Bangla Phone Secure CA Certificate Policy (BPSCA CP)

Bangla Phone Secure CA (BPSCA)

Version: 1.0.0

Date: 23.07.2025

Title	Bangla Phone Secure CA Certificate Policy
Document Type	Public
Current Version	1.0.0
Approval Date:	
Previous Version	NA
Previous Version Revised Date	NA
Pages	59
Status	Submitted
Document owner	Bangla Phone Secure CA

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

Changes History

This section summarizes the changes made to the CP. Please check the archived document versions for detailed comparative differences.

Term	Release Date	Changes Log
Version 1.0.0	23-07-2025	• Base Version

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

Table of Contents

Page No.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

1 INTRODUCTION

1.1 Overview

This Certificate Policy (CP) is the principal statement of policy governing the Bangla Phone Secure CA (BPSCA). It sets forth requirements for issuance, management, and use of public key certificates and associated cryptographic technology used by BPSCA in accordance with regulations of the Office of the CCA of Bangladesh.

This document is structured according to RFC 3647 [RFC3647]. Not all sections of RFC 3647 are used. Sections that are not included have a default value of "No stipulation".

This CP is the foundation for the CPS of BPSCA. All keys, key materials, and certificates issued under this policy are the property of BPSCA. Activities of the certification authority and other entities, and all certificates issued and used under this CP, are intended solely for the conduct of applicable BPSCA policies, Government regulations and CCA policies.

1.2 Document Name and Identification

Document Title: "Bangla Phone Secure CA Certificate Policy", in short, BPSCA CP.

This document comprises of Sections, Clauses & Sub-Clauses. For Example: 'Identification and Authorization' refers to a Section of this CP, with 'Naming' and 'Types of Names' are Clause and Sub-Clause respectively under this section.

Document Version: BPSCA CP 1.0.0

Document OID: 2.16.50.1.10.2

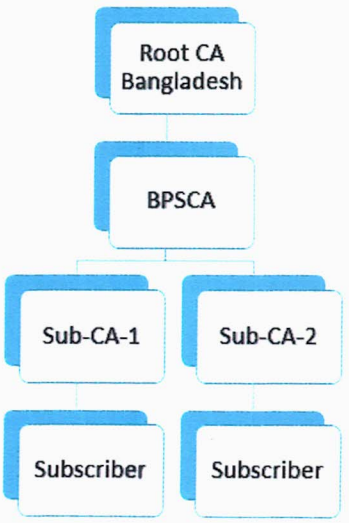
Document Date: 23 July 2025

Document publication link:
https://digitalsignature.com.bd/Content/Repository/CPS.aspx

1.3 PKI Participants

The following diagram shows various PKI members in the trust model.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd



PKI Hierarchical Trust Model

1.3.1 Certifying Authority

BPSCA is named as the 'Certifying Authority (CA)' with respect to the digital certificates it issues to End Users/Subscribers.

BPSCA is named as the 'Subject CA' with respect to the Certifying Authority (CA) License issued to it by the CCA.

1.3.2 Registration Authority

A Registration Authority (RA) is an entity that is responsible for identification and authentication of certificate applicants but does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of an authorized CA). BPSCA has internal RA to perform the following responsibilities:

- Identification and authentication of certificate applicants;
- Approval or rejection of certificate applications;
- Initiating certificate revocations or suspensions under certain circumstances
- Processing subscriber requests to revoke or suspend their certificates
- Approving or rejecting requests by subscribers to renew their certificates

1.3.3 Subscribers

A Subscriber is an individual or an organization who receives digital certificate from a CA. BPSCA recognizes a user of its certificate as a 'Subscriber'.

BPSCA issues personal user certificates, host and service certificates to its Subscribers.

An individual, an employee of an organization, a web-site owner, a person requesting e-Sign etc. are few examples of 'Subscriber'.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

1.3.4 Relying Parties

A Relying Party is any entity that places comfort on information provided by Certificate Authorities regarding a specific electronic transaction that the Relying Party uses to accept or reject its participation in the transaction. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

1.3.5 Other Participants

1.3.5.1 Subordinate Certifying Authority (Sub-CA)

Certifying authority (CA) can create one or more Subordinate Certifying Authority (Sub-CA). The Sub-CA will be part of the same legal entity as the CA. BPSCA has internal sub-CA. The key-pair of the Sub-CA are managed and operated by BPSCA.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The use of Certificates supported by the BPSCA is restricted to parties authorized by contract to do so. Entities and persons other than those authorized by contract may not use certificates for any purpose. Certificates issued under this CP may be used for the purposes designated in the key usage and extended key usage fields found in the certificate. However, the sensitivity of the information processed or protected by a certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a certificate issued under this CP.

1.4.2 Prohibited Certificate Uses

Certificates issued under this CP shall not authorized for use in any circumstances or in any application which could lead to death, personal injury or damage to property, or in conjunction with on-line control equipment in hazardous environments such as in the operation of nuclear facilities, aircraft navigation or communications systems, air traffic control or direct life support machines and the BPSCA shall not be liable for any claims arising from such use.

In particular, BPSCA certificates is strictly prohibited to use for

Anti-government activities
Money Laundering/financing terrorism

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

Any type of hacking/cracking/spamming attempts
Unwanted & unauthorized access to any PC/Network system
Intruding into any IT system of govt./banks/financial institutions
All other activities treated as unlawful &illegal as per state law

1.5 Policy Administration

1.5.1 Organizations Administering the Document

BPSCA, an entity of BPL, is responsible for the drafting, registering, maintaining, and updating of this CP.

1.5.2 Contact Person

BPSCA Managing Director has authorized, until further notice, the following name and address of the person to lead the BPSCA team dedicated for drafting, registering, maintaining, and updating of this CP

Name: Farid Uddin Ahmed

Designation: Chief of CA Administration

Bangla Phone Secure CA

House# 3, Road# 23/A, Gulshan-1212, Dhaka

Email: bpsca@banglaphone.net.bd

Mobile No: +88 01833 103803

1.5.3 Person Determining CPS Suitability for the Policy

BPSCA Chief of CA Administration is responsible to administer and determine CPS suitability for the policy, provided the intended suitability is duly approved by the CCA.

1.5.4 CPS Approval Procedure

Any change or addition made by the office of CCA for its CA's to implement will be handled by Chief of CA Administration on behalf of BPSCA. He will be responsible to make sure that latest guideline/directives of the CCA are reflected in BPSCA's CPS with proper records. The modified/updated CPS will be published in BPSCA's web site as soon as it's approved.

Document publication link is:
https://digitalsignature.com.bd/Content/Repository/CPS.aspx

1.5.5 CP Review, Update and Approval Procedure

Any change or addition made by the office of CCA for its CA's to implement will be handled by Chief of CA Administration on behalf of BPSCA. He will be responsible to make sure that latest guideline/directives of the CCA are reflected in BPSCA's CP with proper records. The modified/updated CP will be published in BPSCA's web site as soon as it's approved.

Document publication link is:
https://digitalsignature.com.bd/Content/Repository/CPS.aspx

1.6 Definitions and Acronyms

1.6.1 Definitions

SL.	Term	Definition
1	Activation Data	Non-key data (e.g., PINs, passwords) required to operate cryptographic modules.
2	Authentication	Establishing identity based on a trusted credential.
3	Authority Revocation List (ARL)	List of compromised or invalidated cross-certificates issued by a CA.
4	Certificate	A public key certificate.
5	Certification Authority (CA)	Entity issuing digital certificates under PKI to authenticate users.
6	Certificate Authority Workstation (CAW)	Systems handling CA software or keys prior to certification.
7	Certification Path	Ordered certificate sequence for deriving a final object's public key.
8	Certification Practices Statement (CPS)	CA's operational practices for compliance with CCA guidelines.
9	Certificate Revocation List (CRL)	List of invalidated certificates issued by a CA.
10	Cross-Certificate	Certificate issued by one CA to certify another CA's public key.
11	Data Integrity	Assurance that data hasn't changed during transmission or storage.
12	Decryption Private Key	Private key for decrypting data encrypted with the corresponding public key.
13	Distinguished Name	Unique name assigned to identify systems in a certificate.
14	Domain (of a CA)	Scope of a CA's authority over RAs and certified entities.
15	Encryption Certificate	Certificate containing a public key used for

SL.	Term	Definition
		encryption or session key establishment.
16	End Entity (EE)	Subject or user of a certificate, excluding CAs and RAs.
17	Entity	Refers to CA, RA, or end entity.
18	Identity Certificate	Certificate binding an identity to a public key.
19	Inter-site Trust Agreement	Agreement allowing cross-site certificate usage.
20	Key	Value used in cryptographic algorithms for encryption/decryption.
21	Key Materials	Physical representation of a key (e.g., smart card, disk).
22	PKI	See Public Key Infrastructure.
23	Private Key	Secret half of a key pair, held by the owner.
24	Public Key	Public half of a key pair, used in certificates.
25	Public Key Certificate	Public key signed by a CA certifying its validity.
26	Public Key Algorithm	Algorithm using separate encryption and decryption keys.
27	Public Key Infrastructure (PKI)	System managing public key distribution and trust.
28	Registration Authority (RA)	Entity under CA responsible for identifying/authenticating subjects.
29	Relying Party	Entity relying on a certificate for validation.
30	Session Key	Temporary symmetric key for a session's encryption/decryption.
31	Signature Verification Certificate	Certificate with a public key to verify a digital signature.
32	Signing Private Key	Private key used to generate digital signatures.
33	Sponsor	Affiliated person/organization of a subscriber.
34	Subject	Entity issued a certificate by a CA.
35	Subject End Entity	End entity named as the subject in a certificate.
36	Subscriber	See Subject.
37	Symmetric Algorithm	Encryption algorithm using the same key for encryption/decryption.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

1.6.2 Acronyms

Sl.	Acronym	Full Form
1	ARL	Authority Revocation List
2	BPSCA	Bangla Phone Secure Certifying Authority
3	CA	Certification Authority
4	CAW	Certificate Authority Workstation
5	CCA	Controller of Certifying Authorities
6	CP	Certification Policy / Certificate Policy
7	CPS	Certification Practices Statement
8	CRL	Certificate Revocation List
9	FIPS	Federal Information Processing Standard
10	FMS	US Department of Treasury, Financial Management Service
11	IEC	International Electro-technical Commission
12	IETF	Internet Engineering Task Force
13	IP	Internet Protocol
14	ISO	International Organization for Standardization
15	ITU	International Telecommunications Union
16	NIST	National Institute of Standards and Technology
17	OS	Operating System
18	PCA	Policy Certification Authority
19	PIN	Personal Identification Number
20	PKI	Public Key Infrastructure
21	PKIX	Public Key Infrastructure - X.509 (IETF Working Group)
22	PMA	Policy Management Authority
23	RA	Registration Authority
24	RFC	Request for Comments
25	RSA	Rivest-Shamir-Adleman encryption algorithm
26	SA	System Administrator
27	TCSEC	Trusted Computer System Evaluation Criteria

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Repository is defined as a database of digital certificate information. The repository shall be maintained by the certification authority (CA) and shall be queried to find out if a certificate is valid, has expired or has been revoked.

BPSCA shall have the organizational structure to manage its repository functions by assigning a dedicated person.

2.2 Publication of Certification Information

BPSCA web site shall contain repository and other publicly available information such as CPs, CPSs, Certificates and CRLs etc. in the following link

https://www.digitalsignature.com.bd/

2.2.1 Publication of Certificates and Certificate Status

BPSCA shall make the following items available to Subscribers and Relying Parties:

Copies of Public Key Certificates issued
Copies of all CRLs and ARLs issued.

2.2.2 Publication of CA Information

BPSCA shall make the following items available to Subscribers and Relying Parties:

Copies of the CP and CPS.
BPSCA root certificate signed by Root CA/CCA

2.3 Time or Frequency of Publication

The BPSCA shall publish certificates and other information promptly upon issuance or acceptance by it. It will publish its CRLs within one hour upon revocation of any certificate. Apart from this, CRLs will be generated once in every 7 days if there is no certificate revocation.

2.4 Access Controls of Repositories

Information objects of BPSCA, such as CP, CPS, Certificates, Status of Certificates and CRLs, etc., shall be published in the repository portion of BPSCA web site and shall be publicly-accessible.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

The Interoperability Guideline of CCA (i.e. X.500 naming conventions) shall be adhered to by BPSCA for identification of a Subscriber or for recognition of trademark rights in the name of a Subscriber. Subject DN shall consist of following attributes –

- Common Name (CN)
- Serial Number
- Unique Identifier
- Street Address
- House Identifier
- Post Code
- Organizational Unit (OU)
- Organization (O)
- Country (C)

For BPSCA, subject DN will be as follows –

CN= BanglaPhone Secure CA;House Identifier=House No: 3;Street Address:Road No: 23/A, Gulshan-1; Post Code=1212, OU=CA, O= BanglaPhone Ltd, C=BD

3.1.2 Need for Names to be Meaningful

Names used shall identify the person or entity to which they are assigned in a meaningful way. Subscriber/End user CN will be constructed with -last name, followed by a space, followed by first Name. The Interoperability Guideline of CCA shall be adhered to by BPSCA for name meanings.

3.1.3 Anonymity or Pseudonimity of Subscribers

Usually the BPSCA shall not issue any pseudonymous or anonymous certificates. Subscriber Name will verified with identification procedures defined in this document.

3.1.4 Rules for Interpreting Various Name Forms

BPSCA shall use Interoperability Guideline of the CCA to interpret various name forms.

3.1.5 Uniqueness of Names

Name of each certificate shall be unique and distinguished which will be issued to a Subscriber by the BPSCA.

If the DN presented by the Subscriber is not unique, the BPSCA will ask the Subscriber to resubmit the request with some variation to the Common Name to ensure uniqueness.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

3.1.6 Recognition, Authentication, and Role of Trademarks

BPSCA shall follow X.500 standard and interoperability guideline for implementing naming conventions.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The BPSCA shall verify the possession of the private key relating to certificate requests at the time of identity verification by BPSCA Operator. The applicant or any system designated by the applicant shall have to submit a Certificate Signing Request (CSR) in PKCS#10 format. Also the information in CSR shall be checked to find match with the certificate requestor.

3.2.2 Authentication of Organization and Domain Identity

The RA operating under BPSCA shall verify the authorization letter to ensure if the person is authorized by the organization. Following documents shall be checked for verification of the organization –

- Trade License
- VAT Registration
- TIN
- Certificate of Incorporation
- Memorandum & Articles of Association
- Postal mail, Telephone & Website address

Also the organizational information in Certificate Signing Request is checked to find match with the authorized person.

3.2.3 Authentication of Individual Identity

The RA operating under the BPSCA shall perform appropriate verification of an individual entity based on the information provided in the online application form. The RA shall perform the verification depending on the Digital Certificate class types as specified in this section. The following documents are accepted by BPSCA:

Photo ID: Passport, NID, Driving License
Address Proof: Telephone Bill, Electricity Bill, Gas Bill

BPSCA will also provide e-KYC system for subscribers based on Facial and Fingerprint matching.

3.2.3.1 Class 1 Certificates

For Class 1 certificates, only non-ambiguity of the common name and email address of the applicant shall be ensured within the BPSCA repository and also verification of the email address is done.

3.2.3.2 Class 2 Certificates

For Class 2 certificates, applicant's identity shall be verified by determining if identifying information in the certificate application matches with that of identity proof documents or through e-KYC system provided by BPSCA

3.2.3.3 Class 3 Certificates

For Class 3 certificates, applicant's identity shall be verified physically along with the verification done for Class 2 Certificates or through e-KYC system provided by BPSCA.

For Class 3 Certificates, The BPSCA might, in future, consider exceptions to the above restrictions for cases in which it is impossible or impractical to have the end entity appear in person. In such cases and once permitted, the BPSCA shall consider issuing a certificate based on the signed statement of a sponsor affirming he or she personally knows the Applicant and accepting responsibility for compliance with this CP.

For SSL certificate, BPSCA will verify the domain ownership through specific file uploading process. The applicant shall upload the file provided by BPSCA, so that the BPSCA verification system can access the file through the domain URL.

3.2.3.4 e-Sign Certificates

For e-Sign certificates, the applicant will be verified by CCA approved e-KYC system provided by BPSCA.

3.2.4 Non-Verified Subscriber Information

For Class 1 - Individual certificates verified only by email address, the Issuer CA shall not be required to confirm that the common name requested by the Applicant is the legal name of the Subscriber, and such certificates shall contain a notice advising potential relying parties that the person's identity has not been verified.

SSL Certificates may contain a pseudo-domain for use within the Subscriber's internal, non-public-DNS networks. The Issuer CA may rely on the Subscriber's indication of the server or host name to issue a certificate containing the fully qualified domain name that includes the server or host name.

Any other non-verified information included in a certificate shall be designated as such in the certificate. No unverified information shall be included in any Class 2 and Class 3 certificate.

3.2.5 Validation of Authority

BPSCA Operator shall verify a Subscriber to authenticate his affiliation/association/ representation with the Organization for which he requested the certificate for. There must be at least one valid document which unambiguously corroborates the proof that the Subscriber's declared relationship with an organization is founded.

3.2.6 Criteria for Interoperation

Interoperability criteria will be as per Interoperability guideline from CCA.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

A Subscriber will be treated as being the same as stipulated in the Clause 3.2 will be applicable for Subscriber's Routine Authentication.

3.3.2 Identification and authentication for Re-key after Revocation

When authenticating a Subscriber's identity for Re-key after certificate revocation, he will be treated as a fresh requestor. Clause 3.2 of this document will be followed to authenticate this Subscriber.

The procedure for re-authentication is exactly the same with an initial registration.

3.4 Identification and Authentication for Revocation Request

Certificate revocation requests made by a Subscriber of individual entity or on behalf of his associated Organization, shall have to be identified and authenticated through one of the following ways:

– By signing a revocation request with the private key of the corresponding certificate which is being requested for revocation, and sending the request to BPSCA via e-mail. BPSCA will authenticate the revocation request using the requestor's public key to decrypt, also communicating with the requestor via phone/fax/mail. The certificate, for which revocation is requested, must be a valid, non-expired and non-revoked certificate.

– By a person who retains authorization as an Administrator for a host or service certificate, requests a revocation to the BPSCA Admin by signing e-mail with the private key of the corresponding certificate. When e-mail is not an option, the identification of the requestor and authentication of his eligibility for such a request will be made by using the guideline stipulated in the Clause 3.2.3 of this CP Document.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Certificate application processing will be done by RA and certificate issuing will be done by BPSCA for all classes of certificate. For e-Sign certificates, certificate request will be received from e-Sign system through secured API channel.

4.1.1 Who Can Submit a Certificate Application

For class 1, class 2 and class 3 certificates, any person or authorized representative of organizational entity can apply for a certificate to BPSCA Operator. In case of device

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

certificate (such as, SSL, code-Signing etc.), the person responsible for support & maintenance of the device will submit the application. For e-Sign certificates, the e-Sign system will submit certificate request through secured API.

4.1.2 Enrollment Process and Responsibilities

BPSCA Chief of CA Administration shall be responsible to establish an enrollment process for his CA team to assist in receiving a certificate application requested by a user.

- User Certificate:

A user, applying by way of filling out relevant online application form, may send the request via e-mail or directly come over to the RA that operates under BPSCA. RA shall receive the application and take steps to authenticate the validity of application information with regard to the Clause 3.2.3 of this document.

If a Subscriber of BPSCA Certificate requests for re-key of his certificate, guideline stipulated in Clause 4.7 of this document shall be followed to address this request.

- SSL Certificate

A Person, authorized by his organization to apply for SSL certificate, sends e-mail to BPSCA as per guideline of the Clause 1.5.2 of this document stating identities of being the authorized person for the mentioned certificate.

BPSCA Help Desk shall receive this application, keep records and forward to the Operator to verify the authentication of the Person as per the guideline mentioned in the Clause 3.2.3, and processing of the request as per Clauses 4.2.1 and 4.2.2 of this document.

- e-Sign Certificates

For e-Sign certificates, certificate request will be received from e-Sign system through secured API channel. Applicant will be verified through CCA approved e-KYC process.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Guideline described in the Clauses 3.2.3 shall be used to validate individual identity.

Validation of Organizational information and documents shall be done using the guideline described in Clause 3.2.2 in the event that certification is requested for an organization.

4.2.2 Approval or Rejection of Certificate Applications

If the individual or organization fails to prove his/her identity, it will be rejected with no exception.

4.2.3 Time to Process Certificate Applications

A request for certification is normally handled within 3 working days except for e-Sign certificates. For e-Sign certificates, the certificate will be generated automatically and sent

to e-Sign system through secured API.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Processing of a request upon completion of validation shall be made by BPSCA. BPSCA Chief of CA Administration shall ensure strict adherence to establish procedures in order to maintain security and integrity of BPSCA properties, products, equipment, and personnel involved in these activities.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

BPSCA Support Desk shall notify the applicant via e-mail/phone about the issuance and availability of certificate and stipulate specific timeline to collect the certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Once a Subscriber comes to BPSCA office at the notified date and time and receives the certificate, the event will be deemed as his acceptance of the certificate. It's the responsibility of subscriber to install the certificate on his/her machine according to standard certificate installation process. For e-Sign certificates, the certificate will be sent to e-Sign system through secured API and this event will be deemed as acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

Certificate will be published in BPSCA's website within 24 hours of acceptance.

4.4.3 Notification of Certificate Issuance by the CA to other Entities

BPSCA shall not follow any other means of notification or publication of information pertaining to issuing certificate for an entity except for the means as described in the Clause 2.2 of this document.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Key usage shall be specified in certificate - in 'Key Usage' extension filled of any digital certificate. It shall be subscriber's responsibility to protect and use the private key. A certificate with key usage field containing 'digital signature and non-repudiation' shall only be used for digital signing – it cannot be used for encryption.

BPSCA shall not record any information of a Subscriber's Private Key associated with an issued certificate. Subscribers shall be required to be extra careful to protect individual Private Key from being compromised or disclosed to any other entity.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall be required to use public key certificates and associated public keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates.

4.6 Certificate Renewal

As per IT CA Rules 2010, BPSCA shall not support renewal of certificates in any circumstances. It is treated as certificate Re-key.

4.6.1 Circumstances for Certificate Renewal

Not Applicable.

4.6.2 Who may Request Renewal

Not Applicable.

4.6.3 Processing Certificate Renewal Requests

Not Applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not Applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not Applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not Applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not Applicable.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-key

The following events shall warrant the circumstances for a Subscriber to apply for certificate re-key:

- When the validity period of a particular certificate expires in just 30 days.
- When the certificate is revoked and the Subscriber applies again

4.7.2 Who may Request Certification of a New Public Key

A subscriber may request the re-key of its certificate.

4.7.3 Processing Certificate Re-keying Requests

Sub-Clauses 4.2.1, 4.2.2, 4.2.3 describes BPSCA policy for processing of Certificate Re-key request i.e. the same procedure to issue a new certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See Section 4.4

4.7.6 Publication of the Re-keyed Certificate by the CA

Same as Clause 2.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

As per IT CA Rules 2010, BPSCA shall not support modification of certificates in any circumstances.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not supported.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not supported.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Revocation of a digital certificate may occur under two distinct circumstances:

1. **Subscriber-Initiated Revocation**:
   The Subscriber lawfully and intentionally requests revocation of their certificate. Clause 3.4 of this document outlines the acceptable methods for submitting such revocation requests within the scope of the Subscriber's lawful authority.
2. **BPSCA-Enforced Revocation**:
   The Bangladesh Public Sector Certification Authority (BPSCA) may initiate revocation of a certificate when the Subscriber fails to comply with the terms and conditions binding upon them, or when other risk factors compromise the trustworthiness of the certificate.

The BPSCA may enforce revocation of a certificate under the following circumstances:

- The certificate contains incorrect, inaccurate, or false information, or its implied assertions are known or suspected to be compromised.
- The Subscriber is found to have violated the obligations they agreed to comply with.
- Substantiated evidence is presented by any third party indicating a serious breach of obligations by the Subscriber.
- The Subscriber has contravened any provision of the **ICT Act 2006** or the **Information Technology (CA) Rules 2010**.
- The private key corresponding to the certificate's public key has been lost, disclosed without authorization, stolen, or otherwise compromised.
- The BPSCA suspects or determines that revocation is necessary to protect the integrity of its operations.
- The certificate was improperly or erroneously issued due to:
  - A material prerequisite for issuance not being fulfilled.
  - A material fact stated in the certificate being known, or reasonably believed, to be false.
- The Subscriber is deceased.
- The Subscriber has been declared insolvent by a competent court or legal authority.
- Revocation is ordered by appropriate government authorities, a court of law, or law enforcement agencies.

4.9.2 Who Can Request Revocation

The BPSCA or any of its Subscribers or any entity holding evidence of a revocation circumstance committed by any other entity is eligible to request for a revocation. So the entities are –

- BPSCA
- Subscriber/ End user
- Any entity holding evidence of a revocation circumstance committed by any other entity
- Law enforcement agencies of Bangladesh Government

4.9.3 Procedure for Revocation Request

Revocation request will be submitted in writing or e-mail to BPSCA nominated contact person. BPSCA will confirm the requestor about receipt of the revocation request. Clause 3.4 of this document is used to authenticate identity of the Subscriber requesting the revocation. If identity can be confirmed, the certificate will be revoked using BPSCA software. The revocation information will be included in CRL and published accordingly.

4.9.4 Revocation Request Grace Period

BPSCA will handle revocation requests with priority as soon as the request is recognized as such. When a Subscriber submits a revocation request, the following steps shall be taken to ensure proper, secure, and timely handling:

1. Submission Verification
    - The revocation request must be submitted through authorized channels as defined in Clause 3.4 of this document.
    - The identity of the Subscriber must be authenticated to prevent unauthorized revocation.
2. Request Validation
    - The BPSCA shall validate the authenticity and completeness of the revocation request.
    - The reason for revocation must be reviewed to ensure it falls within acceptable grounds (e.g., key compromise, change of affiliation, loss of control over private key, etc.).
3. Certificate Status Update
    - Once verified, the certificate shall be marked as revoked in the BPSCA repository and immediately added to the Certificate Revocation List (CRL).
    - The OCSP (Online Certificate Status Protocol) responder shall also be updated to reflect the certificate's revoked status.
4. Acknowledgment to Subscriber
    - The BPSCA shall notify the Subscriber that the revocation request has been processed and confirmed the revocation status, including the effective date and time.
5. Public Notification

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

- The revocation shall be published through appropriate public repositories (e.g., CRL Distribution Points) to ensure that relying parties are informed of the change in certificate status.

6. Record Keeping

- All relevant logs, correspondence, and verification evidence related to the revocation request shall be retained by the BPSCA for audit and compliance purposes as per the defined retention policy.

4.9.5 Time within Which CA Must Process the Revocation Request

The BPSCA will process all revocation requests within 3 days (excluding weekends and public holidays of Bangladesh) after receiving a revocation request.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties are responsible for checking the validity of each certificate in the certificate path, including checks for certificate validity, issuer-to-subject name chaining, certificate policy and key usage constraints, and the status of the certificate through the Certificate Revocation List (CRL).

4.9.7 CRL Issuance Frequency

CRLs shall be updated, re-issued and published within 1 hour after every approved certificate revocation, but at least seven 7 days before the stated next update time in the latest-issued CRL.

4.9.8 Maximum Latency for CRLs

CRLs shall be published on BPSCA's website as soon as it's generated.

4.9.9 On-line Revocation/Status Checking Availability

BPSCA may provide on-line revocation status (OCSP) checking for relying parties. It will be available for relying parties on request. BPSCA will share the URL for OCSP responder with relying parties as and when required.

4.9.10 On-line Revocation Checking Requirements

It is the responsibility of relying party to check certificate status. BPSCA will recommend relying party to check certificate status as and when required.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Related to Key Compromise

Subscribers must notify relying parties as soon as practical regarding its key compromise.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

4.9.13 Circumstances for Certificate Suspension

A certificate may put on hold (i.e. suspended) for a short period due to following circumstances -

- Due to order from law enforcement agency, court or Bangladesh Government
- Subscriber requests to suspend his/her certificate
- Suspicious activity of subscriber reported to BPSCA
- Any other circumstance which may lead BPSCA to suspend the certificate

4.9.14 Who can Request Suspension

- BPSCA
- Subscriber/ End user
- Any entity holding evidence of a suspension circumstance committed by any other entity
- Law enforcement agency of Bangladesh Government

4.9.15 Procedure for Suspension Request

Suspension request will be submitted in writing or e-mail to BPSCA nominated contact person. BPSCA will confirm the requestor about receipt of the suspension request. Clause 3.4 of this document is used to authenticate identity of the Subscriber requesting the suspension. If identity can be confirmed, the certificate will be suspended using BPSCA software.

4.9.16 Limits on Suspension Period

A certificate will be suspended for maximum 15 days. If no information is available from requestor, the certificate will be revoked by BPSCA.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Any individual or relying party can check status of certificate from public repository of BPSCA.

4.10.2 Service Availability

BPSCA shall have to put the best efforts to make such services available 24x7.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

If a certificate is revoked prematurely for the reasons stated in this document, the subscription of that certificate will be treated as no longer active from the time of

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

revocation.

4.12 Key Escrow and Recovery

In case of key escrow service provided by a CA, the generation of the encryption key pair for key escrow is done at the CA end in secure premises and is protected with a password. A copy of the Encryption key of the subscriber is retained in the safe custody of the CA. BPSCA shall not generate or archive subscriber's private key. So BPSCA shall not provide key escrow service.

Also, there shall be no key recovery services provided or implied, and subscribers should exercise care not to lose their private keys after they have generated them.

4.12.1 Key Escrow and Recovery Policy and Practices

Under no circumstances end entity signature key will be escrowed by a third-party.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Security Controls

5.1.1 Site Location and Construction

All CA and RA operations shall be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical Access

Access to certificate issuance systems is only allowed for the responsible officers of BPSCA. In case other individuals need to access the service area where the CA systems are located, proper authorization must be obtained in advance. All visiting individuals must be recorded in the access log and must be accompanied by the responsible officer during the whole visit.

The certificate issuing servers and Cryptographic Module must be stored in a secure area where physical access to such systems requires dual-control and two-factor authentication.

5.1.3 Power and Air Conditioning

BPSCA shall have backup power capability sufficient to lock out input, finish any pending

actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The repositories (containing certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of 6-hour operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 Water Exposures

The secure facilities of BPSCA shall be constructed and equipped, and procedures shall be implemented, to prevent floods or other damaging exposure to water, e.g.: on raised floor equipped with water sensor.

5.1.5 Fire Prevention and Protection

The secure facilities of BPSCA shall be constructed and equipped, and procedures shall be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures shall meet all local applicable safety regulations.

5.1.6 Media Storage

BSPCA shall protect the magnetic media holding backups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and shall use protective measures to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media.

Protective Measures

To ensure the confidentiality, integrity, and availability of critical system data and sensitive information, BPSCA shall implement the following protective measures for the storage of magnetic and other forms of backup media:

1. Environmental Protection

- Fire Protection: Store backup media in fire-resistant storage cabinets or vaults certified to withstand high temperatures.
- Water Protection: Use waterproof and moisture-resistant containers or enclosures; locate storage areas away from plumbing and other water sources.
- Climate Control: Maintain controlled temperature and humidity levels in storage areas to prevent media degradation.
- Seismic Safety: Where applicable, ensure storage racks or cabinets are anchored to withstand minor seismic activity.

2. Physical Security

- Secure Locations: Store media in restricted-access, locked rooms or vaults with 24/7 surveillance and access logs.
- Access Control: Grant access only to authorized personnel through multi-factor authentication mechanisms (e.g., biometric + keycard).
- Media Labeling: Clearly label backup media with classification levels and handling instructions, but avoid displaying sensitive content titles on the label.

3. Logical and Operational Protection

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

- Encryption: Encrypt all sensitive data stored on backup media using strong encryption standards (e.g., AES-256).
- Data Integrity Checks: Periodically verify the integrity of stored data using checksums or hash validation techniques.
- Audit Logging: Maintain audit trails of all access to media storage locations and media handling operations.

4. Backup and Redundancy

- Offsite Storage: Maintain redundant copies of critical backups in geographically separate, secure offsite locations.
- Regular Backup Schedule: Follow a defined backup schedule (e.g., daily incremental, weekly full) and test restorability periodically.

5. Media Handling and Disposal

- Transport Security: When media is in transit, use tamper-evident packaging and secure transportation protocols.
- Media Reuse: Sanitize media before reuse using approved data-wiping or degaussing techniques.
- Media Disposal: Destroy expired or unusable media using secure destruction methods such as shredding, incineration, or degaussing, and document the disposal process.

6. Incident Response

- Monitoring: Continuously monitor media storage environments for signs of tampering or environmental threats.
- Incident Protocols: Define response procedures in case of media compromise, damage, or unauthorized access attempts.

5.1.7 Waste Disposal

BPSCA shall implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing Confidential/Private Information.

Paper waste containing sensitive data shall be shredded before disposal. Sensitive data on magnetic or other digital media must be permanently erased before disposal.

5.1.8 Off-site Backup

A backup media must be stored at a secure off-site facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the PKI is weakened. The functions performed in these roles form the basis of trust for all uses of the BPSCA. The following shall be the trusted roles for BPSCA:

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

- Chief of CA Administration
- CA System Administrator
- CA Verifier
- CA Operator (RA User)
- CA Auditor
- DBA

5.2.2 Number of Persons Required Per Task

For the CA, at least two persons shall be present and actively aware of the current operation when any of the key operations, (i.e. CA key-pair generation, certificate revocation etc.) are performed.

These persons shall be those assigned one of the roles listed in clause 5.2.1, or an authorized delegate. All such two-person accesses shall be documented, including the names of both persons.

5.2.3 Identification and Authentication for Each Role

Each person will be identified and authenticated before he/she performs any assigned task. Otherwise, he/she will require authorization at first.

5.2.4 Roles Requiring Separation of Duties

Trusted roles will be assigned to separate persons. i.e. one person won't be assigned more than one role.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

BPSCA shall ensure that all personnel involved in Certification Authority (CA) functions meet the required qualifications, possess relevant experience, and have obtained necessary clearances, in alignment with the recruitment procedures defined by Bangladesh Phone Limited (BPL).

BPL, through its dedicated Human Resources (HR) function, is responsible for formulating and executing all recruitment-related activities. This includes the development of eligibility criteria, verification of academic and professional qualifications, assessment of prior work experience, and validation of security clearances as required for CA operations.

All recruitment, onboarding, and role assignment processes shall comply with the guidelines outlined in the **CA Personnel Guidelines, 2024**, and with any applicable national regulatory or legal frameworks.

5.3.2 Background Check Procedures

BPSCA shall ensure that comprehensive background checks are conducted for all personnel assigned to CA-related responsibilities, as per the recruitment procedures and protocols established by BPL.

BPL's HR department shall be responsible for executing background verification, which includes but is not limited to:

- Identity verification (e.g., NID, passport)
- Educational and professional certificate verification
- Employment history checks
- Criminal record checks (through authorized law enforcement channels)
- Financial integrity checks (if applicable to the role)

All background checks shall be conducted before final placement of personnel in sensitive roles, ensuring adherence to the **CA Personnel Guidelines, 2024**, and any relevant compliance or legal requirements.

5.3.3 Training Requirements

BPSCA shall perform a training need assessment for the trusted roles periodically and carries out necessary steps to provide necessary trainings for them. Particular training needed shall be identified by Supervisors for his subordinates for a year on the following topics as needed

- Cryptography, PKI and CA security principles and CA related Law and Guidelines
- HSM administration and CA software operation and maintenance
- CA operational procedures
- Business continuity and disaster recovery procedures
- CA operation roles and responsibilities
- Customer support and Incident management

HR shall manage all the training formalities and maintain records.

5.3.4 Retraining Frequency and Requirements

Retraining needs shall also be identified by supervisor for his subordinates as and when required.

5.3.5 Job Rotation Frequency and Sequence

It shall be governed by HR as per BPL operational procedures.

5.3.6 Sanctions for Unauthorized Actions

BPSCA will take disciplinary actions for any unauthorized access or subversive activities related to its system and operations as per ICT act 2006

5.3.7 Independent Contractor Requirements

No Stipulation.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

5.3.8 Documentation Supplied to Personnel

BPSCA shall make available the required policies, procedures, guidelines to its employees so that they can perform their responsibilities.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

BPSCA shall keep log of the following events:

- Certification requests;
- Issued certificates;
- Requests for revocation;
- Issued CRLs;
- Login/logout/reboot of the signing machine;
- For each approved request, how it was approved by RA;
- For each rejected request, why it was rejected by RA;
- For each approved revocation request, the reason for revocation;
- For each rejected revocation request, the reason for revocation and the reason the request was rejected for.
- Other RA activity logs

The following point shall be included in the log entries:

- Type of entry
- Date and time of the entry
- Serial or sequence number of entry
- Identity of the entity making the log entry

5.4.2 Frequency of Processing Log

Audit logs shall be processed at least once per quarter.

5.4.3 Retention Period for Audit Log

Audit logs will be retained for a minimum of 3 years.

5.4.4 Protection of Audit Log

Only authorized BPSCA personnel shall be allowed to view and process audit logs. Unauthorized access to the audit logs shall be restricted by physical and logical access control systems and such access will be logged.

5.4.5 Audit Log Backup Procedures

Audit logs shall be regularly backed up and stored securely in accordance with BPSCA's official backup policy as per the CA license. These backups shall be transmitted to a designated backup server on a scheduled basis.

To ensure reliability, all backup data shall be tested periodically for validation and successful restoration, in consultation with the Chief of CA Administration. Backup files shall be retained for the duration specified in the data backup retention policy.

Access to audit log backups shall be strictly limited to authorized personnel within the CA Administration.

5.4.6 Audit Log Accumulation System (Internal vs. External)

Security Audit log collection system shall be internal to the BPSCA.

5.4.7 Notification to Event-Causing Subject

This CP 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

BPSCA shall follow defined procedure to identify potential attempts to breach the security of the system. Vulnerability assessments shall be done yearly. Corrective measures shall be taken if any issue is detected after such assessments

5.4.9 Penetration Test Assessments

BPSCA shall assesse penetration testing assessment quarterly according to defined procedures. Corrective measures shall be taken if any issue is detected after such assessments.

5.5 Records Archival

5.5.1 Types of Records Archived

In brief, the following are the types of records that shall be archived:

- Certification requests;
- Issued certificates;
- Requests for revocation;
- Issued CRLs;
- Login/logoff/reboot of the signing machine;
- Personal identification photocopies gathered by BPSCA stuff.

5.5.2 Retention Period for Archive

Records shall be retained for at least 7 (seven) years unless there are specific requirements.

5.5.3 Protection of Archive

Only authorized BPSCA personnel shall be allowed to view and process archived logs. Unauthorized access to the audit logs shall be restricted by physical and logical access control systems and such access will be logged.

5.5.4 Archive Backup Procedures

All data and files shall be copied to secured backup server.

5.5.5 Requirements for time-stamping of records

All system generated logs shall be time stamped.

5.5.6 Archive Collection System (Internal or External)

The archive collection system shall be internal to the BPSCA.

5.5.7 Procedures to Obtain and Verify Archive Information

Archived media shall be verified just after archival operation. Also, archived data are verified for integrity once a year.

5.6 Key Changeover

The BPSCA private key shall be changed periodically; from that time on, the new key will be valid in order to sign new certificates or CRL lists of new certificates. The older private key shall be used to sign CRLs until all the certificates signed using the associated key have expired or been revoked.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If BPSCA detects a potential hacking attempt or other form of compromise to its system/data, it shall perform an investigation in order to determine the nature and the degree of damage. If 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, only some certificates need to be revoked, and/or the CA key needs to be declared compromised

5.7.2 Computing Resources, Software, and/or Data are Corrupted

In case of software, hardware or data failure, BPSCA officers will report such incidents to the higher authorities in order to make decisions and a disaster recovery plan may be used if necessary.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

5.7.3 Entity Private Key Compromise Procedures

If the BPSCA private key is (or is suspected to be) compromised, it will:

- Immediately inform CCA;
- Inform the subscribers and customers of which it is aware;
- Conclude the issuance and distribution of certificates and CRLs;
- Generate a new BPSCA certificate with a new key pair that will be soon available on the website.

5.7.4 Business Continuity Capabilities after a Disaster

BPSCA shall have disaster recovery site physically separated from the primary site. BPSCA shall have Disaster Recovery plan to mitigate any kind of disaster that will make the primary site inoperable. This plan shall be reviewed and upgraded regularly by the BPSCA management team.

The disaster recovery site shall be synchronized with the primary site so that quick restoration of service is possible. CA and Sub-CA keys shall also be backed up to avoid loss due to disaster. DR site's security shall be ensured according to the CA security guidelines.

In case of disaster, operation shall be continued through the DR site so that less system down-time can be ensured. Primary site recovery shall then be done so that operation can be continued from there as soon as possible.

5.8 CA or RA Termination

If **BPSCA (as a CA)** or any affiliated **Registration Authority (RA)** terminates operation—due to convenience, contract expiration, reorganization, or other non-security-related reasons—the following steps shall be taken, as defined in the agreement between the Controller of Certifying Authorities (CCA) and BPSCA:

A. General Actions upon CA Termination

- The Agreement between BPSCA and the CCA shall specify procedures to ensure continuity and support for all certificates issued prior to termination.
- At a minimum, BPSCA shall:
  - Preserve and secure the BPSCA information archive as described in its Certification Practice Statement (CP).
  - Retain and protect all cryptographic materials (e.g., CA private keys, key escrow information) in compliance with CP and legal requirements.
  - Notify all Subscribers, Relying Parties, and stakeholders of the CA termination and associated timelines.
  - Revoke or transfer all valid certificates issued under the CA, as necessary.
  - Ensure continuity of certificate status services (e.g., CRL, OCSP) through coordination with CCA or a successor CA.
  - Conduct a final compliance audit if required by regulatory authorities.
  - Provide documentation and technical assistance to the CCA or designated successor entity.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

B. RA-Specific Termination Procedures

In case of **RA termination**, whether operated internally or through a delegated entity, the following steps must be performed:

- Notification and Coordination
  - The RA shall formally notify BPSCA of its intent to terminate operations, including reasons and proposed termination date.
  - BPSCA shall notify the CCA of the RA termination and coordinate the reassignment of RA functions if required.
- Secure Handover of Records
  - All RA records, including identity validation documents, registration requests, logs, and audit trails, shall be securely transferred to BPSCA or another designated RA.
  - The RA shall ensure the integrity and confidentiality of data during transfer and archival.
- Revoke or Transition Pending Requests
  - Any pending certificate requests or identity validation processes must be completed, transitioned, or cancelled under supervision of BPSCA.
  - Subscribers whose requests are in progress shall be informed and guided accordingly.
- Disable Access Privileges
  - All system access rights, credentials, tokens, and cryptographic devices assigned to the RA and its personnel shall be revoked or deactivated immediately upon termination.
  - RA personnel shall return all hardware, software, and sensitive documents to BPSCA or its designated authority.
- Final Compliance and Exit Audit
  - A final audit may be conducted by BPSCA or a third-party to ensure full compliance with RA responsibilities and proper decommissioning of RA operations.
- Public Communication
  - Appropriate public notification shall be issued to inform Subscribers and relying parties about the change in RA operations, including updated contact information for continued services.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key Pair generation shall be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys. The Hardware Security Modules (HSM's) used for key generation shall have to meet the requirements of FIPS 140-2 Level 3 to store the BPSCA keys.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

BPSCA shall generate the Key Pair in HSM room, which shall be very secure and restricted for authorized personnel, during key generation ceremony. It shall be a formal event and witnessed by CCA officials and other invited guests.

6.1.2 Private Key Delivery to Subscriber

Subscriber will generate his/her own private key pair in a secure way. For e-Sign certificates, one time private key will be generated at e-Sign system and destroyed after signing. So delivery of private key by BPSCA is not applicable here.

6.1.3 Public Key Delivery to Certificate Issuer

Subscriber public key shall be delivered via soft/hard crypto token with the exception of e-Sign certificates where certificate along with public key is delivered to e-Sign system BPSCA will keep subscriber's public key and will publish in its website.

6.1.4 CA Public Key Delivery to Relying Parties

BPSCA will keep its public key in its CA's website enabling any one to access it.

6.1.5 Key Sizes

As per CCA guideline, key size will be 2048 bits or higher.

6.1.6 Public key Parameters Generation and Quality Checking

RSA and ECC keys shall be generated in accordance with FIPS 186-2.

6.1.7 Key Usage Purposes

Public keys that are bound into end user certificates shall be certified for use in authenticating, signing or encrypting, but not all, except as specified by BPSCA. The use of a specific key shall be determined by the key usage extension in the X.509 certificate.

BPSCA keys shall be used for certificate signing and CRL signing.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

BPSCA shall keep its private key in a very secure place and it will be almost impossible to temper it. Moreover BPSCA shall have its HSM to contain private key which maintain FIPS-140-2 level 3 standards.

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

BPSCA shall maintain a Multi-Person Control approach (n out of m rule) to generate and use its private key.

6.2.3 Private key Escrow

BPSCA shall not support private key escrowing.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

6.2.4 Private Key Backup

BPSCA private key shall be backed up using multi person control periodically.

6.2.5 Private key archival

At the end of the validity period, CA private key will be destroyed and will not be archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

BPSCA private key shall not be transferred to anywhere, except for taking backup via secure way. It will not be saved temporarily or permanently in any software for any purpose.

6.2.7 Private Key Storage on Cryptographic Module

BPSCA private key shall be stored in a FIPS-140 level 3 supported cryptographic module.

6.2.8 Method of Activating Private key

BPSCA's private key shall be activated by the main stakeholders and authorized personnel, as defined in clause 6.2.2, supplying their activation data.

6.2.9 Method of Deactivating private key

No Stipulation. Cryptographic module that has been activated shall never be left unattended or otherwise available to unauthorized access. After use, cryptographic modules shall be deactivated. After deactivation, the use of the cryptographic modules-based CA key pair shall require the presence of the trusted roles with the activation data in order to reactivate said CA key pair.

6.2.10 Method of Destroying Private Key

All Private Signing and Authentication keys shall be destroyed when they are no longer needed, or when the Certificates to which they correspond expire or are revoked.

6.2.11 Cryptographic Module Rating

Cryptographic Module Rating shall comply with FIPS 140-2 Level 3 standard.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public keys of all issued certificates shall be archived as a part of certificate archival.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

BPSCA's root certificate shall have a validity of ten years. For subscribers, the maximum validity period for a certificate shall be maximum 24 (twenty four) months. For e-Sign certificates, the validity will be according to CCA guideline.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data holders shall be responsible for their accountability and protection. When they are not used, activation data shall always be stored in a safe for which access is controlled by holders in limited roles.

6.4.2 Activation Data Protection

The activation data used to unlock private keys shall be protected from disclosure.

6.4.3 Other Aspects of Activation Data

Not applicable.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Following steps shall be applied to ensure technical security requirements –

- operating systems shall be maintained at a high level of security by applying in a timely manner all recommended and applicable security patches;
- monitoring shall be done to detect unauthorized software changes;
- System services shall be reduced to the bare minimum.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

The software shall be developed in a controlled environment, such as one that follows or is equivalent to the Trusted Software Development Methodology [TSDM] level T2 or higher. It ensures protection against the insertion of malicious logic into software that implements CA functionality.

6.6.2 Security Management Controls

The configurations of the BPSCA systems as well as any modifications and upgrades shall are documented and controlled. A formal configuration management methodology shall be used for installation and ongoing maintenance of the system.

6.6.3 Life Cycle Security Ratings

Not applicable.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

6.7 Network Security Controls

BPSCA signing server shall always be disconnected from any external network. Public servers shall be protected via firewall and other network security devices.

6.8 Time Stamping

BPSCA will provide Time Stamping service according to "Time Stamping Services Guidelines for Certifying Authorities (CA)" provided by CCA.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Number

The certificates issued by BPSCA shall be in accordance with X.509 version 3.

7.1.2 Certificate Extensions

X509v3 Certificate extensions shall be supported. Interoperability guideline from CCA will supersede in this case.

7.1.3 Algorithm Object Identifiers

Algorithm	Object Identifier
RSA Encryption	1.2.840.113549.1.1.1
SHA256 With RSA Encryption	1.2.840.113549.1.1.11
SHA256	2.16.840.1.101.3.4.2.1

7.1.4 Name Forms

Issuer: DC=Bangla Phone Secure CA, O=banglaphone.net.bd, CN= Bangla Phone Secure CA Certification Authority

Interoperability guideline from CCA will supersede in this regard.

7.1.5 Name Constraints

No Stipulation.

7.1.6 Certificate Policy Object Identifier

CA and Subscriber Certificates issued under this CP shall assert a certificate policy OID.

7.1.7 Usage of Policy Constraints Extension

According to the guideline of CCA, BPSCA will define this extension. BPSCA may discuss with other CA to set their Certificate Policies Extension for Email Protection.

7.1.8 Policy Qualifiers Syntax and Semantics

Not Applicable.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not Applicable.

7.2 CRL Profile

7.2.1 Version Number(s)

All CRLs will be issued in accordance with RFC5280 version 2.

7.2.2 CRL and CRL Entry Extensions

The BPSCA shall support and use the following CRL and CRL entry extensions:

– cRLNumber: monotonically increasing sequence number for each CRL issued by the CA;

– X509v3 CRL Reason Code: non-critical extension, carrying the revocation reason code as specified in RFC3647.

7.3 OCSP Profile

The Online Certificate Status Protocol (OCSP) is the way for subscribers to obtain information about the revocation status of certificates.

7.3.1 Version Number(s)

BPSCA shall issue Version 1 OCSP responses.

7.3.2 Fields in OCSP Responses

Fields in the OCSP responses shall be in accordance with RFC 6960.

7.3.3 OCSP Extensions

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

BPSCA shall conduct internal compliance audit once in every 3 months. The frequency is subject to change after one year of commercial operation, which will be fixed when needed. External Audit will be conducted as per IT CA Rules 2010 and instructions from Office of the CCA.

8.2 Identity and Qualifications of Assessor

BPSCA shall have a trusted role for compliance audit purpose. Eligibility for this role is deep knowledge of PKI and its operations and expertise in auditing IT system.

8.3 Assessor's Relationship to Assessed Entity

The person having role for compliance audit shall not be engaged in day-to-day operations of BPSCA. So he/she is able to leverage unbiased and independent evaluation.

8.4 Topics Covered by Assessment

The scope of BPSCA's compliance audit shall include CA environmental controls, CA key management, certificate life cycle management, CA business practices disclosure, physical movement of employees to operate the system, system log which contains logs of activities performed by authorized auditors with the BPSCA system.

There will be an audit checklist which will include all the topics to be audited.

8.5 Actions Taken as a Result of Deficiency

The audit report shall be submitted to the higher management of BPSCA. Assessor shall describe the scenario to the higher management, take his guidelines, and action plan shall be prepared by assigning resources to address the findings and close them within a stipulated time.

8.6 Communications of Results

The entire audit system, various steps, findings and actions taken, etc. shall be recorded properly. The results shall be communicated to the respective stakeholders at a pre-defined sequence.

8.7 Self-Audits

BPSCA shall monitor adherence to its CP and CPS and these requirements by performing self-audits on at least a quarterly basis.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

BPSCA shall establish a structure for fees/charges it wishes to propose against certificate issuance and renewal. This fee structure shall be established as per guideline from office of the CCA.

9.1.2 Certificate Access Fees

No fee is required to access certificate from BPSCA public repository.

9.1.3 Revocation or Status Information Access Fees

BPSCA shall not charge a fee as a condition of making the CRLs available in a repository or otherwise available to Customers.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

9.1.4 Fees for Other Services

BPSCA shall not charge a fee for access to this CP. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification. Creation of derivative works shall be subject to a license agreement with the entity holding the copyright to the document.

9.1.5 Refund Policy

If a Subscriber cancels a Certificate request before the Certificate has been issued, BPSCA will refund as per agreement with subscriber.

After Certificate has been issued and a Subscriber believes that he has grounds to demand refund, he must request such a refund from the BPSCA. Grounds for such a refund would be:

- Technical problems due to an error on BPSCA system, where its Technical Support team has been unable to rectify the situation.
- If the reason for the cancellation or revocation is due to BPSCA breaching a warranty or other material obligation under this Agreement, or the BPSCA CP/CPS, then the Subscriber will be entitled to a full refund of the Certificate fees paid to BPSCA. Alternatively the Subscriber may choose to receive a new Certificate at no charge.

9.2 Financial Responsibility

No financial responsibility shall be accepted for certificates issued under this CP.

9.2.1 Insurance Coverage

No Insurance coverage shall be accepted by BPSCA.

9.2.2 Other Assets

No Stipulation

9.2.3 Insurance or Warranty Coverage for End-Entities

It will be governed as per agreement with subscriber.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

- BPSCA is fully committed to delivering high-quality services to its clients, in strict compliance with the laws of the land and all applicable directives issued by the Controller of Certifying Authorities (CCA).
- BPSCA shall treat all information provided by Subscribers as confidential, especially where the Subscriber has explicitly identified such information as sensitive or confidential in nature.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

- No subscriber information shall be disclosed to any third party without the Subscriber's consent, unless such disclosure is required by a legal obligation, court order, or directive from a competent authority.
- Any **business-related information** shared by BPSCA with its Subscribers—during service delivery or operations—which, if unlawfully disclosed, could impact BPSCA's:
    - Business reputation
    - Competitive position
    - Financial interests
    - Operational security
    - Future opportunities

Shall be treated as Confidential Business Information.

- To safeguard its confidential business information, BPSCA shall obtain a written undertaking from its Subscribers confirming that:
    - They shall not disclose any such information to unauthorized persons.
    - They shall take reasonable measures to secure the information from leaks, misuse, or accidental exposure.
- BPSCA shall also implement internal information classification and handling procedures, access controls, and staff confidentiality agreements to prevent unauthorized disclosure of sensitive or business-critical information.

9.3.2 Information Not within the Scope of Confidential Information

Information released by BPSCA via website, papers, transactions, etc. that are accessible to public without any access prohibition shall be considered as non-confidential business information.

9.3.3 Responsibility to Protect Confidential Information

BPSCA's Subscribers will acknowledge through signing an agreement with it (BPSCA) to keep confidentiality of its business information. Subscribers shall be responsible to handle and secure any paper or document or soft copy or hardware etc. which contain classified or business confidential information from compromise, from the state of being compromised or disclosed to any third party.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

BPSCA shall put necessary control and multi-layer surveillance systems in place to protect privacy of personal information of Subscribers from all kinds of risks of being disclosed. BPSCA shall establish its software system which protects personnel from unauthorized access, ensures storage and processing of personal information in a controlled environment. BPSCA shall also establish requisite procedures and guidelines to ensure physical control of the personal information.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

9.4.2 Information Treated as Private

The following records of Subscribers are considered private:

- CA application records, whether approved or disapproved,
- Certificate Application records
- All information provided by customers to obtain BPSCA services
- All documents and supporting papers submitted by customer to BPSCA
- Transactional records (both full records and the audit trail of transactions),
- BPSCA audit trail records created or retained by BPSCA or a Customer,
- BPSCA audit reports created by Bangla Phone Secure CA or their respective auditors (whether internal or public)

9.4.3 Information not deemed private

Certificate class, status, conditions, duration, etc. of a Subscriber are not considered private. Certificate revocation, suspension records of a Subscriber which are stored at BPSCA's repository and other customer information stored at its repository for purpose of serving service utility and complying with regulatory authority are Subscribers' information which shall be neither private nor confidential.

9.4.4 Responsibility to protect private information

BPSCA shall acknowledge its responsibilities to protect privacy of customer information by co-signing agreement with customer during handing over certificate. BPSCA shall describe all its measures that it will establish to protect any kind of unlawful use of customer information and to prevent them from leaking out to third parties.

9.4.5 Notice and consent to use private information

Subscriber Agreement shall be signed between BPSCA and Subscriber which shall contain a clause to protect each other's confidential/personal information from leaking out to any third party and any use of it will require consent from the other party. For e-Sign certificates, the submission of e-Sign request to e-Sign system will be deemed as such agreement.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

While it is the responsibility of BPSCA to protect private and confidential information of its Subscribers, it may be compelled to, in reasonable situation to release information of a Subscriber in order to comply with the law of land.

9.4.7 Other information disclosure circumstances

No Stipulation.

9.5 Intellectual Property Rights

The BPSCA shall retain exclusive rights to any products or information developed under

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

or pursuant to this CP.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

BPSCA shall warrant to the Subscriber the following assurances:

- Accuracy of Digital Signature Certificate (DSC):
  BPSCA affirms that no errors have been introduced into the Subscriber's DSC due to any failure on its part to exercise reasonable care during the creation process.
- Compliance with Certification Practice Statement (CP):
  The Subscriber's DSC shall conform in all material respects to the provisions outlined in the Certification Practice Statement (CP) of BPSCA.
- Conformance of Revocation and Repository Services:
  BPSCA ensures that its certificate revocation services (e.g., CRL, OCSP) and the use of its repository systems align with the CP of BPSCA in all material aspects.

9.6.2 RA Representations and Warranties

The following responsibilities and liabilities of the BPSCA or RA shall be discharged by the RA on behalf of BPSCA:

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

9.6.3 Subscriber Representations and Warranties

The Subscriber shall warrant to BPSCA and anyone who relies on the Subscriber's DSC that (a) all the information provided by the Subscriber to BPSCA in the Subscriber's DSC Application is accurate; (b) no DSC information provided by the Subscriber (including the Subscriber's e-mail address) infringes the intellectual property rights of any third parties; (c) the DSC Application information provided by the Subscriber (including the Subscriber's email address) has not been and will not be used for any unlawful purpose; (d) the Subscriber has been (since the time of its creation) and will remain the only person possessing the Subscriber's private key except e-Sign certificate cases where one time Private Key will be created in the e-Sign system and no unauthorized person has had or will have access to private key of the Subscriber; (e) the Subscriber has been (since the time of its creation) and will remain the only person possessing any Challenge Phrase),

PIN, software, or hardware mechanism protecting the Subscriber's private key and no unauthorized person has had or will have access to the same; (f) the Subscriber is using the DSC exclusively for authorized and legal purposes consistent with the Subscriber's Agreement; (g) the Subscriber is using the DSC as an end-user Subscriber and not as a certification authority issuing DSCs, certification revocation lists, or otherwise; (h) each digital signature created using the private key of the Subscriber is the Subscriber's digital signature, and the DSC has been accepted and is operational (not expired or revoked) at the time the digital signature is created; (i) the Subscriber manifest assent to the Subscriber's Agreement as a condition of obtaining a DSC. The Subscriber also agrees that the Subscriber will not monitor, interfere with, or reverse engineer the technical implementation of BPSCA, except with the prior written approval from BPSCA, and shall not otherwise intentionally compromise the security of BPSCA.

9.6.4 Relying party representations and warranties

Relying parties will (a) read the procedures published in this document, (b) read and comply with provisions of licensed CA's CP/CPS, (c) verify the purpose of a certificate, it's validity period, key usage, class of certificate and path to trust anchor.

9.6.5 Representations and Warranties of Other Participants

Not applicable.

9.7 Disclaimers of Warranties

THE SUBSCRIBER AGREES THAT THE SUBSCRIBER'S USE OF BPSCA'S SERVICE(S) IS SOLELY AT THE SUBSCRIBER'S OWN RISK. THE SUBSCRIBER AGREES THAT ALL SUCH SERVICES ARE PROVIDED ON AN "AS IS" AND AS AVAILABLE BASIS, EXCEPT AS OTHERWISE NOTED IN THE SUBSCRIBER AGREEMENT. BPSCA EXPRESSLY DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. OTHER THAN THE WARRANTIES AS SET FORTH IN SECTION 6, BPSCA DOES NOT MAKE ANY WARRANTY THAT THE SERVICE WILL MEET THE SUBSCRIBER'S REQUIRMENTS, OR THAT THE SERVICE WILL BE UNINTERRUPTED, TIMELY, SECURE OR ERROR FREE; NOR DOES BPSCA MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF THE SERVICE OR TO THE ACCURACY OR RELIABILITY OF ANY INFORMATION OBTAINED THROUGH BPSCA'S SERVICE. THE SUBSCRIBER UNDERSTAND AND AGREE THAT ANY MATERIAL AND/OR DATA DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF BPSCA'S SERVICES IS DONE AT THE SUBSCRIBER'S OWN DISCRETION AND RISK. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY THE SUBSCRIBER FROM BPSCA OR THROUGH BPSCA'S SERVICES SHALL CREATE ANY WARRANTY NOT EXPRESSLEY MADE HEREIN, THE SUBSCRIBER MAY NOT RELY ON ANY SUCH INFORMATION OR ADVICE. TO THE EXTENT JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, SOME OF THE ABOVE EXCLUSIONS

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

MAY NOT APPLY TO THE SUBSCRIBER. BPSCA IS NOT RESPONSIBLE FOR AND SHALL HAVE NO LIABILITY WITH RESPECT TO ANY PRODUCTS AND/OR SERVICES PURCHASED BY THE SUBSCRIBER FROM A THIRD PARTY.

9.8 Limitations of Liability

9.8.1 THIS CLAUSE 9.8 APPLIES TO LIABILITY UNDER CONTRACT (INCLUDING BREACH OF WARRANTY), TORT (INCLUDING NEGLIGENCE AND/OR STRICT LIABILITY), AND ANY OTHER LEGAL OR EQUITABLE FORM OF CLAIM. IF THE SUBSCRIBER INITIATES ANY CLAIM, ACTION, SUIT, ARBITRATION, OR OTHER PROCEEDING RELATING TO SERVICES PROVIDED UNDER THE SUBSCRIBER AGREEMENT, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, BPSCA'S TOTAL LIABILITY FOR DAMAGES SUSTAINED BY THE SUBSCRIBER AND ANY THIRD PARTY FOR ANY USE OR RELIANCE ON A SPECIFIC DSC SHALL BE LIMITED, IN THE AGGREGATE, TO THE AMOUNTS SET FORTH IN THE APPENDIX A.

THE LIABILITY LIMITATIONS PROVIDED IN THIS CLAUSE 9.8 SHALL BE THE SAME REGARDLESS OF THE NUMBER OF DIGITAL SIGNATURES, TRANSACTIONS, OR CLAIMS RELATED TO SUCH DSC. BPSCA SHALL NOT BE OBLIGATED TO PAY MORE THAN THE TOTAL LIABILITY LIMITATION FOR EACH DSC.

9.8.2 IN NO EVENT SHALL THE BPSCA BE LIABLE FOR ANY PERSONAL INJURY OR ANY INDIRECT, SPECIAL, EXEMPLARY, PUNITIVE, CONSEQUENTIAL OR INCIDENTAL DAMAGES WHATSOEVER, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO THE USE OR INABILITY TO USE THE DSC, HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY, WHETHER IN CONTRACT, TORT, PRODUCT LIABILITY OR OTHERWISE, AND EVEN IF THE BPSCA HAS REASON TO KNOW OR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

9.9 Indemnities

Subscriber Agreements shall contain a clause to indemnify BPSCA of any losses and damages from their conducts. BPSCA's CP requires that subscriber agreements contain a term under which a subscriber is responsible for indemnifying BPSCA for the losses that it sustains arising out of a subscriber's fraudulent misrepresentations on the certificate application under which the BPSCA issued the subscriber an inaccurate certificate. BPSCA will not be liable for any misuse of device or token of the subscriber.

9.10 Terms and Terminations

9.10.1 Terms

The term of the Agreement between the Subscriber and BPSCA shall commence on the date the Digital Certificate/eSign Enrollment Form (i.e., e-KYC) is submitted to BPSCA.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

This Agreement shall automatically terminate upon the earliest occurrence of any of the following conditions:

a) The expiration of the Digital Certificate's operational period as stated within the certificate.
b) The revocation of the Digital Certificate by BPSCA due to valid reasons such as compromise, policy violation, or request by the Subscriber.
c) The rejection of the Digital Certificate enrollment form by BPSCA due to incomplete, invalid, or non-compliant information.
d) Thirty (30) days after BPSCA notifies the Subscriber of a breach of obligations under this Agreement, provided the Subscriber fails to cure the breach within the 30-day notice period

9.10.2 Terminations

This CP takes effect until it is terminated or replaced by a version.

9.10.3 Effect of Termination and Survival

The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

9.11 Individual Notices and Communications with Participants

Notices, demands or requests shall be in writing, and shall be sent to the Subscriber at the address and contact person as declared by Subscriber while signing agreement for digital certificate. Any notices, demands or requests to be communicated by Subscriber shall be sent to BPSCA at the address mentioned in clause 1.5.2 of the CP.

9.12 Amendments

9.12.1 Procedure for Amendment

An amendment of this CP requires approval by the CCA before announcement. The amendment shall be performed under laws, regulation or other related service announcements of BPSCA.

9.12.2 Notification Mechanism and Period

Any revisions or changes made will be binding and effective immediately upon the posting of the changes or revisions to the Repository. Subscriber agrees to periodically review the Repository in order to be aware of any changes. Latest CP is published in the following link:

https://www.digitalsignature.com.bd/Content/Repository/CPS.aspx

9.12.3 Circumstances under which OID must be changed

It will be as per direction from CCA.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

9.13 Dispute Resolution Provisions

Any dispute or difference arising out of the operation or interpretation of the BPSCA Subscriber's Agreement shall be resolved throughout joint discussion of the authorized representatives of the concerned parties. Both the Subscriber and BPSCA shall make efforts in good faith to resolve such dispute via business discussions. However, if the disputes are not resolved within one hundred twenty (120) days after the initial notice then the matter will be referred to competent court of law.

9.13.1 Disputes between Issuer and Subscriber

Unless the provision for dispute resolution under the ICT Act is invoked, any dispute based on the contents of this CP, between CA and one of its customers who has availed specific services will be resolved according to provisions in the applicable agreement between the parties. Any dispute based on the contents of this CP, between/among CAs shall be resolved by CCA.

9.13.2 Disputes between Issuer and Relying Parties

The same procedure as stated in section 9.13.1.

9.14 Governing Law

This CP and BPSCA Subscriber's Agreement and any disputes relating to the services provided hereunder shall be governed and interpreted according to the laws of Bangladesh.

9.15 Compliance with Applicable Law

The relevant Subscribers/End User shall be obliged to comply with all applicable laws, rules and regulations applicable to them. If the relevant Subscribers/End User fails to comply with any applicable laws, rules and regulations then the responsibility will be upon the Subscribers/End User. If Bangla Phone is held responsible due to the Subscribers/End Users' failure to comply with the applicable laws, rules and regulations then the Subscribers/End Users shall indemnify Bangla Phone from all direct, indirect, remote and consequential costs, expenses, actions, claims, proceedings etc. arising out of or in connection with the non-compliance.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CP and all documents referred to herein contain the entire and exclusive agreement and understanding between the parties on the subject matter of the Agreement. This guideline supersedes all prior agreements, arrangements, understandings, communications, representations, and arrangements relating thereto. Except as may be expressly included in this CP, no oral or written representation, agreement,

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd

communication, understanding, or promise related to the subject matter is given or implied from anything previously said or written in negotiations between the parties.

9.16.2 Assignment

Except where specified by other contracts, no party may assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of CCA.

9.16.3 Severability

If any term or provision or part of the Subscriber Agreement and/or any document contemplated herein is declared illegal or unenforceable, in whole or part, it will be enforced to the maximum extent permissible, and the remainder of the Subscriber Agreement will remain in full force and effect to the fullest extent permitted by law and the parties hereto agree to replace the illegal or unenforceable provisions with valid provisions which are as close as possible to the Parties' original intentions in their respective meaning, purpose, and commercial effect.

9.16.4 Enforcement

It should be determined that if any section of this CP is illegal, unenforceable or void then any offending words will be deleted to the extent necessary to make it legal and enforceable while preserving its intent.

9.16.5 Force Majeure

BPSCA shall not be liable for any failure or delay in its performance under this CP due to causes that are beyond their reasonable control, including, but not limited to, an act of God, act of civil or military authority, fire, epidemic, flood, earthquake, riot, war, and failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action.

9.17 Other Provisions

Not applicable.

Bangla Phone Secure CA
House 03, Road 23/A, Gulshan-1, Dhaka-1212. Tel: 9860352, 9888746, Email: bpsca@banglaphone.net.bd