Notification of new certificate issuance to subscriber

Refer to Appendix A

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Refer to section 4.4.1

4.7.6 Publication of the re-keyed certificate by the CA

Refer to section 4.4.2

4.7.7 Notification of certificate issuance by the CA to other entities

Refer to section 4.4.3

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

No stipulation

4.8.2 Who may request certificate modification

No stipulation

4.8.3 Processing certificate modification requests

No stipulation

4.8.4 Notification of new certificate issuance to subscriber

No stipulation

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation

4.8.6 Publication of the modified certificate by the CA

No stipulation

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation

4.9 Certificate revocation and suspension

Suspension is the process of making a certificate invalid temporarily, pending certain investigations. In such situations, CSL-CA revokes the certificate as suspension of certificate is not supported by CSL-CA. Revocation is the process of making a certificate to be invalid permanently. The revoked certificates cannot be reused and are listed in the CRL.

CSL- CA reserves the right to revoke any of its issued digital certificates as per IT (CA) Rules 2010 or as instructed by the CCA. As per, the revoked Electronic Signature Certificate shall be added to the Certificate Revocation List (CRL). All revocation information is published and held in LDAP directory server where it is made publicly available when required for certificate verification processes.

4.9.1 Circumstances for revocation

A digital certificate will be revoked in the following instances on notification:

- A material fact represented in the certificate is false and has been concealed
- CSL-CA private key or security system is compromised
- Subscriber"s private key corresponding to the public key in that certificate has been compromised
- Information in the digital certificate is changed
- The subscriber has breached or failed to meet his obligations under this CPS, or any other agreement, regulation or law that may be in force
- Misuse of the Electronic Signature Certificate
- Electronic Signature Certificate is no longer required
- Upon death or insolvency of the subscriber
- Upon dissolution of the firm or winding up of the company, where the subscriber is a firm or a company
- Where the subscriber or any other person authorized by him makes request to that effect
- Any other circumstances as may be determined by CSL-CA from time to time in accordance with any requirements, rules or regulations of the governing law.

4.9.2 Who can request revocation?

The following entities may request revocation of a subscriber digital certificate:

- The subscriber in whose name certificate has been issued
- The duly authorized representative of the subscriber
- Authorized personnel of CSL-CA or RA when subscriber has breached the agreement, regulation or law that may be in force
- The CSL-CA RA, on behalf of the individual subscriber.
- Any other entity holding evidence of a revocation circumstance about that certificate

4.9.3 Procedure for revocation request

4.9.3.1 ***Hand Delivery or Courier***

i. Subscriber will download revocation request form from CSL-CA website at www.ca.computerservicesltd.com or collect from CSL-CA office or CSL-CA RA office
ii. Subscriber will duly fill in the form and hand sign it
iii. Duly filled in and signed form will either be couriered or hand delivered to CSL-CA office
iv. CSL-CA will verify the information contained in the revocation request with the issued certificate and application form.
v. In the event of mismatch the subscriber will be intimated accordingly through email and revocation request will not be processed

4.9.3.2 ***Online:***

I. An email with revocatioin form in an attachment will be sent to CSL-CA helpdesk at helpdesk@ca.computerservicesltd.com with subject line "Revocation Request". The subscriber shall encrypt this transaction by using the public key of CSL-CA. It shall be digitally signed by the subscriber even though the private key may have already been compromised
II. CSL-CA shall verify the information and will proceed for revocation as per the revocation grace period.
III. In the event of mismatch the subscriber will be intimated accordingly through email and revocation request will not be processed

4.9.4 Revocation request grace period

Table below gives the time frame available as revocation request grace period

Class of Certificate	Revocation	CRL publication with revoked certificate
Class 1, 2 & 3	On receipt of the revocation request and information in the prescribed format, CSL-CA will decide acceptance / rejection of the revocation request. After determining suitable acceptability, CSL-CA will revoke the certificate and shall update and publish the CRL in the repository once every business working day	The revoked certificate will be updated in the CRL which would be published in the repository once every business working day

4.9.5 Time within which CA must process the revocation request

CSL- CA will process all revocation requests within 1 working day.

4.9.6 Revocation checking requirement for relying parties

Relying parts must download the CRL from the online-repository at least once a day and implement its restrictions while validating certificates.

4.9.7 CRL issuance frequency (if applicable)

Refer to section 4.9.4

4.9.8 Maximum latency for CRLs (if applicable)

No stipulation

4.9.9 On-line revocation/status checking availability

CSL-CA hosts a dedicated LDAP directory server for verifying the status of Certificates issued within the CSL-CA. Details of the directory path will be provided in the CSL-CA certificate. The public will have access to the information contained within this directory.

4.9.10 On-line revocation checking requirements

CRL checking is the responsibility of the relying party whenever a transaction takes place. An entity that downloads a CRL from a repository shall verify the authenticity of the CRL by checking its digital signature and the associated certification path.

4.9.11 Other forms of revocation advertisements available

No stipulation

4.9.12 Special requirements re key compromise

No stipulation

4.9.13 Circumstances for suspension

CSL-CA does not support suspension

4.9.14 Who can request suspension

CSL-CA does not support suspension

4.9.15 Procedure for suspension request

CSL-CA does not support suspension

4.9.16 Limits on suspension period

CSL-CA does not support suspension

4.10 Certificate status services

4.10.1 Operational characteristics

CSL CA operates an on-line LDAP repository that contains all the certificates have been issued. The repository also contains CRL list. Promptly following revocation, the certificates and CRL status in the repository, as applicable, shall be updated.

4.10.2 Service availability

The on-line repository is maintained on best effort basis with intended availability of 24x7.

4.10.3 Optional features

No stipulation

4.11 End of subscription

No stipulation

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

CSL-CA will not escrow the private keys of subscribers

4.12.2 Session key encapsulation and recovery policy and practices

No Stipulation

Section 5

5 Section 5: Facility, Management and Operational Controls

5.1 Physical Controls

CSL-CA hosts it CA in a site that has been designed and built to ensure reasonable protection is maintained. They facility is protected from unauthorized access by access control and surveillance system.

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

5.1.1 Site location and construction

CSL-CA operates its main facility in Dhaka, Bangladesh in its own premises. Operations are carried out in a physically secured environment The site is equipped with surevellance system, environmental controls like fire protection, HVAC. This site is protected 24x7 by trained professional guards. In addition to this, there are certain areas of the location that require two specific individuals to be authenticated before access is granted.

- Remote surveillance system equipped with camera
- 24x7 trained professional guard to secure the datacenter

5.1.2 Physical access

The CSL-CA has implemented necessary physical security controls to restrict access to the CSL-CA Hardware and Software. The controls are applied to the CSL-CA servers, workstations and other devices used for performing the CA operations. The control includes physical and electronic locks to prevent penetration. The access to the CSL-CA facility is limited to the trusted roles only. The trusted roles gain access to the CSL-CA facility by means of Trusted Role Identification Card. The physical access is logged manually as well as electronically. A minimum of two people is required to be present to gain access into the secure CA room itself.

- Single door standalone proximity time attendance controller
- Keep record of all visitor in enter and exit log
- Access control system & server which can generate report
- Security Camera & keep record of the movement.

5.1.3 Power and air conditioning

CSL-CA servers, workstations and devices are powered by Uninterruptible Power Supply (UPS). The necessary ambience control measures (air conditioning, ventilation etc.) are used to facilitate the continuous operation of the CSL-CA servers and workstations. The site has online UPS system, Primary power supply

from PDB, Secondary power supply from generator, adequate cooling system and dehumidifier system.

5.1.4 Water exposures

The CSL-CA has taken reasonable precautions to minimize the impact of water exposure to CSL-CA facilities.

5.1.5 Fire prevention and protection

Sufficient fire protection mechanism put in place at CSL-CA site.
The facilities provided for fire prevention and protection measures have been designed to comply with the fire safety regulations of respective civic bodies.

- Aerosol Gas cylinder Model
- Thermal Activation Generator
- Manual Release activator,
- Extinguishing control panel with 4 Detection Zone control panel and releasing area with Rechargeable Battery back up
- Heat Detector
- Photo electric smoke detector,
- 24V DC Bell, Diameter 6",
- Flash Light Light,
- Discharge Indicator
- Double Flashing light,
- Auto Exit Sign,
- Manual Release or Break Glass,
- Rotating light, 6" fire alarm bell, strobe horn and warning sign

5.1.6 Media storage

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

5.1.7 Waste disposal

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

5.1.8 Environment Monitoring System

CSL CA has Environment Monitoring system installed to check the various physical infrastructure of the CSA CA Facility & Data Centre. It includes Environment Monitoring System Controller, Temperature &Humidity Combination Sensor, Liquid Detection Sensor.

5.1.9 Off-site backup

All the backups of software, databases will be stored offsite with all the security measures.

5.2 Procedural controls

5.2.1 Trusted Roles

Trusted Roles are defined to perform effective and secure operations of CA. These trusted roles are collectively known as trusted personnel. As these trusted personnel have access to the CSL-CA facilities, they may affect the:

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

5.2.1.1 ***CA Technical Administrator***

The CA Technical Administrator shall be responsible for:

- Installation, configuration, and maintenance of the CA;
- Establishing and maintaining CA system accounts;
- Configuring certificate profiles or templates and audit parameters, and;
- Generating and backing up CA keys.
- Administering HSM
- Database administration
- LDAP administration
- Administrators shall not issue certificates to subscribers.

5.2.1.2 ***CA Administrator***

The CA Technical Administrator shall be responsible for issuing certificates, that is:

- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates, and;
- Requesting, approving and executing the revocation of certificates.
- Registering RAs

5.2.1.3 ***Audit Administrator***

The Audit Administrator shall be responsible for:

- Reviewing, maintaining, and archiving audit logs;
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS;

5.2.1.4 ***System Administrator***

The System Administrator shall be responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.1.5 ***Registration Authority Administrator***

An RA's responsibilities are:

- Point of contact for customer support relating to registration
- Verifying identity
- Entering Subscriber information, and verifying correctness;
- Notification of authenticated digital certificate request to the CA;
- Authentication of subscriber"s identification information, which is necessary to issue a digital certificate, to the CA
- Acceptance and verification of digital certificate revocation requests and notification of the verified requests to the CA
- The RA role is highly dependent on public key infrastructure implementations and local requirements.

5.2.2 Number of persons required per task

The duties to be performed by each of the trusted personals in the CSL-CA Organizational structure are defined in such a manner that no single person would take control of the certificate issuance/revocation process.

At least two people are assigned to each trusted role to ensure adequate support at all times.

Some roles are assigned to different people to ensure no conflict of interest occurs and to prevent the possibility of accidental or intentional compromise of any component of the CA infrastructure

CA key-pair generation and initialization of each of the CAs shall require the active participation of at least two trusted individuals in each case. Such sensitive operations also required the active participation and oversight of senior management.

Two or more persons shall be required to perform the following tasks:

- CA key generation;
- CA signing key activation; and
- CA private key backup.

5.2.3 Identification and authentication for each role

The persons filling the trusted roles must undergo an appropriate security screening procedure, described as per HR policy of CSL-CA.

Identification and authentication mechanisms (such as passwords and tokens) are used to control account access for each role. All access by each role to accounts requires password and/or token identification and authentication. Password policy is implemented for strong passwords.

5.2.4 Identification and authentication for each role

Roles requiring separation of duties

Role separation, when required as set forth below, may be enforced either by the equipment, or procedurally, or by both means.

Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role.

5.3 Personnel Controls

CSL-CA employees are capable to operate, administer and manage all the aspects of PKI infrastructure. They have qualifications necessary to perform allocated duties. In accordance with the requirements for specific duties, employees undergo security clearance prior to being granted permission to partake in the service and or related operations.

5.3.1 Qualifications, experience, and clearance requirements

Personnel appointed to the trusted roles will be chosen in accordance with CSL-CA hiring practices for positions of this sensitivity.

Personnel in key operational positions will have received proper training in the performance of their duties, be aware of disciplinary measures for breaches of security controls/processes, Not be assigned other duties that may conflict with their duties and responsibilities

5.3.2 Background check procedures

Background checks shall be carried out by CSL-CAand staff fulfilling sensitive roles shall be formally appointed.

5.3.3 Training requirements

The persons identified would have undergone adequate training to handle CSL-CA operations, understand PKI concepts, exposure to software and hardware of PKI, computer security, and operation of CSL-CA functions.

5.3.4 Retraining frequency and requirements

At frequent intervals training will be provided to all CSL-CA employees on the products and new features.

5.3.5 Job rotation frequency and sequence

Personnel will undergo job rotation practices as per the Human Resources Policy

5.3.6 Sanctions for unauthorized actions

Disciplinary action will be initiated for all unauthorized actions

5.3.7 Independent contractor requirements

The persons contracted in CSL-CA operations will be trust worthy and qualified.

5.3.8 Documentation supplied to personnel

Detailed operations documents will be provided to all the operations persons to perform their duties without ambiguity. The operations documents will be updated regularly with the changes, if any.

5.4 Audit logging procedures

5.4.1 Types of events recorded

- All security auditing capabilities of CA, LDAP, operating system applications shall be enabled. As a result, most of the events identified in the table below shall be automatically recorded.
- Events involved in the generation of the CSL-CA key pairs will be recorded.
- Data involved in each individual digital certificate registration process will be recorded
- All data and procedures involved in the certification and distribution of digital certificates
- Data relevant to the publication of digital certificates and CRLs to the LDAP server will be recorded.
- Digital certificate revocation request details will be recorded
- Firewall logs will be recorded
- Database Auditing will be enabled and recorded
- CA Backup logs will be enabled and recorded
- Details of maintenance performed on the machines will be recorded.

5.4.2 Frequency of processing log

Frequency of processing log will be maintained as per CCA determined.

5.4.3 Retention period for audit log

Retention period of audit log will be maintained as per CCA determined.

5.4.4 Protection of audit log

Archives shall be retained and protected against modification or destruction. Audit log will be securely protected and will be accessible only by authorized personnel of CA.

5.4.5 Audit log backup procedures

Audit logs and audit summaries will be backed up in manual form using access log.

5.4.6 Audit collection system (internal vs. external)

Audit log collection system is internal to the CSL CA.

5.4.7 Notification to event-causing subject

This CPS imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability assessments

The relevant audit data collect shall be regularly analyzed by the appointed CSL-CA personnel for any attempts to violate the integrity of any element of the CSL-CA PKI. All the major security events will be analyzed and acted upon.

5.5 Records Archival

5.5.1 Types of records archived

CSL-CA archives records that will be adequately detailed to establish the proper operation of the component or the validity of any certificate (including those revoked or expired) issued.

5.5.2 Retention period for archive

The minimum retention periods for archive data are listed below. However, this can vary based on CCA directions.

Assurance Level Archive Retention Period

Class 1 - 7 Years
Class 2 - 7 Years
Class 3 - 7 Years

5.5.3 Protection of archive

The archive shall be protected from unauthorized write, modify, or delete. For CSL-CA, the authorized individuals are Audit Administrators. The contents of the archive shall not be released except as determined by the CCA, or as required by law.

Archive media shall be stored in a safe, secure storage facility separate from CSL-CA facility with adequate security.

5.5.4 Archive backup procedures

No stipulation.

5.5.5 Requirements for time-stamping of records

All events that are recorded include the date and time of when the event took place. This date and time are based on the system time on which the CA program is operating.

5.5.6 Archive collection system (internal or external)

Archive collection system is internal to the CSL-CA.

5.5.7 Procedures to obtain and verify archive information

Upon proper request (see Sections 9.3 and 9.4) and payment of associated costs, CSL-CA will create, package and send copies of archive information.

5.6 Key changeover

CA Key pair change will be notified on CSL-CA website.

Once an issued digital certificate has expired the subscriber may be required to reapply for a new digital certificate in the same manner as they originally applied. The subscriber will be notified in advance of the expiration date and they will be given details as to how they must reapply for their new digital certificate.

5.7 Compromise & Disaster Recovery

5.7.1 Incident and compromise handling procedures

Robust physical, logical, and procedural controls are implemented by CSL-CA to minimize the risk and potential impact of a key Compromise or disaster.

The Disaster Recovery Plan would consist of a detailed manual covering all the aspects of compromise and disaster recovery like key compromise, crashing of systems both software and hardware, corruption of systems both the hardware and software, communication failures, problems arising out of strike, fire, flood or any other natural disaster.

The staff would be identified and trained to conduct these operations if, any disaster happens.

If a potential hacking attempt or other form of compromise is detected, CSL-CA shall perform an incident analysis in order to determine the nature and the degree of damage. In case the CA key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt or revoke certain certificates

5.7.2 Computing resources, software, and/or data are corrupted

The plan incorporates measures to minimize system down time for all critical components of the PKI system, including the hardware, software and keys, in the event of a failure or compromise of one or more of these components.

Using the backups and archives necessary software, hardware and databases shall be restored. In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to Review Committee of CCA and CSL-CA incident handling actions are endorsed. Based on the requirement, CSL CA"s disaster recovery procedures will be implemented. CSL-CA maintains offsite backups of important CA information.

5.7.3 Entity private key compromise procedures

In case of suspected or know cases of CA private key compromise:

- Inform CCA
- Request CCA to revoke CSL-CA certificate
- The subscribers and relying parties will be informed through website
- All certificates will be revoked and CRL will be generated.
- No new certificates will be generated with compromised key pair.
- CSL-CA will generate a new key pair.
- Subscribers need to reapply for getting new certificate after the notification by CSL-CA.

In the case of end subscriber key compromise:

- Inform the CSL-CA/RA and relying parties
- Request the revocation of the end entity"s certificate.

5.7.4 Business continuity capabilities after a disaster

CSL-CA creates the backup of important data and stores in offsite in accordance with its backup policy. This data will be used for recovery and continuity of the business or data are corrupted

5.8 CA or RA termination

Before ceasing to act as a Certifying Authority, CSL-CA shall:

- Give notice to the CCA of its intention to cease acting as a Certifying Authority, ninety days before ceasing to act as a Certifying Authority or ninety days before the date of expiry of license;
- Advertise sixty days before the expiry of license or ceasing to act as Certifying Authority, as the case may be, the intention in such daily newspaper or newspapers and in such manner as the CCA may determine;

- Notify its intention to cease acting as a Certifying Authority to the subscriber at least sixty days before ceasing to act as a Certifying Authority or sixty days before the date of expiry of unrevoked or unexpired Digital Certificate, as the case may be;
- The notice will be sent to the Controller, affected subscribers and Cross Certifying Authorities by digitally signed e-mail and registered post;
- Revoke all Digital Certificates that remain unrevoked or unexpired at the end of the ninety days of notice period, whether or not the subscribers have requested revocation;
- Make a reasonable effort to ensure that discontinuing its certification services causes minimal disruption to its subscribers and to persons duly needing to verify digital signatures by reference to the public keys contained in outstanding Digital Certificates;
- Make reasonable arrangements for preserving the records for a period of seven years;

Section 6

6 Section 6: Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

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

6.1.2 Private key delivery to subscriber

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

6.1.3 Private key delivery to subscriber

CSL-CA accepts Certificate requests in PKCS#10 request format.(See RFC 3647). The preferred transport method for certification requests is SSL protected HTTP.

6.1.4 CA public key delivery to replying parties

CSL-CA public keys are published on the CSL-CA Certificate Repository

6.1.5 Key Sizes

The key length of CSL-CA module will be 2048 bit.

6.1.6 Public key parameters generation and quality checking

Public key parameters are generated by the relevant applications

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Key pair for CSL-CA is generated by using a hardware security module (HSM) conforming to FIPS 140-2 Level 1, 2 and Level 3. The Subscriber keys may be generated in hardware/software. However Class 3 certificates shall be generated in hardware (Crypto smart card/USB token) only.

The Subscriber keys may be generated in software.

6.2.2 Private key (n out of m) multi-person control

CSL-CA technical and procedural controls require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. Two out of three multi-person controls for particular cryptographic module is required to activate CSL-CA private key stored on the module

6.2.3 Private key escrow

CSL-CA do not escrow the private keys of subscribers

6.2.4 Private key backup

The Backed up keys are stored in the same manner on hardware Security Module HSM 140-2 Level 3 Backup tokens containing CA private keys are stored securely offsite for backup and disaster recovery purposes.

6.2.5 Private key archival

CSL-CA private keys are archived for a period of 10 years or when it reaches their validity period. Archived key pairs will be securely stored on cryptography module. CSL-CA does not archive the private keys of RA and subscriber signing keys.

6.2.6 Private key transfer into or from a cryptographic module

CSL-CA Private Key is generated onboard, stored in encrypted form and remains in encrypted form and it is decrypted only when it is used. When CA key pair is backed up to another hardware cryptographic module, such key pair is transported between modules in encrypted form.

6.2.7 Private key storage on cryptographic module

Refer section 6.2.6

6.2.8 Method of activating private key

Activation of private key requires more than one person. The relevant person possesses the smart cards, the passphrase and enters them together to activate the private key

6.2.9 Method of deactivating private key

The private key is deactivated upon removal from the token reader.

6.2.10 Method of destroying private key

At the expiry the copies of the CA private key are securely destroyed after archival. In addition, archived CA private keys are securely destroyed at the conclusion of their archive periods. The same methods will be followed for destruction of private key in case of key compromise.

In case of subscriber, for Smart card based keys, the private keys can be deleted by personalization/Initialization of card/token.

6.2.11 Cryptographic Module Rating

CSL-CA shall utilize hardware cryptographic modules rated FIPS-140-2 level 3 to perform all digital signing operations.

6.3 Other aspects of key pair management

6.3.1 Public key archival

All certificates containing public are archived by CSL-CA upon expiry as part of CA"s routine backup procedures and kept for a period of seven years as per the Act.

6.3.2 Certificate operational periods and key pair usage periods

CSL-CA private key will have a key validity period of 5 years. The validity period of subscriber certificates will be dependent on the class of digital certificate in question. Refer to Appendix B for details of the various validity periods.

6.4 Activation Data

6.4.1 Activation data generation and installation

After personalization, no activation data other than access control mechanisms (PIN) are required to operate cryptographic modules

6.4.2 Activation data protection

Pass phrases or PIN shall not be accessible to anyone except the operator and the certificate holder

6.4.3 Other aspects of activation data

No stipulation

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

CSL-CA computer system satisfies the following requirements:

- CSL-CA is run on dedicated computer systems.
- Only the software needed to perform the CSL-CA tasks is installed on the system.
- Access to the operating system and the CSL-CA software is allowed only to the authorized CSL-CA trusted personnel.
- Physical access to the system is allowed only to the authorized CSL-CA trusted personnel.
- All security related events are audited in the CSL-CA system.

6.5.2 Computer security rating

No Stipulation

6.6 Life cycle technical controls

6.6.1 System development controls

The development of the software shall be carried out in a controlled secure environment. Production and development environment are totally separated.

6.6.2 Security management controls

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

6.6.3 Life cycle security controls

No stipulation

6.7 Network security controls

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

6.8 Time-stamping

System time for CSL-CA computers is updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours (Windows default). The synchronization of NTP is provided from CCA facility.

All components shall regularly synchronize with the time service. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a Subscriber‟s Certificate
- Revocation of a Subscriber‟s Certificate
- Posting of CRL updates

Section 7

7 Section 7: CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

To ensure global compatibility and conformity to public key standards, the CSL-CA will utilize the "RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999" (ITU-T X.509 version 3) digital certificate standard.

7.1.1 Version number(s)

Refer to Appendix B and Appendix C for detailed description of certificate profile

7.1.2 Certificate extensions

Refer to Appendix B and Appendix C for detailed description of certificate profile

7.1.3 Algorithm object identifiers

Refer to Appendix B and Appendix C for detailed description of certificate profile

7.1.4 Name forms

Refer to Appendix B and Appendix C for detailed description of certificate profile

7.1.5 Name constraints

Refer to Appendix B and Appendix C for detailed description of certificate profile

7.1.6 Certificate policy object identifier

Refer to Appendix B and Appendix C for detailed description of certificate profile

7.1.7 Usage of Policy Constraints extension

Refer to Appendix B and Appendix C for detailed description of certificate profile

7.1.8 Policy qualifiers syntax and semantics

Refer to Appendix B and Appendix C for detailed description of certificate profile

7.1.9 Processing semantics for the critical Certificate Policies extension

Refer to Appendix B and Appendix C for detailed description of certificate profile

7.2 CRL profile

To ensure global compatibility and conformity to public key standards, COMPUTER SERVICES LTD CA will utilize the "RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999" (ITU-T X.509 version 2) Certificate Revocation List standard.

7.2.1 Version number(s)

Refer to Appendix B and Appendix C for detailed description of CRL profile

7.2.2 CRL and CRL entry extensions

Refer to Appendix B and Appendix C for detailed description of CRL profile

7.3 OCSP Profile

OCSP requests and responses shall be in accordance with RFC 2560 as listed below.

For a detailed description of the CSL CA OCSP, refer to Appendix-B

7.3.1 Version Number(s)

For a detailed description of the CSL CA OCSP, refer to Appendix-B

7.3.2 OCSP Extensions

For a detailed description of the CSL CA OCSP, refer to Appendix-B

Section 8

8 Section 8: COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

The frequency of audit shall be governed by CCA Rules.

CSL-CA shall conduct-

- Half yearly audit of the Security Policy, physical security and planning of its operation;
- Quarterly audit of its repository.

8.2 Identity/qualifications of assessor

A certified Information Security Auditor empanelled by the CCA shall audit services of the COMPUTER SERVICES LTD CA and any designated authorized agents on an annual basis. CSL-CA reserves the right to appoint this independent external auditor.

8.3 Assessor's relationship to assessed entity

- The auditor shall be independent of the CSL-CA and shall not be a software or hardware vendor which is, or has been providing services or supplying equipment to CSL-CA.
- The auditor for the purpose is approved by the CCA being satisfied that that the auditor has sufficient expertise for auditing Certifying Authority ;
- The auditor and CSL-CA have no current or planned financial, legal or other relationship, other than that of an auditor and the audited party.

8.4 Topics covered by assessment

The compliance audit mechanism is to ensure that the requirements of this CPS are being implemented and enforced.

8.5 Actions taken as a result of deficiency

- If any deficiencies/non-conformities is found in the audit reports, CSL-CA will implement appropriate correction within a reasonable time frame.
- Any failure to comply with the specified requirements of CSL-CA CPS shall be addressed by the CSL-CA or its authorized agent as soon as is operationally possible.

8.6 Communication of results

CSL-CA shall submit copy of each compliance report to the CCA within four weeks of the completion of such audit and where irregularities are detected

Section 9

9 Section 9: OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees:

The fees for Certificates services provided by CSL-CA will be published in the CSL-CA website. These fees are subject to change.

9.1.2 Certificate access fees:

There is not charge for access to any certificate

9.1.3 Revocation or status information access fees:

CSL-CA does not charge for certificate revocation. Relying parties are also not charged to check CRL status. However, CSL-CA may charge reasonable fee for providing certificate status information via OCSP as an when it is setup

9.1.4 Fees for other services:

Fee for other services like access to archive records will be reasonable and will published on CSL-CA website

9.1.5 Refund policy:

The refund policy will be published on CSL-CA website

9.2 Financial responsibility

CSL-CA does not give any warranties on the financial transactions which the subscribers and relying parties do using the digital certificates obtained from CSL-CA. The subscribers and relying parties are solely responsible for any loss, damage or any consequences due to such transactions.

Subscribers or certificate holders have no authority to bind CSL-CA by contract or otherwise to any obligation.

9.2.1 Insurance coverage

Not applicable

9.2.2 Other assets

CSL-CA shall maintain reasonable financial resources to maintain operations and duties and to address commercially reasonable liability obligations to PKI participants.

9.2.3 Insurance or warranty coverage for end-entities

CSL-CA does not provide any insurance or warranty to end entities that extend the protection beyond the protections provided in this CPS. Subscribers should refer to subscriber agreement and relying parties should refer to relying party agreement which are located at <www.ca.computerservicesltd.com>

9.3 Confidentiality of business information:

9.3.1 Scope of confidential information

CSL-CA keeps the following information confidential and maintains reasonable controls to prevent exposure to such records to unauthorized persons:

- All private keys
- Activation and authorization codes
- Business continuity, incident response, disaster recovery plans
- Any information held by CSL-CA as private information
- Any transactional records and archived logs, including certificate applications, successful or rejected
- Financial audit records, audit trail records, audit reports

9.3.2 Information not within the scope of confidential information

Subscriber information published in the certificates is considered public and not within the scope of confidential information. Subscriber certificate revocation information is public.

9.3.3 Responsibility to protect confidential information

CSL-CA puts reasonable controls to protect the confidential information

9.4 Privacy of personal information:

9.4.1 Privacy plan

Digital certificates are public information. CSL-CA does not divulge any additional subscriber information to any third party unless required by law or by order of the court of law or by competent regulator authority

9.4.2 Information treated as private

All information, except that goes into digital certificate or held in publicly available repositories, will be kept confidential

9.4.3 Information not deemed private

Information that goes into digital certificate or held in publicly available repositories will not be confidential

9.4.4 Responsibility to protect private information

CSL-CA will put reasonable controls to protect the confidentiality of private information that is in its possession.

9.4.5 Notice and consent to use private information

In the course of accepting the digital certificates, all subscribers will be notified that their personal data submitted in the course of registration to be processed by and on behalf of CSL-CA during registration process. They are given the option to decline from having their personal data used for particular purpose. They also agree to let certain personal data to appear in publicly accessible directories and be communicated to others

9.4.6 Disclosure pursuant to judicial or administrative process

CSL-CA shall not release any confidential information, unless otherwise required by law, regulatory authority or a court order.

9.4.7 Other information disclosure circumstances

All other information disclosure circumstance shall be governed by the requirements of laws of Bangladesh concerning the protection of personal data.

9.5 Intellectual property rights

- CSL-CA retains all right, title, and interest (including all intellectual property rights), in, to and under all CSL-CA Digital Signature Certificates, except for any information that is supplied by an Applicant or a Subscriber and that is included in an CSL-CA Digital Signature Certificate, which information shall remain the property of the Applicant or Subscriber.

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

9.6 Representations and warranties:

9.6.1 CA representations and warranties

CSL-CA verify the information contained in a digital certificate vary according to the digital certificate fee charged, the nature and identity of the subscriber, and the applications for which the digital certificate will be marked as trusted. CSL-CA warrants that:

- It has taken reasonable steps to verify the information contained in the digital certificate is accurate at the time of issue
- The digital certificate shall be revoked in case CSL-CA believes that or has been notified that the contents are no longer accurate or private key associated with the certificate is compromised
- Publish the accepted digital certificate in the CSL-CA repository
- Put the revoked certificates into CRL and publish the updated CRL in the CSL-CA repository

9.6.2 RA representations and warranties

- Take necessary approval from the CSL-CA through CSL Coordinator to function as RA administrator for CSL-CA for the concerned office.
- Verify the authenticity of the subscriber requesting the Certificate for issuance or revocation and forward the same to the designated CSL Coordinator.
- Verify the information provided by the subscriber and make sure that the DN (Distinguished Name) is unique.
- Request for revocation or suspension of a Certificate for any reason such as transfer, suspension, long leave, change of duties, superannuation and death.
- Maintain records of requests for application, revocation, and suspension of Certificates.

9.6.3 Subscriber representations and warranties:

CSL-CA requires Subscribers to warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- No unauthorized person has ever had access to the Subscriber‟s private key,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are accurate,
- All information supplied by the Subscriber and contained in the Certificate is accurate,
- The Certificate is being used solely for authorized and legal purposes, specifically for the purpose as stipulated/stated by the submission in the certificate application only, and
- The Subscriber is an end-user Subscriber and not a CA

9.6.4 Relying party representations and warranties

- The relying party should have knowledge of the IT Act 2006, CA Rules 2010.

- The reliance is reasonable and in good faith in light of all the circumstances known to the relying party at the time of the reliance.
- The Certificate is used exclusively for purposes mentioned in the Certificate.
- The purpose for which the Certificate is used is appropriate under this CPS.
- The Certificate is being used within its operational period.
- The relying party checked the status of the Certificate by using the CRL published in the repositories prior to reliance, or a check of the Certificate"s status would have indicated that the Certificate was valid.

9.6.5 Representations and warranties of other participants

No stipulation

9.7 Disclaimers of warranties:

- CSL-CA will not be responsible for any data loss/damage arising from the use of this Certificates/Tokens/Technology. The user is solely responsible for the same. Encrypting/decrypting/storing/sharing/transmitting of any message or document or electronic data should be in conformity with the Bangladesh Telegraphic Act, IT Act and all other relevant parts of the Bangladesh legal system and will be the sole responsibility of the user and the relying parties. CSL-CA shall not be held responsible and no legal proceedings shall be taken against CSL-CA for any loss and damage that may occur due to any reason whatsoever including technology up gradation, malfunctioning or partial functioning of the software, Crypto device or any other system component. Digital Certificates issued by CSL-CA will valid only for the suggested usage and for the period mentioned in the certificate. These Certificates shall not be valid for any other purpose.

- The CSL-CA reserves the right to suspend or revoke Certificates issued by it, in accordance with the Sections 37 & 38 of the IT Act. Before revocation, Subscriber shall be given due opportunity of being heard in the matter. It is assumed that the users are conversant with PKI technology, and the underlying risks and obligations before applying and using Digital Signature Certificate, issued by CSL-CA

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

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

9.8 Limitations of liability

CSL is not liable for any loss:

- due to war, natural disasters, acts of terrorism or other uncontrollable forces.
- incurred between the times a Certificate Revocation request is received and the stipulated period of revocation as per Section 3.4.2 .
- due to unauthorized use of Certificates issued by the COMPUTER SERVICES LTD CA, and use of Certificates beyond that prescribed.
- caused by fraudulent or negligent use of Certificates or Certificate revocation lists issued by the COMPUTER SERVICES LTD CA.
- due to disclosure of information contained within Certificates and revocation lists.
- indirect, consequential or punitive damages arising from or in connection with its services. The COMPUTER SERVICES LTD CA has no liability for indirect, special, incidental or consequential damages, or for any loss of data/information or other indirect, consequential or punitive damages arising from or in connection with its services. Except as expressly provided in this CPS, the COMPUTER SERVICES LTD CA disclaims all other warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of information provided.
- CSL disclaims any liability that may arise from the use of the Digital Certificate(s) issued by COMPUTER SERVICES LTD CA.

9.9 Indemnities:

9.9.1 Indemnification by Subscribers

a. To the extent permitted by applicable law, COMPUTER SERVICES LTD CA requires, Subscribers to indemnify COMPUTER SERVICES LTD CA for:
b. Deception or falsification of fact by the Subscriber on the Subscriber‟s Certificate Application,
c. The Subscriber‟s failure to guard the Subscriber‟s private key, to use a Trustworthy System, or to
d. otherwise take the precautions necessary to prevent the compromise, loss, disclosure,
e. modification, or unauthorized use of the Subscriber‟s private key,
f. Failure by the Subscriber to disclose a material fact on the Certificate Application, if the
g. misrepresentation or omission was made neglectfully or with intent to deceive any party, or

h. The Subscriber‟s use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, COMPUTER SERVICES LTD CA requires, Relying Parties to indemnify COMPUTER SERVICES LTD CA for:

a. The Relying Party‟s failure to act upon the obligations of a Relying Party,
b. The Relying Party‟s confidence on a certificate that is not reasonable under the circumstances, or
c. The Relying Party‟s failure to check the status of such certificate to find out if the certificate is
d. expired or revoked

9.10 Term and termination:

9.10.1 Term

This CPS and any amendments hereto shall become effective upon publication in the Repository and shall remain in effect perpetually until terminated in accordance with this Section 9.10.

9.10.2 Termination

This CPS as amended from time to time shall remain in force until it is replaced by a new version or is otherwise terminated in accordance with this Section 9.10.

9.10.3 Effect of termination and survival

The conditions and effect resulting from termination of this document will be communicated via the

CSL-CA Repository upon termination. That communication will outline the provisions that may survive termination of this CPS and remain in force. The responsibilities for protecting business confidential and private personal information shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the Validity Periods of such Certificates.

9.11 Individual notices and communications with participants

Any notice required or permitted to be given to CSL-CA shall be in writing and shall be sent to its designated office from time to time. The current designated office is: <12B Ataturk Tower, 22 Kemal Ataturk Avenue, Banani, Dhaka-1213> Any such notice shall be delivered personally or sent in a letter by recorded delivery service and shall be deemed to have been served, if by personal delivery when delivered, and if by recorded delivery, 48 hours on receipt by the CSL-CA. Any such notices may be sent to CSL-CA via electronic mail and such notices shall only be deemed to be valid if the

subscriber confirms such email notices to the CCL-CA in writing within 24 hours of the receipt of the e-mail notice by CSL-CA.

9.12 Amendments

9.12.1 Procedure for amendment

The amendments are approved by:

- CSL-CA policy approval committee
- CSL-CA legal department
- However, final approval of the CPS is made by CCA. Amended versions of CPS shall be published in CSL-CA repository

9.12.2 Notification mechanism and period

CSL-CA reserves the right to amend CPS devoid of notification for amendments that are not material such as corrections of typographical errors, URL changes, and contact information. CSL-CA shall make material amendments to the CPS in accordance with this section.

9.12.3 Circumstances under which OID must be changed

No stipulation

9.13 Dispute resolution provisions

Dispute resolution between CSL-CA, the Subscribers, and the Relying parties will be as per the ICT Act 2006. Resolution of disputes should be overall governed by the ICT Act 2006, and will be referred to the CCA from time to time for arbitration.

9.14 Governing law

The Information and Communication Technology Act, 2006 and IT (CA) Rule, 2010, by Government of the People"s Republic of Bangladesh, and The Rules and Regulations for Certifying Authorities formulated by Controller of Certifying Authorities (CCA) under ICT division shall govern the enforceability.

9.15 Compliance with applicable law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16 Miscellaneous provisions:

9.16.1 Entire agreement

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances, and intended usage of the product or service described herein. In interpreting this CP/CPS the parties shall also take into account the international scope and application of the services

and products of Computer Services Ltd CA as well as the principle of good faith as it is applied in commercial transactions.

The headings, subheadings, and other captions in this CP/CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS.

Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS.

If/when this CPS conflicts with other rules, guidelines, or contracts, this CPS shall prevail and bind the Subscriber and other parties. If there is any conflict between the sections of this CPS and any other document that relate to Computer Services Ltd CA, then the sections benefiting Computer Services Ltd CA and preserving Computer Services Ltd CA‟s best interests, at Computer Services Ltd CA‟s sole determination, shall prevail and bind the applicable parties.

9.16.2 Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent of Computer Services Ltd CA

9.16.3 Severability

To the extent permitted by applicable law, Subscriber Agreements, Agreements and Relying Party Agreements under the Computer Services Ltd CA 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 will 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.

9.16.4 Enforcement (attorneys’ fees and waiver of rights)

Computer Services Ltd CA reserves the right to seek indemnification and attorneys' fees from any party related to that party's conduct described in Section 9.9. Except where an express time frame is set forth in this CPS, no delay or omission by any party to exercise any right, remedy or power it has under this CPS shall impair or be construed as a waiver of such right, remedy or power. A waiver by any party of any breach or covenant in this CPS shall not be construed to be a waiver of any other or succeeding breach or covenant. Bilateral agreements between Computer Services Ltd CA and the parties to this CPS may contain additional provisions governing enforcement.

9.16.5 Force Majeure

Computer Services Ltd CA accepts no liability for any breach of warranty, delay or failure in performance that results from events beyond its control such as acts of God, acts of war, acts of terrorism, civil unrest, strikes, flood, epidemics, power or telecommunication services failure, fire, and other natural disasters; any provision of any applicable law, regulation or order; civil, government or military authority; the failure of any electrical communication or other system operated by any other party over which it has no control; or other similar causes beyond its reasonable control and without its fault or negligence.

9.17 Other provisions:

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties that this CPS applies to. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CPS articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

Appendix-A

10 Section 10: Appendix-A

10.1 A.1 Certificate Classes

CSL-CA supports 4 classes of certificates and reserves the right to introduce more distinct classes or sub-classes than what has been specified here. CPS shall be appropriately amended when such classes are introduced. Each class provides for distinguished level of trust. The following sections describe each certificate class.

A.1.1 Class 0 Certificate

Test certificate only.

A.1.2 Class 1 Certificate

Class-1 Certificate	OID- 2.16.50.1.9
Category	Issued to the Individuals only
Suggested Usage	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 CSL-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	The verification of the certificate request of this class represent a simple check of the certainty of the subject name within the CSL-CA repository, plus a limited verification of the address, other personal information and e-mail address.
Verification Process	In case of online or offline certificate request for Class 1 certificate, the applicant submits online or paper application form. CSL-CA or its RA verifies the name e-mail address and postal address in the request. CSL-CA has right to reject the certificate request if finds the application and supporting documents are not meeting the criteria.
Physical Presence	Physical presence is not required
Validity	1 Year

A.1.3 Class 2 Certificate

Class-2 Certificate	OID- 2.16.50.1.9
Category	Class 2 certificates are issued to
Suggested Usage	In addition to the „suggested usage" mentioned in class I, the class II Signing certificate may also be used for digital signing, authentication for VPN Client, web form signing, smart card logon, user authentication, single sign-on and signing involved in e-procurement/e-governance applications. In addition to the „suggested usage" mentioned in class I, the class II Encryption certificate may also be used for encryption involved in e-procurement/e-governance applications.
Assurance Level	Class 2 certificates are appropriate for digital signature and encryption requiring high level of assurance regarding subscriber's identity
Verification Process	For Class 2 digital certificate, the applicant submits online/paper application form and required documents. CSL-CA verified the name, e-mail address, supporting documents and postal address in the request. CSL-CA has right to reject the certificate request if finds the application and supporting documents are not meeting the criteria.
Physical Presence	Physical presence may or may not be required. This will be decided on case to case basis
Validity	1 Year

A.1.4 Class 3 Certificate

Class-3 Certificate	OID- 2.16.50.1.9
Category	Class 3 Certificates are issued to individuals, Enterprises and Devices
Suggested Usage	Encryption, Signing for individuals and Authentication for the devices
Assurance Level	Class 3 certificates are appropriate for digital signatures and encryption requiring a high assurance about the subscriber"s identity
Verification Process	For Class 2 digital certificate, the applicant submits online/paper application form and required documents. CSL-CA verified the name, e-mail address, supporting documents and postal address in the request. CSL-CA has right to reject the certificate request if finds the application and supporting documents are not meeting the criteria.
Physical Presence	Physical presence may or may not be required. This will be decided on case to case basis
Validity	1 year

10.2 A.2 Documentation and Verification

The certificate issuance lifecycle consists of Application by the subscriber with the required documents as details below in the table, verification of the documents and identity based on the class of the certificate applied for and enrollment of the user and issue the certificated.

CSL-CA issues class-1, class-2 and class-3 certificates. Before issuing the certificated the identity of the user is verified as described below:

Class of Certificate	Entity	Verification Documents Required	Verification Process	Verification Done By
Class 1	Individual	Digital communication address verification for email	email verification	RA Administrator
Class 1	Proprietorship firms	Digital communication address verification for email	email verification	RA Administrator
Class 1	Partnership firms	Digital communication address verification for email	email verification	RA Administrator
Class 1	Public & Pvt Ltd companies	Digital communication address verification for email	email verification	RA Administrator
Class 1	For Trust	Digital communication address verification for email	email verification	RA Administrator
Class 1	For Club/society/school	Digital communication address verification for email	email verification	RA Administrator
Class 2	Individual	Two copies of attested passport size photograph of the Applicant Copy of valid Passport (1 to 7 page) or Copy of National ID Card (front and back)	Verify the documents submitted for completeness	RA Administrator
Class 2	Proprietorship firms	2 copies of attested Passport size photograph of the Applicant. Valid Trade License Proprietorship declaration in letterhead pad. Copy of valid Passport (1 to 7 page) or Copy of National ID Card (front and back) of Applicant TIN certificate VAT registration certificate	Verify the documents submitted for completeness	RA Administrator

Class 2	Partnership firms	2 copies of attested Passport size photograph of the applicant. Valid Trade License Resolution signed by the partners to obtain & operate digital certificate. Notarized copy of partnership deed duly signed by all partners Copy of valid Passport (1 to 7 page) or Copy of National ID Card (front and back) of Authorized Signatory TIN Certificate VAT registration certificate	Verify the documents submitted for completeness	RA Administrator
Class 2	Public & Pvt Ltd companies	Certified true copy of Memorandum of Association & Article of Association duly signed or authenticated at each page by the Managing Director/Chairman Certified copy of company incorporation certificate Resolution of the Board of Directors for obtaining & operation of digital certificate, duly attested by the Managing Director or Chairman. List of Director"s with name, father"s name, mother"s name, spouse"s name, date of birth & signature (up-to-date) in letterhead pad of the company duly signed by the Chairman or Managing Director Valid Trade License Copy of valid Passport (1 to 7 page) or Copy of National ID Card (front and back) of Authorized Signatory TIN certificate VAT registration certificate Certified copy of commencement of Business duly authenticated by the Chairman or Managing Director (in case of public limited company)	Verify the documents submitted for completeness	RA Administrator

Class 2	For Trust	Two copies of attested passport size photograph of the Authorized Signatory • Up to date list of members of the Trustee Board • Certified copy of Deed of Trust • Certified copy of the Resolution of the Trustee Board for obtaining & operation of digital signature. • Copy of valid Passport (1 to 7 page) or Copy of National ID Card (front and back) of Authorized Signatory	Verify the documents submitted for completeness	RA Administrator
Class 2	For Club/society/school	Two copies of attested passport size photograph of the Applicant • Registration Certificate • Certified true copy of Memorandum of Association & Article of Association duly attested by the Chairman/Secretary • Resolution for obtaining & operation of the digital signature duly attested by the chairman/secretary. • Up to date list of office Bearers/Governing Body/Managing Committee duly certified by the chairman/secretary. • Passport/Commissioner certificate of signatory • Copy of valid Passport (1 to 7 page) or Copy of National ID Card (front and back) of Authorized Signatory	Verify the documents submitted for completeness	RA Administrator
Class 3	Individual	Same as for class 2 Individual	In addiion to documents verification, identity shall be established by in-person proofing before the RA	RA Administrator

Class 3	Proprietorship firms	Same as for Class 2 Propritorship firms	In addiion to documents verification, identity shall be established by in-person proofing before the RA	RA Administrator
Class 3	Partnership firms	Same as for Partnership firms	In addiion to documents verification, identity shall be established by in-person proofing before the RA	RA Administrator
Class 3	Public & Pvt Ltd companies	Same as for Public & Pvt Ltd companies	In addiion to documents verification, identity shall be established by in-person proofing before the RA	RA Administrator
Class 3	Trust	Same as for Class 2 Trust	In addiion to documents verification, identity shall be established by in-person proofing before the RA	RA Administrator
Class 3	Club/society/school	Same as for Class 2 Club/society/school	In addiion to documents verification, identity shall be established by in-person proofing before the RA	RA Administrator

Class 3	Device	Details of domain registrant Copy of passport/national ID of the person applying device certificate Copy of Official telephone bill of the person to establish the relationship between organization owning the device	Verify the documents	RA Administrator

After the completion of the identity verification, CSL-CA will enroll the user and issue the certificate. The certificate will be delivered over the Internet through secured SSL connection or by USB crypto token.

APPENDIX B – CERTIFICATE PROFILES

11 Section 11: APPENDIX B – CERTIFICATE PROFILES

This appendix details the digital certificate profiles of subscriber certificate, CA certificate and CRL. This appendix also details the standards followed. The Digital Certificates issued by CSL-CA confirm to "RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999".

11.1 B.1. Certificate Profile (Subscribers)

At minimum the CSL-CA subscriber certificates contains the basic fields and indicated prescribed values or value constraints in Table below

Basic Fields

Field	Content
X.509v1 Field	
Version	3
Serial Number	Allocated automatically by issuing CA
Signature Algorithm	SHA256 RSA
Issuer Distinguished Name	
Country (C)	BD
Organization (O)	Computer Services Limited
Organizational Unit (OU)	CSL-CA
Common Name (CN)	CSL-CA
Validity	
Valid From	<From Date>
Valid To	<To Date>
Subject	
Country (C)	User Entry
Organization (O)	User Entry
Organizational Unit (OU)	User Entry
Common Name (CN)	User Entry
Subject Public Key Info	Public key encoded in accordance with RFC2459 & PKCS#1
X.509v3 Key Details and Extensions	
Key Size & Algorithm	512/1024/2048 bit RSA

B.2 CERTIFICATE PROFILE (CA)

This corresponds to the key used to sign all certificates issued by CSL-CA to subscribers and end users

Field	**Content**
Version	v3
Serial Number	Allocated automatically by issuing CA
Signature Algorithm	SHA256 with RSA Signature
Issuer Distinguished Name	
Country (C)	BD
Organization (O)	Computer Services Limited
Organizational Unit (OU)	CSL-CA
Common Name (CN)	CSL-CA
Validity	
Not Before	<date to be put>
Not After	<date to be put>
Subject	
Country (C)	User Entry
Organization (O)	User Entry
Organizational Unit (OU)	User Entry
Common Name (CN)	User Entry
Subject Public Key Info	Public key encoded in accordance with RFC2459 & PKCS#1
X.509v3 Key Details and Extensions	
Key Size & Algorithm	2048 bit RSA
Key Usage	
Digital Signature	Selected
Non Repudiation	Selected
Data Encipherement	Selected
Key Agreement	Selected

Key Certificate Signing	Selected
Off-line CRL Signing	Selected
CRL Signing	Selected
Certificate Policies	
Policy Identifier OID	OID- 2.16.50.1.9
Policy Notice	http://www.ca.computerservicesltd.com/repository
Policy Qualifier	This certificate is issued subject to the CSL-CA CPS terms and conditions. By accepting this certificate a relying party is acknowledging acceptance of the terms and conditions.
Basic Constraints	
Subject Type	CA
Path Length Constraint	3

11.2 B.3 SERVER SSL CERTIFICATE PROFILE

Field	**Value or Value Constraint**
Version	V3
Serial Number	Allocated automatically during the issue by issuing CA
Signature Algorithm	SHA256 with RSA Signature
Issuer Distinguished Name	
Country (C)	BD
Organization (O)	Computer Services Ltd CA
Organization Unit (OU)	CSL CA
Common Name (CN)	CSL CA
Validity	
Valid From	<daate>
Valid To	<daate>
Subject	
Country (C)	User Entry
Organization (O)	User Entry
Organization Unit (OU)	User Entry
Common Name (CN)	User Entry

Subject Public Key info	Public key encoded in accordance with RFC2459 & PKCS#1
X.509v3 Key Details and Extensions	
Key Size & Algorithm	2048 bit RSA
Key Usage	
Digital Signature	Selected
Non Repudiation	Selected
Key Encipherment	Selected
Data Encipherment	Selected
Key Agreement	Selected
Key Certificate Signature	Selected
CRL Signature	Selected
Extended Key Usage	
Server Authentication	Selected
Certificate Policies	
Policy Identifier OID	OID- 2.16.50.1.9
Policy Notice	http://ca.computerservicesltd.com/repository
Policy Qualifier	This certificate is issued subject to the CSL CA CPS terms and conditions. By accepting this certificate a relying party is acknowledging acceptance of the terms and conditions.

11.3 B.4 CRL Profile Details

The CRL issued by CSL-CA confirm to "RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999". At a minimum, CSL-CA X.509 CRL contains the basic fields and indicated prescribed values or value constraints in Table below:

Field	Value or Value Constraint
Version	X.509 CRL version 2
Signature Algorithm	Algorithm used to sign the CRL. CSL- CA CRL is signed using md5RSA in accordance with RFC 2459.
Issuer	Entity that has signed and issued the CRL. The CRL Issuer Name is in accordance with the Issuer Distinguished Name requirements specified in section 3.2.1.
Effective Date	Issue date of the CRL. CSL-CA CRL is effective upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in accordance with the requirements of section 4.4.4.
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

11.4 B.5 OCSP PROFILE

OCSP requests and responses shall be in accordance with RFC 2560 as listed below

B.5.1 OCSP Request Format:

Requests sent to Issuer PKI OCSP Responders are not required to be signed, but may be at the discretion of the Issuer PKI. See RFC2560 for detailed syntax. The following table lists the fields that are expected by the OCSP Responder.

Field	Value
Version	V1 (0)
Requester Name	DN of the requestor (required)
Request List	List of certificates as specified in RFC 2560
Request Extension	**Value**
None	None
Request Entry Extension	**Value**
None	None

B.5.1 OCSP Response Format:

The following table lists which fields are populated by the OCSP Responder

Field	Value
Response Status	As specified in RFC 2560
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	Octet String (same as subject key identifier in Responder certificate)
Produced At	Generalized Time
List of Responses	Each response will contain certificate id; certificate status (If the certificate is revoked, the OCSP Responder shall provide revocation time and revocation reason from CRL entry and CRL entry extension), thisUpdate, nextUpdate (The OCSP Responder shall use thisUpdate and nextUpdate from CA CRL.)
Responder Signature	Sha256WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Certificates	Applicable certificates issued to the OCSP Responder
Response Extension	Value
Nonce	c=no; Value in the nonce field of request (required, if present in request)
Response Entry Extension	**Value**
None	None

11.5 B.5 STANDARDS

Product	Standard
Public Key Infrastructure	PKIX
Digital Signature Certificates and Digital Signature revocation list	X.509. version 3 certificates as specified in ITU RFC 1422
Directory (DAP and LDAP)	X500 for publication of certificates and Certification Revocation Lists (CRLs)
Database Management Operations	Use of generic SQL
Public Key algorithm	RSA & ECC
Digital Hash Function	SHA256

RSA Public Key Technology	PKCS#1 RSA Encryption Standard (512,1024, 2048 bit) PKCS#5 Password Based Encryption Standard PKCS#7 Cryptographic Message Syntax standard PKCS#8 Private Key Information Syntax standard PKCS#9 Selected Attribute Types PKCS#10 RSA Certification Request PKCS#12 Portable format for storing/transporting a user‟s private keys and certificates
Digital Encryption and Digital Signature	PKCS#7
Digital Signature Request Format	PKCS#10