DohatecCA
Certifying Authority

Dohatec New Media

Dohatec-CA

Certificate Practice Statement

In support of PUBLIC KEY INFRASTRUCTURE SERVICES

November 2020

Version 1.3.0

THIS DOCUMENT NAMELY THE CERTIFICATE PRACTICE STATEMENT HAS BEEN DRAFTED BASED ON THE RFC-3647: INTERNET X.509 PUBLIC KEY INFRASTRUCTURE CERTIFICATE POLICY AND CERTIFICATION PRACTICES FRAMEWORK AND THE CPS GUIDELINES TO OPERATE AS A CERTIFYING AUTHORITY UNDER THE ICT ACT, 2006 (AMENDED IN 2013) AND IT (CA) RULES 2010.

WHEREVER THE PHRASE "DOHATEC NEW MEDIA" OR THE ABBREVIATION "DOHATEC" APPEARS IN THIS DOCUMENT, INCLUDING WITHIN THE ABBREVIATION "DOHATEC-CA", IT SHALL BE TAKEN TO MEAN "DOHATEC NEW MEDIA".

WARNING

DIGITAL CERTIFICATION SERVICES PROVIDED BY DOHATEC-CERTIFYING AUTHORITY ARE SUBJECT TO VARIOUS BANGLADESH LAWS AND JURISDICTION OF COURTS, TRIBUNALS AND AUTHORITIES IN BANGLADESH.

THISCERTIFICATE PRACTICE STATEMENT SHALL BE READ WITH ANY STATEMENT WITH SUCH PARTICULARS AS THE CONTROLLER OF CERTIFICATION AUTHORITIES (CCA), BANGLADESH MAY SPECIFY BY REGULATION IN EXERCISE OF HIS POWERS UNDER THE INFORMATION AND COMMUNICATION TECHNOLOGY ACT, 2006 (Amended in 2013).

WRONG USE OF THE DIGITAL CERTIFICATES OR ITS SERVICES SHALL BE LIABLE TO BE PROCEEDED WITH CONSEQUENCES CIVIL AND CRIMINAL AND SHALL BE SUBJECTED TO PENALTIES AND PUNISHMENT.

ACRONYMS

CA	Certifying Authority
CCA	Controller of Certifying Authorities
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CRMF	Certificate Request Message Format
CUG	Common User Group
DN	Distinguished Name
e-mail	Electronic Mail
FIPS	Federal Information Processing Standard
GMT	Greenwich Mean Time
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
ICT	Information and Communication Technology
IPSec	Internet Protocol Security
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
OID	Object Identifier
OU	Organization Unit
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKCS#10	Certification Request Syntax Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comment
RSA	The Rivest Shamir Adleman Cryptographic Algorithm
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer

SUB-CA	Subordinate Certifying Authority
URL	Uniform Resource Locator
WAN	Wide Area Network
WWW	World Wide Web
X.509	The ITU-T standard for Certificates and CRLs

IMPORTANT CPS RIGHTS AND OBLIGATIONS

1. This Certificate Practice Statement controls the provision and use of Dohatec New Media – Certifying Authority's (Dohatec-CA) digital certification services – including Digital Certificate application, application validation, Digital Certificate issuance, acceptance, use, suspension, activation and revocation of a Digital Certificate.

2. Dohatec-CA assumes that the applicant will make himself/herself aware of the subscriber representations and warranties, section 9.6.3 of this CPS prior to applying for a Digital Certificate.

3. Dohatec-CA offers different classes and types of Digital Certificates under the Dohatec-CA Trust Network. The applicants must decide which class and type of Digital Certificates suit their need.

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

5. The applicant must accept a Digital Certificate before communicating it to others, or otherwise invoking use of it. By accepting a Digital Certificate, the applicant makes certain important representations as described in subscriber representations and warranties, section 9.6.3 of this CPS.

For more information or to provide feedback:

- Visit the Dohatec-CA Trust Portal at http://www.dohatec-ca.com.bd or
- Contact Dohatec-CA Administrator at helpdesk@dohatec-ca.com.bd

Revision History

Version	Date	Section affected	Change Description	Author	Review	Approved
V 1.3.0	11-11-2020	Entire Document	Background Check Procedure, Identification and Authentication, Contact person and Publication	Nuzhat Atiqua	Farhana Haque	Luna Shamsuddoha
V1.2.2	23-01-2016	Section 2.1 and section 1.5.2	Phone number changed	Nuzhat Atiqua	Farhana Haque	Luna Shamsuddoha
V1.2.2	30-03-2014	Section 2.1 and section 1.5.2, all ICT ACT, 2006 are replaced by ICT ACT, 2006 (AMENDED IN 2013)	Minor Change	Farhana Haque	Jinat Rehana	Luna Shamsuddoha
V1.2.1	18-03-2014	Section 9.1.1 Certificate issuance or renewal fees	Minor Change	Jinat Rehana	Kashif Nizam Khan	Luna Shamsuddoha
V1.2.0	14-11-2013	Section 1.2 Document name and Identification, section 9.12.3 Circumstances under which OID must be changed	Minor Change	Jinat Rehana	Kashif Nizam Khan	Luna Shamsuddoha
V1.0.0	10-02-2012	Baseline	Baseline	Jinat Rehana	Kashif Nizam Khan	Luna Shamsuddoha

Dohatec New Media 43, Purana Paltan Line, Dhaka-1000 Dohatec

Table of Contents

Dohatec New Media ★ 43 Purana Paltan Line, Dhaka-1000 ★ Dohatec

1. Introduction

This Certificate Practice Statement (CPS) for Dohatec Certifying Authority (CA) aims at describing the practices employed by the CA to cater to Digital Certificate issuance, Certificate Life Cycle Management including Suspension, Activation, Revocation and Re-Issuance of Digital Certificates, its operational procedures and members of its Trust Network. The Dohatec Certifying Authority, Registration Authorities and the Subordinate Certifying Authorities under the CA form the Trust Network.

This CPS is drafted as per RFC 3647 and takes into consideration the Bangladesh Information and Communication Technology Act 2006 (Amended in 2013), IT (CA) Rules 2010, CPS Guidelines to Operate as a CA and the Interoperability Guidelines, e-Sign Guideline for Certifying Authorities 2020 – Published by the Controller of Certifying Authorities, Bangladesh.

1.1 Overview

Dohatec–CA operates as a Certifying Authority within Bangladesh and issues Digital Certificates to end entities who can be Individuals, Organizations or Machines/Devices. Dohatec–CA operates through its members of the Trust Network.

This CPS gives an understanding of the members of the Dohatec–CA Trust Network, their roles and responsibilities, obligations while documenting the basis for issuing, revoking, suspending and activating Digital Certificates issued by the CA.

This CPS also aims to legally bind the various stake holders including the Dohatec–CA along with the members of its Trust Network, the holders of the Digital Certificates and the Relying Parties who are involved in verifying the Digital Signatures created using the Digital Certificates.

This CPS is a public document intended for the perusal of the various stake holders in the PKI system.

1.2 Document name and Identification

This CPS is called the Dohatec–Certifying Authority Certification Practice Statement.

OID assigned to this CPS is 2.16.50.1.7.1

1.3 PKI Participants

The following is a diagrammatic representation of the various members in the Dohatec-CA's trust chain.

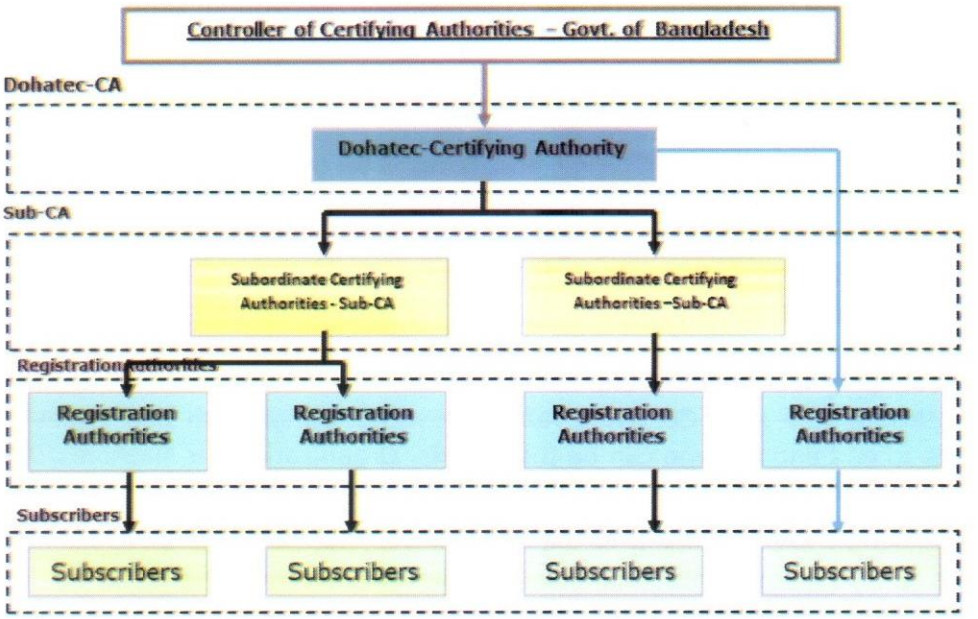

Figure 1 - Dohatec - CA TRUST NETWORK – TRUST MODEL

1.3.1 Certification Authorities

The Dohatec–CA will issue Digital Certificates to end entities or subscribers who request for Digital Certificates. The Digital Certificates thus issued legally binds the subscriber's Public Key (hence the Private Key) with his/her Identity.

The CA also manages Suspension, Activation, Revocation and/or Re-issuance of Digital Certificates which constitutes the Certificate Life Cycle. Apart from this, the CA also publishes the Certificate Revocation List (CRL) which contains the list of certificates that have been revoked/suspended by the CA. Such Certificates should not be used / trusted by the relying applications.

1.3.2 Registration Authorities

A Registration Authority (RA) is an entity appointed by the Dohatec–CA under its Trust Network that collects and processes Applicant's application form (see Section 12 – Application Forms of this CPS), An RA receives the applications for the Digital Certificate from the Applicant and verifies the details contained in the application and cross checks the details against the submitted documents as required by the IT (CA) Rules 2010.On successful verification, the request is forwarded to the Dohatec–CA recommending generation of a Digital Certificate for the verified Applicant.

The RA Administrator and RA Operator (optional) shall be provided Class 3 Digital Certificates issued by Dohatec–CA and all the approvals shall be digitally signed by the RA Administrator and RA Operator before forwarding to the Dohatec–CA. For life cycle management, these certificates will be treated on par with Subscriber certificates.

1.3.3 Subordinate Certifying Authority (Sub-CA)

Certifying authority (CA) can create a "Subordinate Certifying Authority" (Sub-CA). The Sub-CA will be part of the same legal entity as the CA. Sub-CA is created under Dohatec-CA Trust Network and operated by Dohatec-CA for a partner who is authorized by Dohatec-CA to verify the Applicants. The set of Applicants can be affiliated users of the Sub-CA or can be employees of the organization under the Sub-CA forming a Closed User Group (CUG). Upon successful verification of the Applicant, the Sub-CA can request the Dohatec CA to generate a Digital Certificate. The Dohatec-CA generates the Digital Certificate for the respective Applicants under the Sub-CA in accordance with the Information and Communication Technology Act, 2006 (Amended in 2013), IT (CA) Rules 2010 and Interoperability Guidelines published by CCA, Bangladesh.

Dohatec-CA will issue a special Digital Certificate for each Sub-CA. This Digital Certificate shall contain "Certifying Authority Name" sub-CA for "Branding Name" {Generation qualifier} {re-issuance number} whose Private Key shall be under the control of Dohatec-CA, and Dohatec-CA shall issue Digital Certificates to subscribers who are duly authorized by the partner, and such Digital Certificates shall contain the name "Certifying Authority Name" sub-CA for "Branding Name" {Generation qualifier} {re-issuance number} in the issuer field.

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

1.3.4 Subscribers / Applicants

The Subscribers / Applicants are the End Entities who ask for Digital Certificates from CA and make use of them. The Subscribers raise request for Digital Certificates by filling in the application form and submitting the associated documentation for verification by the RAs.

End Entities requesting for a Digital Certificate can be

1. Individuals
2. Individuals representing Organizations
3. Devices / machines

1.3.5 Relying parties

Relying parties are Individuals and organizations doing business with subscribers who have received their certificates from Dohatec–CA issuing certificates to the public. The Relying Parties receive the Digital Signatures which are signed using the Digital Certificates issued by the Dohatec–CA and have to verify these Digital Signatures to authenticate the Subscriber.

1.3.6 Other participants

None

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The Digital Certificates issued under the Dohatec–CA Trust Network are used for lawful purposes as further described in the Section4.5Key Pair and Certificate Usage in this CPS. Use of issued Digital Signature Certificates under the Dohatec–CA Trust Network for other than usage mentioned in this CPS is prohibited. The Dohatec–CA either by its own judgment, or guided by the advice of a concerned RA, reserves the rights to revoke Digital Certificates of Subscriber, entity, or organization for indulging in illegal use or misuse of Digital Signature Certificates, among other reasons.

1.4.2 Prohibited certificate uses

The Digital Certificates issued under this CPS are not designed, intended or authorized for use or resale as control equipment in hazardous circumstances or for users requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, etc. where failure could lead directly to death, personal injury or severe environmental damage. Also, Class 1 Certificates shall not be used as proof of identity or as support of non-repudiation of identity or authority. Client Certificates are intended for client applications and shall not be used as server or organizational Certificates.

CA Certificates may not be used for any functions except CA functions. In addition, Subscriber Certificates shall not be used as CA Certificates.

1.5 Policy administration

1.5.1 Organization administering the document

This CPS will be administered by Dohatec New Media which is the Dohatec–CA. This CPS will be revised as and when there are changes to the operations or operating procedures. The Subscribers, RAs and the Relying Parties will be appropriately informed about the changes and the CPS will be published on the Dohatec–CA's web site.

1.5.2 Contact person

The Dohatec New Media – Certifying Authority can be contacted at the following address:

Dohatec New Media-Certifying Authority
Farhana Haque, Dohatec CA
Mobile: +880-1678625350
Doha House,
43, Purana Paltan Line, Dhaka-1000, Bangladesh.
Phone: 880-2-9341003, 9348119
Fax: 880-2-9569326
Web: http://www.dohatec-ca.com.bd
Email: helpdesk@dohatec-ca.com.bd

1.5.3 Person determining CPS suitability for the policy

The Certifying Authority of Dohatec-CA will represent Dohatec-CA in determining CPS suitability for the policy.

1.5.4 CPS approval procedures

Dohatec-CA CPS shall be submitted to CCA, Bangladesh for approval before commencing CA operations. The approved CPS shall be made available in Dohatec-CA Trust Portal.

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

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

Any changes to the CPS arising due to changes in policies, procedures or any updates to the Act or Guidelines defined by CCA, Bangladesh shall be approved by Dohatec-CA Management. The updated CPS will be shared with CCA for approval. On obtaining the approval, the CPS will be published on Dohatec–CA website. The Dohatec-CA management must approve the proposed changes.

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Publication

Users can obtain the Dohatec–CA CPS in the following formats:

- In electronic form:

http://www.dohatec-ca.com.bd

- In paper form from:

Dohatec New Media-Certifying Authority
Doha House,
43, Purana Paltan Line,
Dhaka-1000
Bangladesh.
Phone: 880-2-9341003, 9348119
Fax: 880-2-9569326
Web: http://www.dohatec-ca.com.bd
Email: helpdesk@dohatec-ca.com.bd

2.2 Repositories

The Dohatec-CA maintains a web portal to allow end users to login and place certificate requests and manage their life cycle. The CPS is published on this portal. Apart from this Dohatec–CA also maintains an LDAP where the Digital Certificates issued under the Dohatec–CA trust network are published in Dohatec–CA Trust Portal http://www.dohatec-ca.com.bd

The Public Key Certificate Information issued under the Dohatec–CA trust network, Certificate Revocation Lists (CRL) are published in an LDAP maintained by Dohatec–CA and is also sent to the CCA periodically for publication in the National Repository.

The following information is published in the Dohatec-CA repository

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

2.3 Publication of certificate information

Every Public Key Certificate that has been issued by the Dohatec–CA is published in a LDAP. This LDAP is maintained by the Dohatec–CA and allows people to query and download public key certificates based on the Email ID, or Common Name of the Subscriber.

2.4 Time or frequency of publication

Digital Certificates are published as and when they are issued. CRLs are generated upon every revocation, suspension or activation. When there is no revocation, suspension or activation requests, CRLs are generated once a week as long as the CA Certificate is valid. The CRLs are published as soon as they are generated.

2.5 Access controls on repositories

The Dohatec–CA repositories are maintained by Dohatec–CA and are accessible to authorized personnel. The Dohatec–CA repositories are the source for the most current CRL and other information regarding Digital Certificates issued under the Dohatec–CA Trust Network. Dohatec – CA maintains a list of authorized personnel who are allowed to update / modify the repository. All others including subscribers and relying parties are only allowed to search/query the repository.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The names in the Digital Certificates issued under the Dohatec–CA Trust Network shall comply with the X.500 naming conventions as specified in Section 5.3.1 Root CA Certificate Profile of Interoperability Guidelines published by CCA, Bangladesh. These Digital Certificates shall use Distinguished Names (DN) to provide the identities to Subscribers, the Dohatec–CA and the Partner for whom Sub-CA has been created under the Dohatec–CA Trust Network. The Digital Certificates contain the following types of names.

- Common Name (CN), which is the unique name of the Subscriber. (In case of SSL Certificates, the Common Name (CN) shall be the fully qualified hostname or path used in the DNS of the World Wide Web server on which the Applicant is intending to install the SSL Certificate)
- Organization (O).
- Organizational Unit (OU), which is used to distinguish various organizational groups within the same organization.
- State or Province (ST), which is an identifier of the state or the province to which the Subscriber belongs.
- Country(C), which is the identifier for the country to which the Subscriber belongs.
- Serial Number, which is the SHA1 hash of the ID (National Identity (NID)/ Passport Number (PPN)/ Tax Identification Number (TIN)/Birth Registration Number (BRN)) of the Subscriber.
- Postal Code, which is the postal code of the Subscriber residential or office address.

3.1.2 Need for names to be meaningful

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

3.1.3 Anonymity or Pseudonymity of subscribers

Subscriber names cannot be anonymous or pseudonyms. The name provided in the Common Name field should be verifiable against the identity proofs

3.1.4 Rules of interpreting various name forms

The names will be interpreted as specified in the section 3.1.1 of this CPS. Other terms, numbers, characters and letters may be appended to existing names to ensure the uniqueness of each name in case of Sub-CA. The naming convention for Sub-CAs will follow the Interoperability Guidelines specified by CCA, Bangladesh.

3.1.5 Uniqueness of names

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

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

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The Subscriber / Applicant of a Digital Certificate from Dohatec-CA will produce supporting documents along with the filled in application form to the RA. The request is standards based PKCS#10 / CRMF form. The RA verifies the request details against the application form and the submitted Identity/Address Proofs.

The RA will forward the request along with the digitally signed approval to the Dohatec-CA only after establishing the proof of possession of the private key of the Subscriber.

3.2.2 Authentication of organization identity

The RAs will be responsible for verifying the identity of the organization. Organization requesting for a Digital Certificate has to identify the appropriate representative of organization, such as - Head of Department, Finance Head, General Manger etc, depending on the business requirement for Digital Certificates.

The RA operating under the Dohatec-CA Trust Network will perform appropriate verification of an organization as well as the bona fides of the representative of the organization, based on the information given in the application form.

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

- NID
- Passport
- Trade License
- Partnership Deed
- TIN/ eTIN
- Birth Registration
- Certificate of Incorporation
- Memorandum of Understanding and Articles of Association

- Trade Body Membership as applicable for
  - proprietary firm
  - partnership firm
  - private limited company
  - public limited company
- professionals:
  - NGO Bureau Registration
  - Registration Under Societies Act
  - Registration Under Trust Act
  - Registration Under Waqf Act
  - Government Order

In addition, proof that the person representing the organization with due authorization from the organization has to be submitted. Further the identity and address proofs of company representative requesting Digital Certificate should be submitted to the RA.

Note: For Web server (SSL) certificates, in addition to the above list of acceptable documents, the domain registration form is also required.

For System or Device Certificates, a request for a certificate should contain any electronically verifiable information such as IP Address of the system, MAC Address, or CPU Serial number. A proof that the particular system or device belongs to an organization on a company letter head has to be submitted.

The RA upon receiving the request for a System Certificate or SSL Certificate verifies the Subject DN details in the request against the submitted documentation and proofs.

3.2.3 Authentication of individual identity

The RA operating under the Dohatec-CA Trust Network shall perform appropriate verification of an individual entity based on the information provided in the application form. The RA shall perform the verification depending on the Digital Certificate classes' type as specified in the CPS. This verification will take the form of checking the validity and authenticity of details. The following documents are accepted by Dohatec-CA:

Photo ID: Passport, NID, Driving License, Employer ID.
Address Proof: Telephone Bill, Electricity Bill, Gas Bill, Bank statement Attested by the bank.

For class 3 applications, a physical visit of the applicant to the RA may be required.

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

Following are the validations that are performed based on the above list of documents.

- Primary ID: Passport, NID, Driving License, Employer ID, Social Security Number, Aadhar Number.
- Secondary ID: Birth Certificate, TIN/ eTIN.
- Address Proof: Utility Bills, Rent Receipt, Ownership Documents, Ward Commissioner Certification.
- Attestation of copy: Following is the list of acceptable attesters: Gazetted Officer, Bank Manager, Public University Teachers, Private University VC/Registrar, College Principal, City Mayor, and Municipality Chairman.

3.2.4 Non-verified subscriber information

Entries such as telephone number, mobile number, educational certificates, etc, which are not mandatory for identification of the Subscriber or End Entity is not verified. This information is also not part of the generated Digital Certificate issued by Dohatec–CA.

3.2.5 Validation of authority

A Subscriber requesting for a Digital Certificate on behalf of the organization must carry an authorized document from the organization such as the "Letter of Authority", showing that he is a bona fide employee of that company and is authorized to represent the organization for procuring a Digital Certificate.

3.2.6 Criteria for interoperation

The Digital Certificates issued under Dohatec-CA Trust Network will be in accordance with the Interoperability Guidelines published by Bangladesh CCA.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Subscribers will be sent a notification email 30 days prior to the expiry of Digital Certificate. The Subscriber, will apply for a new Digital Certificate by re-generating his/her Public/Private key pair in a secure medium and the Certificate Request in PKCS#10 / CRMF format and is submitted to the RA. The details already filled-in by the Subscriber will be displayed and the subscriber is allowed to modify only details pertaining to the supporting documents as specified in Section 3.2.3. Every modification has to be substantiated with relevant supporting documents. Any changes to the details in the Digital Certificate will be treated as a new request and will have to follow the initial identity validation process as mentioned in Section 3.2.

The RA upon successful verification of the Certificate Request details against the details filled-in by the Subscriber and comparing them with the submitted documents will forward the request for further processing by the CA.

3.3.2 Identification and authentication for re-key after revocation

Upon revocation, the Subscriber will apply for a new Digital Certificate by re-generating his/her Public/Private key pair in a secure medium and the Certificate Request in PKCS#10 / CRMF format and submits it electronically to the RA. This request will be treated as a new Certificate Request and the Applicant/Subscriber has to follow the same process as he/she would do for a new Certificate as mentioned in Section 3.2 Initial Identity Validation.

The RA upon successful verification of the Certificate Request details against the details filled-in by the Subscriber and comparing them with the submitted documents will forward the request for further processing by the CA.

3.4 Identification and authentication for revocation request

A Subscriber can ask for revocation of his/her certificate for reasons such as lost token or Private Key compromise. The subscriber can log-in to the Dohatec–CA portal and request for revocation of a particular certificate or approach the RA for revoking the certificate.

When the Subscriber places the certificate revocation request, the RA verifies the request and upon proper subscriber verification approves the revocation request and transfers the request electronically for further processing by the CA.

In case of lost tokens or keys, the Subscriber approaches the RA to place a revocation request on his/her behalf. The RA upon successful subscriber verification places a revocation request for the said certificate on behalf of the Subscriber. The CA further processes the request and revokes the certificate.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

To obtain the certificate from the Dohatec–CA Trust Network, the Subscriber/Applicant has to follow the initial identity validation process specified in the Section 3.2 of this CPS. The RAs operating under the Dohatec–CA Trust Network will perform verification of the information provided by the applicant to establish their identity.

4.1.1 Who can submit a certificate application

The application for obtaining a Digital Certificate can be submitted by individuals/ private subscribers, business personnel and individuals representing organizations. The application for a certificate can also be raised for devices or machines such as (SSL, IPSec, etc..,). In case of device certificates the person responsible for maintaining the device will submit the certificate application.

4.1.2 Enrollment process and responsibilities

Dohatec-CA supports 4 classes of certificates. The class of certificate determines the level of assurance that the certificate carries. The level of assurance is provided based on the level of validations / verifications of the subscriber applying for the certificate. Dohatec-CA supports the following classes of certificates.

4.1.2.1 Certificate Classes

Class 0 Certificate: Class 0 Certificates are demo certificates. This Class of Certificates will be issued through the demo setup of Dohatec-CA and may be used for demo purposes only.

Class 1 Certificate: - Class 1 Certificate will be issued to individuals / business and organizations. Class 1 Certificate requires that the Subscriber name and email ID form an unambiguous Subject name in the Dohatec-CA repository.

The level of assurance associated with this class of certificate is the lowest. Other than the email Id and Subscriber name combination, no subscriber details are verified by the CA to issue these Certificates.

Class1 certificates are not intended for commercial use where there is a stringent need to identify or authenticate a user, such as in financial transactions, user login or e-Filing. These certificates can be used to secure emails or data which are meant solely for personal use.

Dohatec-CA does not make any representation and does not give any warranties regarding the identity of the subscriber or any consequences, which the Subscribers and the relying parties may face or potentially face by using the Class 1 Digital Certificate obtained from the Dohatec-CA Trust Network.

Enrollment process & Obtaining a Class 1 Certificate

- A Class 1 Digital Certificate application can only be verified by a RA.
- The Subscriber logs in to the Dohatec-CA Trust Portal to self-register and generates the Digital Certificate request (and key pair) preferably in a secure medium.
- User fills the online request form.
- Email ID of the Subscriber is the only verification and the verification is achieved by sending emails regarding the certificate request.
- RA approves the request and forwards it to the CA to issue a Digital Certificate.
- Authentication Code which is a pre-requisite to download the certificate is sent to the same email id that was used during enrollment by the Subscriber.
- CA issues the Digital Certificate. This can only be downloaded by presenting the authentication pin

Class 2 Certificates: - Class 2 Certificate will be issued to Individuals / Businesses and Organization representatives upon recommendation from the RA's under the Dohatec-CA's Trust Network. It is the responsibility of the RAs to appropriately verify the Subscriber, as described in Section 3.2 of this CPS, before recommending the Dohatec-CA to issue Digital Certificate.

Class 2 Certificates have a higher level of assurance compared to Class 1 Certificates, as the validation of the Subscriber is carried as per the defined process. Hence the Class 2 Certificates can be used in all applications requiring the use of legally valid Digital certificate. Further it is recommended that public/private key pair corresponding to Class 2 Certificates should be generated and stored in tamper proof cryptographic devices such as FIPS 140-2 Level 2 supported smart cards or tokens. This provides higher assurance when compared to Class 1 Certificates.

Enrollment Process & Obtaining a Class 2 Certificate

Class 2 Digital Certificate applications will be verified by RAs as stated below.

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

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

When a Subscriber wishes to obtain a Digital Certificate:

- The Subscriber will approach the RA with his details
- The RA will verify (using the policies described earlier) eligibility and authenticate the applicant details
- The Subscriber registers and generates the Digital Certificate request (key pair) in a secured manner
- The RA operator/administrator at the concerned Dohatec RA will then verify the details submitted
- If verified successfully the RA Administrator would recommend the Digital Certificate request for generation
- Dohatec-CA issues the Digital Certificate based upon the request approved by RA

The details given in the application form are verified against supplied documentary evidence. The documents to be verified depends on the type of user whether individual, organization, etc.

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

Class 3 Certificates: - Class 3 Certificates provide the highest level of assurance as these certificates are issued only after the RA/Dohatec-CA verifies the Subscriber Identity in various ways. Apart from the verification procedures mentioned in Section 3.2 of this CPS, verification process may involve the physical presence of the Subscriber, if required, at the Dohatec-CA office. These validation procedures provide stronger assurances of a Subscriber's identity than Class 2 Digital Certificates.

The RA verifies the details of the Subscriber and only after ascertaining that the details are correct will recommend the Dohatec-CA to process the certificate request.

The Private keys of the Class 3 Certificates should be generated and stored in tamper proof cryptographic devices such as FIPS 140-2 Level 2 supported smart cards or tokens.

Class 3 Certificates have the highest level of assurance and hence can be used where ever there is a need for legally valid digital certificates such as e-commerce transactions, e-filing etc.

Enrollment Process & Obtaining a Class 3 Certificate

- The Subscriber logs in to the Dohatec-CA Trust Portal to self-register and generates the Digital Certificate request (and key pair) preferably in a secure medium
- The Subscriber submits all supporting documents to the RA.
- The RA verifies the details in the application against the document proofs submitted by the Subscriber as per Section 3.2 of this CPS.
- The Subscriber may be called to personally visit the Dohatec-CA Office for verification.
- Based on the above details submitted the RA forwards the request to CA.
- CA issues a Digital Certificate based on RA recommendation.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The Section 3.2 of this CPS describes the Subscriber Identification and Authentication process.

4.2.2 Approval or rejection of certificate applications

Applications for digital certificates are verified as per the mentioned validation processes. Applications can be rejected for the following reasons:

- For Class 2 and 3 types of Certificates, if any of the mandatory information (as specified in Section 3.2 of this CPS) is not verifiable, this information is deemed to be missing and the application will be rejected.
- Incomplete or Incorrect application forms
- In the event the Subscriber does not indicate acceptance of obligations as per CPS or inaccurate information furnished by the Subscriber.

4.2.3 Time to process certificate applications

A request for Digital Certificate will be processed and the certificate will be issued to the Applicants within 3 business days after a duly verified certificate request is received from RA. The Applicant can know the status of the certificate request from the Dohatec-CA Trust Portal.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

The Dohatec–CA processes the Digital Certificate Requests and approves their issuance only after the RAs approve the requests.

For Class 0 Certificates: - As Class 0 Certificates are issued from a demo system, Dohatec–CA does not play any part in certificate issuance. Dohatec Team responsible for maintaining the Demo CA System will issue the certificate.

For Class 1 Certificates: - The Dohatec–CA simply verifies the RA's signatures and issues the certificate. CA does not perform any additional validation / verifications.

For Class 2 Certificates: - The Dohatec–CA apart from verifying the RA's Signature also verifies the subscriber's details against submitted supporting documents. In case of any mismatch of data, the certificate request is rejected.

For Class 3 Certificates: - The RA verifies the Subscriber details and the supporting documents. The Subscriber details are verified over phone or the Subscriber may be asked to appear personally at the Dohatec–CA office. Once the verification is successful the RA recommends the generation of Certificate.

The CA verifies the RA Signatures and also verifies the subscriber's details against submitted supporting documents and approves the request based on the result of verification. The Subscriber may be called to personally visit the Dohatec–CA Office for verification.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Subscribers or Applicants requesting for a Digital Certificate from Dohatec–CA or the Partner for whom the Sub-CA has been created will be informed by an email upon certificate generation.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

The certificate will be considered as accepted by the subscriber when the subscriber downloads the certificate. Once the certificate is generated, an email will be sent to the Subscriber with the authentication code. The Subscriber can log in to the Dohatec-CA Trust Portal, check the details and can download the certificate by providing the authentication code. Subscriber entering the authentication code and downloading the certificate is treated as certificate acceptance. There is no time limit within which certificates have to be downloaded for certificates other than the Encryption Certificate. Encryption Certificates shall be made available for a period of 21 days within which the subscriber needs to download and accept the certificate. All the accepted Digital Certificates will be published to the repository.

4.4.2 Publication of the certificate by the CA

The Digital Certificates accepted by the subscribers will be published in the Dohatec–CA repository by the CA

4.4.3 Notification of certificate issuance by the CA to other entities

Subscribers are notified through email once their Digital Certificates are issued. No other entities are notified.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

Dohatec–CA supports the following types of Digital Certificates with the corresponding Key Usages

4.5.1.1 Signing Certificate

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

4.5.1.2 Encryption Certificate

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

Subscribers requesting for Encryption Certificates from Dohatec–CA should have already procured a Signing certificate from Dohatec–CA.

4.5.1.3 SSL / Web Server Certificates

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

4.5.2 Relying party public key and certificate usage

The Relying party shall be obliged to the following:

- Any relying party seeking to rely upon a Digital Certificate is solely responsible for deciding whether or not to rely upon the said Digital Certificate.
- In the case of verifying a Digital signature, the relying party should check that the Digital Certificate was valid and the Digital Certificate status was not revoked at the time that the Digital Signature in question was affixed.
- In the case of encrypting data for a subscriber, the relying party should check that the Digital Certificate is valid and the Certificate status is not revoked at the time that the encryption is carried out.
- Using the Digital Certificate only for purposes that are specified in this CPS and avoiding unauthorized, illegal uses of the Digital Certificate.
- Verifying the Digital Certificate and its chain of trust before using it for the authorized purposes.
- Verifying the Signature as specified in this CPS before trusting the Digital Certificate.
- May rely on a valid Digital Certificate issued under the Dohatec–CA Trust Network and under this CPS for the purpose of verifying the Digital Signature only if:
    - The relying party acknowledges the obligation under this CPS.
    - The relying party acknowledges the limitation in liability of the Dohatec–CA or RA as well as any warranty disclaimer that may apply.
- Additional obligations as mentioned in the Relying Party agreement.

4.6 Certificate renewal

Certificate renewal is always treated as re-key and new Digital Certificates are issued as per the Rule 27 (2) of the IT (CA) Rules 2010.

4.7 Certificate re-key

4.7.1 Circumstances for Certificate Re-key

The Subscribers of Dohatec–CA who intends to continue availing the Digital Certificate Service may return for a new Certificate by applying for a Re-Key. Dohatec–CA issues a new certificate to the Subscriber upon receiving such a request before the expiry of his original Digital Certificate.

The corresponding RA may put reasonable efforts to inform the subscriber in advance about the expiration of the subscriber's certificate.

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

4.7.2 Who may request certification of new public key

The Subscriber needs to generate a new private-public key pair preferably on a trustworthy medium and complete the initial identity validation process once again as specified in the section 3.2 of this CPS.

4.7.3 Processing certificate re-keying requests

The processing of certificate re-key requests will be same as original requests as specified in Section 4.2 Certificate Application Processing.

4.7.4 Notification of new certificate issuance to subscriber

Subscribers or Applicants requesting for a Digital Certificate from Dohatec-CA or the Partner for whom the Sub-CA has been created will be informed by an email upon certificate generation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

The acceptance of re-keyed certificate will be in the same lines as mentioned in Section 4.4.1 Conduct constituting certificate acceptance.

4.7.6 Publication of a re-keyed certificate by the CA

The Digital Certificates accepted by the subscribers will be published in the Dohatec-CA repository by the CA.

4.7.7 Notification of certificate issuance by the CA to other entities

Subscribers are notified through email once their Digital Certificates are issued. No other entities are notified.

4.8 Certificate revocation

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

The RA which has processed the application in respect of any Digital Certificate has the right to recommend the revocation of such Digital Certificate based on conditions specified in this CPS. Wherever reasonably possible this will be done with reasonable notice to the affected subscribers. The revoked certificates are added to the Dohatec-CA CRL and the same is published and the Subscribers shall be notified via email. A revoked Digital Certificate shall not be used again by the subscriber.

It is the subscriber's obligation to notify the RA with a request to revoke a subscriber's Digital Certificate on conditions as specified in this CPS. Upon receipt of such a request, the RA verifies to confirm the revocation request. This verified request is subsequently

transmitted to the Dohatec-CA as applicable, where the revocation request is processed. The RA may also initiate a revocation request without a request from the subscriber or participant if the situation warrants it. The Dohatec-CA itself may also initiate a revocation request without a request from a subscriber, RA if the situation warrants it.

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

The Digital Certificates shall be revoked under the Dohatec-CA Trust Network in accordance to the Information and Communication Technology Act, 2006 (Amended in 2013), IT(CA) Rules 2010 – Rule 30 and Information and Communication Technology Act 2006 (Amended in 2013) clause 38.

4.8.1 Circumstances for revocation

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

- Where the subscriber or any person authorized by him/her makes a request to that effect
- Upon the death of the subscriber
- In case where the Subscriber is a firm or a company, if it has been dissolved or wound up or has otherwise ceased to exist.
- In case the private key of the Dohatec-CA or a Partner for whom Sub-CA has been created was compromised in a manner materially affecting the Digital Certificate's reliability
- In case there is a misuse of Digital Certificate
- Compromise of the private key of an RA
- Violation of the any terms of the Dohatec-CA CPS or Subscriber Agreement by the subscribers
- Later changes in the information contained in the Digital Certificate issued by the Dohatec-CA
- A material fact represented in the Digital Certificate is false or has been concealed
- A determination that the Digital Certificate was not issued in accordance with the requirements of the Dohatec-CA CPS or the Subscriber's Agreement
- Any other reason/circumstances that may reasonably be expected to affect the integrity, security, or trustworthiness of Digital Certificate
- The private key of the subscriber is found to be compromised
- The subscriber has been declared insolvent by a competent court or authority
- Instructions from appropriate government authorities, court of law, or law enforcement agencies.

- When the Digital Certificate is no longer required

4.8.2 Who can request revocation

The Subscriber shall request for Digital Certificate revocation when

- the subscriber's private key is compromised or
- the subscriber has reason to believe that the private key may have been compromised or
- there is a change in the Digital Certificate's information or circumstances that might result in the information provided in the Digital Certificate to become inaccurate, invalid or misleading.

The subscriber may voluntarily request for the Digital Certificate to be revoked for any other reason.

Dohatec-CA or RA can also initiate a revocation request under any of the above mentioned circumstances in section 4.8.1.

The RA who has recommended the issuance of Digital Certificate shall request for Digital Certificate revocation when:

- there is evidence leading to the conclusion that the subscriber's private key is compromised or that the private key may have been compromised or
- there is a change in the Digital Certificate's information or circumstances that might result in the information provided in the Digital Certificate to become inaccurate, invalid or misleading.

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

4.8.3 Procedure for revocation request

4.8.3.1 Request from the Subscriber

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

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

The validity of the request will be checked as follows:

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

4.8.3.2 Request from government/courts/law enforcement

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

4.8.3.3 Request from the RA

RA prepares the subscriber's details and signs with the RA's private key and forwards the request to the Dohatec–CA.

RA sends evidence based on which revocation is being requested to Dohatec–CA, under signed covering letter.

After receiving the request for revocation signed by the RA, the Dohatec–CA shall evaluate a revocation request and promptly act to revoke the Digital Certificate. In case Dohatec–CA is in doubt about the genuineness of a revocation request, it reserves the right to conduct further enquiries and take steps including but not limited to suspending the Digital Certificate before making a final determination on whether or not to revoke the Digital Certificate.

In cases where the revocation request is not raised by the Subscriber himself, the Dohatec-CA gives an opportunity to the Subscriber to justify in this matter, before revoking the Digital Certificate, unless otherwise instructed in writing by appropriate government authorities, court of law, or law enforcement agencies

In certain circumstances where there is no evidence, Dohatec–CA or RA may first suspend the certificate and then wait for evidence under signed covering letter, to revoke the certificate. Dohatec–CA then updates the CRL with the list of all revoked certificates and publishes to the repository.

4.8.4 Revocation request grace period

If the private key of the subscriber is compromised, the subscriber shall request for the revocation immediately.

4.8.5 Time within which CA must process the revocation request

A Digital Certificate will be revoked by close of business day for revocations placed online by subscriber from his/her user login and if the request for revocation is received vide email/letter, verification of a revocation request is made and the revocation will be done

on once the verification of is satisfactory. Until the verification is in process, the Digital Certificate may be suspended.

Action on a revocation request made over a weekend or holiday may be delayed until the following business day of the RA.

4.8.6 Revocation checking requirement for relying parties

A relying party shall use the certificates issued under the Dohatec-CA Trust Network only after checking the same with the latest CRL of the corresponding certificate issuer available at the repository. The Dohatec-CA or the RA shall not be liable to any damages/loss caused by the certificates or CRLs.

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

4.8.7 CRL issuance frequency (if applicable)

The Dohatec-CA will update and issue the CRL (including certificates issued for any partner for whom sub-CA has been created) whenever certificates under their respective user groups are revoked or suspended. Irrespective of the occurrence of revocations or suspensions, CRL will be updated once in 7 days. The CRLs will be issued with a validity of 30 days. The CRL issued shall be published to the repository immediately.

4.8.8 Maximum latency for CRLs (if applicable)

There is no latency for Publishing CRLs as it is immediate. CRLs are generated as soon as any Suspension / Activation or Revocation of Certificates takes place. The CRLs are published onto the Dohatec-CA web portal as soon as they are generated.

4.8.9 Certificate Status Service

4.8.9.1 On-line revocation/status checking availability

Dohatec-CA supports on-line revocation status check by hosting OCSP service. The service can be accessed by relying parties from the url:

4.8.9.2 On-line revocation checking requirements

Dohatec-CA supports on-line revocation status check through OCSP service. The relying parties who intend to make use of this service needs to procure OCSP client from Dohatec-CA. Response to the OCSP Request will be digitally signed response using a certificate issued to Dohatec - CA as per the OCSP profile in the Interoperability Guidelines. Details of procuring the OCSP client will be available in Dohatec-CA Trust Portal which can be accessed from the URL http://www.dohatec-ca.com.bd

4.8.10 Other forms of revocation advertisements available

Not Applicable

4.8.11 Special requirements regarding key compromise

Dohatec-CA uses reasonable efforts to notify potential Relying Parties if it discovers, or have reason to believe, that there has been a compromise of the private key of one of their own CAs or Sub-CAs.

4.9 Certificate suspension

Suspension is the process of making the subscriber's certificate to be invalid temporarily based on conditions as specified in this CPS.

The Dohatec–CA either on its own or on the recommendation of a concerned RA shall reserve the right to suspend the certificates of its subscribers. Wherever possible this will be done with reasonable notice to the affected subscribers. By suspension, the certificate usage shall be made invalid temporarily. All suspended certificates shall be listed in the CRL of the Dohatec–CA and published to the repository of the Dohatec–CA. The Dohatec–CA shall reserve the right to activate the certificate when the validity of the certificate has been confirmed.

The Digital Certificates shall be suspended under the Dohatec-CA Trust Network in accordance to the Information and Communication Technology Act, 2006 (Amended in 2013) Clause 39, 40.

4.9.1 Circumstances for suspension

The Dohatec–CA, by itself or on the recommendation of the RA or on the request of a subscriber may suspend a certificate in the following circumstances:

- Upon subscriber requesting for suspension of his/her Digital Certificate
- Non receipt of applicable certificate fees from the RA or Subscriber within the stipulated time
- Any circumstance which leads Dohatec–CA to believe that the trust of the Dohatec–CA Trust Network may be jeopardized
- If it is of opinion that the Digital Certificate should be suspended in public interest by Dohatec-CA

4.9.2 Who can request suspension

Dohatec–CA, RA or the subscriber may request for suspension.

Dohatec–CA, RA or the subscriber may only request for the suspension of the certificate if there is reason to believe that circumstances exist that require the certificate to be suspended.

4.9.3 Procedure for suspension request

The subscribers and the RAs will request for the certificate suspension using the same procedures as for the certificate revocation specified in Section 4.8.3 of this CPS.

4.9.4 Limits on suspension period

The Dohatec–CA reserves the right to revoke the suspended certificates of its subscribers, if a request for activation of suspended certificate is not received within 15 days of the date of suspension.

4.10 Activation of suspended certificates

Activation is the process of making the applicant/subscriber's suspended certificate to be valid for use based on conditions as specified in this CPS.

4.10.1 Who can request Activation

A subscriber can always initiate a request for activation of his/her suspended certificate. RAs may only initiate the request for activation for those certificates for which they had initiated the suspension. CA may initiate the request for activation for any suspended certificate. A certificate shall be activated only if the Dohatec–CA is satisfied that the reason for suspension is no longer valid.

4.10.2 Procedure for activation request

The suspended certificates shall be re-activated upon approval by the Dohatec–CA or when the same party that had the certificate suspended initiates the request. This should be done within 15 days after the Digital Certificate has been suspended. The Dohatec–CA shall remove the re-activated certificates from the corresponding CRL listing and a new CRL will be generated and published to the repository.

4.11 End of subscription

A Subscriber can be terminated or inactivated by the Dohatec- CA, if certificate has been found to be misused or if involved in fraud or illegal activities. In such cases, Dohatec-CA reserves the right to revoke the Subscriber's certificate immediately and inactivate the Subscriber.

A subscriber may also end a subscription for a Dohatec-CA certificate by:

- Allowing the Digital Certificate to expire without re-keying that certificate
- Revoking the Digital Certificate before certificate expiration without requesting for a new certificate.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Dohatec – CA only Archives the CA keys, Subscriber Encryption Keys.

The Subscriber public key of the Signing Certificate will be retained and archived by the Dohatec–CA for the Certificate life-cycle management.

A signing private key is generated at the subscriber end and neither the Dohatec–CA nor RA gets to see this key at any time.

The generation of the encryption key pair will be in at the Dohatec–CA end in secure premises and is protected with a password. A copy of the Encryption key of the subscriber shall be retained in the safe custody of the Dohatec–CA.

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

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

The Dohatec–CA system components and operations will be contained within a physically protected environment. The environment will have sufficient controls to deter, detect and prevent unauthorized use of, access to, or disclosure of sensitive information. The physical security standards are modeled as per the industry best practices for physical and operational security.

5.1.2 Physical access

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

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

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

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

5.1.3 Power and air conditioning

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

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

5.1.4 Water exposures

All precautions will be taken to protect critical systems on Dohatec–CA operation premises from water damages by using raised floors and water detector systems

5.1.5 Fire prevention and protection

Automatic fire detectors and extinguishers compliant with standard requirements specified by the fire brigade will be installed in the Dohatec–CA operating premises to prevent and protect the facility from fire.

5.1.6 Media storage

Appropriate measures will be taken to protect the media relevant to Dohatec–CA operations. The media will be protected in a secure place with access restricted to authorized personnel.

5.1.7 Waste disposal

All the unused, unwanted documents and media relevant to Dohatec-CA operations will be scrutinized before being destroyed or released for disposal.

5.1.8 Off-site backup

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

5.2 Procedural controls

5.2.1 Trusted roles

Employees who will have access to or control operations that may materially affect the issuance, use, suspension, activation or revocation of Digital Certificates, including access to restricted operation of the Dohatec–CA Repository, are considered as serving in trusted positions. Such personnel include but are not limited to, system administration personnel, designated consultant, and executives who will be designated to oversee the Dohatec–CA infrastructure.

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

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

5.2.2 Number of persons required per task

Dohatec-CA will maintain 2 CA Administrators, 2 RA administrators and 2 System Administrators to carry out the designated activities. Separate individuals will be identified for each of these roles. Dohatec-CA may deploy additional persons as needed for satisfying operational and administrative needs.

5.2.3 Identification and authentication for each role

- All personnel performing trusted roles in the Dohatec-CA Trust Network facility will have their identities and authorization verified before they are empowered to perform the appropriate trusted role.
- Class 3 Dohatec-CA Digital Certificates would be issued only to users of type Certifying Authority (CA), Partner for whom Sub-CA has been created Administrator (Sub-CAA), RA Administrator (RAA), RA Operator (RAO), CA Administrator (CAA) and CA Operator (CAO) for performing respective operations under the Dohatec-CA Trust Network. No personnel belonging to other trusted roles would be issued a Digital Certificate for conducting related operations.
- Each of these Certificates and accounts will
    - Be restricted to the actions and uses authorized for that trusted role
    - Not be shared with anyone
    - Be directly attributed to the personnel performing that trusted role

5.2.4 Roles requiring separation of duties

The Dohatec-CA operations will be carried out by the individuals under the roles of CA Administrator, RA Administrator, System Administrator and Helpdesk. Separate individuals will be identified for these roles to prevent same individual performing multiple duties under different roles.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

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

The Dohatec-CA will grant the trusted status to the person after he/she has acquired the required skills and qualification to perform the trusted role.

5.3.2 Background check procedures

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

- Check of qualifications relevant to the trusted role responsibilities.
- Check of prior employment
- Check identification details

- Check Criminal records
- Check Professional Certificate (if any available)
- Background Check (Recheck at least every three years)
- The personnel shall be rejected for the trusted role if any of the above checks reveals misrepresentation or indicates that the concerned individual is not suitable for the corresponding trusted role.

5.3.3 Training requirements

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

- Comprehensive training with respect to the duties to be performed.
- Awareness of the relevant aspects of Information Technology Security Policy and Security Guidelines framed for carrying out Dohatec-CA or RA operations.
- Training in disaster recovery and business continuity procedures formed by the Dohatec-CA or RA as applicable.
- Training in the PKI software used to perform the operations.
- The training method may vary from on-job training, classroom based training, self-study and Computer Based Training (CBT). The training program will be revised as and when necessary to improve the performance of its personnel.
- Use and operation of deployed hardware and software

5.3.4 Retraining frequency and requirements

The Dohatec-CA or RA will provide its personnel ongoing training to update their skills and knowledge to perform their job responsibilities ably and satisfactorily. Refresher training for the personnel in all the trusted roles shall be given by the Dohatec-CA or RA as and when required.

Dohatec-CA will review the training plans for the personnel in all the trusted roles on yearly basis.

5.3.5 Job rotation frequency and sequence

Not applicable

5.3.6 Sanctions for unauthorized actions

Dohatec-CA will take appropriate disciplinary actions against personnel for unauthorized actions or other violations of the policies and procedures of operations of Dohatec-CA.

Dohatec-CA will also recommend the Partner for whom Sub-CA has been created to take appropriate disciplinary actions against personnel for unauthorized actions or other violations of the policies and procedures of Operations. Additionally, all such actions should be brought to the notice of Dohatec-CA.

5.3.7 Independent contractor requirements

All the personnel responsible for carrying out the operations under the Dohatec-CA will be employees of Dohatec.

5.3.8 Documentation supplied to personnel

All the personnel involved in the PKI services under the Dohatec–CA Trust Network will be required to read the Dohatec–CA CPS and Security Policy documents.

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

5.4 Audit logging procedures

The Dohatec–CA will archive all the operational records in accordance to the standards specified by CCA Bangladesh. All the significant security events are time stamped and recorded as audit logs in the audit trail files. These audit trail files are archived periodically.

5.4.1 Types of events recorded

Adequate audit trails will be captured of all sensitive events and pattern analysis made to analyse any misuse as mentioned in this sub-section. All the log files contain the following information:

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

The following sub sections contain the type of events that are logged:

5.4.1.1 Certificate Life Cycle Management

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

5.4.1.2 Key Life Cycle Management

- Key Generation, backup, archival, recovery and destruction of the CA or Sub-CA Key

5.4.1.3 System Security Events

- System start-up and shutdown
- Application start-up and shutdown
- Attempts to create, remove, set passwords or change the system privileges of the Application

- Changes to Dohatec-CA key or any of its details
- Changes to Certificate policies
- Unauthorized attempts at network access to the Dohatec-CA system
- Unauthorized attempts to system files.

5.4.1.4 Other Events

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

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

Audit logs will be retained for seven years.

5.4.4 Protection of audit log

The access to the audit logs will be restricted to the designated administrators of the system. Only the authorized administrators can view or delete the audit log files. Unauthorized access to the audit logs are restricted by physical and logical access control systems and such access will be logged.

5.4.5 Audit log backup procedures

The audit files are backed up on a weekly basis and the backup is archived in a secure location with access limited to a few trusted personnel only.

5.4.6 Audit collection system (internal vs. external)

All the operations related to entry to and exit from the Dohatec-CA system will be logged along with the operational procedures. The Audit collection system is internal to Dohatec-CA.

5.4.7 Notification to event-causing subject

The audit logs will be enabled to provide information of any unauthorized access to the Dohatec-CA system or premises. These Audit logs will be periodically checked and any such events are brought to the notice of the relevant personnel immediately.

5.4.8 Vulnerability assessments

Vulnerability assessments will be performed, reviewed on half yearly basis based on the type of events logged by the authorized personnel. The required mitigation actions will be taken and the vulnerabilities will be closed.

5.5 Records archival

5.5.1 Types of records archived

5.5.1.1 Digital Certificate Life Cycle Management

The Dohatec-CA will archive records of activities involving Digital Certificate generation, revocation, suspension and activation of all their Certificates. Additionally, the certificates generated by Dohatec-CA will also be archived. The events that will be archived as per the Rule 28 of IT (CA) Rules 2010 include:

- The details of the Subscriber/Applicant
- application of the applicant for issue of Digital Certificates
- registration and verification documents of Digital Certificates
- Identity of the RA personnel processing the request
- The requests verified and forwarded by the corresponding RA
- Audit Logs which are retained for time specified in the CPS
- All Digital Certificates generated by the Dohatec-CA under the Dohatec-CA Trust Network will be retained in Dohatec-CA records for at least seven years.
- Notices for suspension
- Information of suspended, revoked and expired Digital Certificates

5.5.1.2 Backup of records

A copy of all records of the operations of the Dohatec-CA will be retained at three different locations within the country including the Dohatec-CA premises stored in a secure place with restricted access. The Dohatec-CA shall verify the integrity of the backups at least once in every six months or any time period as specified by CCA, Bangladesh.

5.5.2 Retention period for archive

All data and records pertaining to the Subscriber, the various states of the Certificate lifecycle and the corresponding application form and the supporting Documents are all archived and retained for a period of 7 years.

5.5.3 Protection of archive

The access to the archives will be restricted to the designated administrators of the system. Only the authorized administrators can view, modify or delete the archives. Unauthorized access to the archives is restricted by physical and logical access control systems and such access will be logged.

5.5.4 Archive backup procedures

Multiple copies of archives shall be taken and shall be backed up as specified in Section 5.5.1.2 Backup of records

5.5.5 Requirements for time-stamping of records

The electronic records are time-stamped with the Server time which is synchronized over the Internet with the Time Server available at CCA Bangladesh premises.

5.5.6 Archive collection system (internal or external)

Archives are stored securely as specified in Archival Procedures Manual

5.5.7 Procedures to obtain and verify archive information

The procedure to obtain the archive and verify is specified in Archival Procedures Manual.

5.6 Key changeover

The keys of Dohatec-CA, Partner for whom Sub-CA has been created, RAs and Subscriber will be changed periodically. The key change will be processed as per Section 6.1.1 Key Pair Generation specified in this CPS.

Key changeover for Dohatec-CA/Sub-CA can happen under the following circumstances:

- When the Dohatec-CA/Sub-CA certificate is due for expiry
- When the Dohatec-CA/Sub-CA key is compromised
- When CCA Bangladesh mandates the CA's to procure a new key due to change in CA certificate profile. This will eventually lead to changes in Sub-CA keys

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

Digital Certificates will be issued to the Subscribers of Dohatec-CA Trust Network for a specified period of time. The Subscribers will generate a new private-public key-pair before or after the expiration of the Certificate and submit the public key along with the new application to the corresponding Dohatec-CA or RA for generating a new Certificate. This process is carried out preferably before the existing Digital Certificate expires.

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

- Dohatec-CA Certifying Authority's keys and associated Certificates - maximum 10 years
- The keys of the partner for whom Sub-CA has been created and associate Certificates - up to a maximum of 5 years not exceeding the expiry period of Dohatec-CA Digital Certificate
- Subscriber Digital Certificate key - One Year.

5.7 Compromise and disaster recovery

The private keys and critical information of Dohatec-CA and the Partner for whom Sub-CA has been created under the Dohatec-CA Trust Network will be backed up. Additionally, the Authority's public keys will be archived permanently. In the event of compromise of Dohatec-CA or Partner for whom Sub-CA has been created, the event will be informed to all the applicable Subscribers as soon as possible. The same will also be published in the Dohatec-CA Trust Portal.

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

In case of Dohatec-CA Key compromise, all Certificates issued by Dohatec-CA shall be revoked and a CRL shall be generated. The CRL is posted on the Dohatec-CA Trust Portal and a communication shall be sent to the CCA notifying the event. A new public - private key pair will be generated for the CA and the corresponding CA certificate request communicated to the CCA. A new CA Certificate will be generated for Dohatec-

CA and the same will be hosted on the Dohatec-CA portal. All customers whose Certificates are still valid will be notified via email, and upon request, will be provided new Certificates signed with the new Dohatec-CA Certificate. There will be no extra charge for this.

5.7.1 Incident and compromise handling procedures

The Dohatec-CA or the Partner for whom Sub-CA has been created under the Dohatec-CA Trust Network shall follow the procedures for handling incidents such as breach of physical security, hacking of systems and/or network.

Any breach of security is immediately brought to the notice of the Dohatec Senior Management and appropriate action will be taken.

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

Any damage to the Systems, software, networking devices, HSM or data when detected is immediately reported and appropriate measures are taken to bring up the stand-by or fail over systems. In case necessary Data will be restored from the back up. Appropriate investigations will be carried out to identify the root cause for any such event and corrective measures are taken within an agreed upon timeframe.

5.7.3 Entity private key compromise procedures

In case of the Subscriber's / End Entity private key being compromised, the Dohatec–CA will immediately revoke the affected Digital Certificate upon receiving information by the Subscriber or on the recommendation of the RA.

5.7.4 Business continuity capabilities after a disaster

Dohatec-CA will maintain a DR Site in a separate location and will ensure synchronization of the data between the Primary and DR site. In case of any disaster, Dohatec–CA will bring up the DR site and resume its operations.

5.8 CA or RA termination

The Dohatec–CA and the Partner for whom Sub-CA has been created shall reserve the right to terminate its operations at any time with reasonable notice as stated in Section 5.8.1 below to all affected parties. The Dohatec–CA will take the necessary steps to destroy all copies of the private keys and notify the details of such activity to CCA (in case of Dohatec–CA) as specified by Rule 22 (9) of IT (CA) Rules 2010.

Dohatec–CA will reserve the right to terminate the operations of the Sub-CA when it receives a notification for withdrawal of Sub-CA operations or when there is no request for renewal of the Sub-CA agreement. In such a case Dohatec CA will communicate the decision to terminate Sub-CA services to the Partner for whom Sub-CA has been created via email.

The Dohatec–CA will take necessary steps to destroy the private key and notify the details of such activity to the Partner for whom Sub-CA has been created.

In case of RA termination, the Dohatec-CA takes the responsibility of certificate Revocation, Suspension or Activation requests arising from the Subscribers belonging to that RA, until all the certificates issued under that RA expire. No new Certificate requests or routine re-key requests will be accepted from the terminated RA. All new certificate requests shall be raised under a new RA.

5.8.1 Requirements prior to Cessation

The following obligations will be followed by Dohatec-CA and the Partner for whom Sub-CA has been created to reduce the impact of termination of service by providing for timely notice, transfer of responsibilities to succeeding entities, maintenance of records, etc.

Before ceasing the operations, Dohatec–CA will perform the following operations as specified in IT (CA) Rules 2010 – Rule 22

- Notify CCA of its intention to cease acting as Dohatec–CA. Such notice shall be made at least ninety (90) days before ceasing to act as Dohatec–CA or ninety days before the date of expiry of license.
- advertise sixty days before the expiry of license or ceasing to act as Certifying Authority, as the case may be by publishing notice of the intention in such daily newspaper or electronic media and website and in such manner as the Controller may determine
- notify its intention to cease acting as a Certifying Authority to the subscribers and Cross Certifying Authority of each unrevoked or unexpired Digital Certificate issued by it; provided that the notice shall be given 60 (sixty) days before ceasing to act as a Certifying Authority or 60(sixty) days before the date of expiry of Digital Certificate, as the case may be
- the notice shall be sent to the Controller, affected subscribers and Cross Certifying Authorities by electronically signed e-mail and registered post
- After the date of expiry as mentioned in the license, the Certifying Authority shall destroy the certificate signing private key and inform the date and time of destruction of the private key to the Controller.
- Revoke all Certificates that remain unrevoked or unexpired at the end of the sixty (60) day notice period, whether or not the Subscribers have requested revocation. This is to enable the Subscribers to find alternate means of certification and thereby prevent undue disruption to their business.
- Give notice of the revocation to each affected Subscriber.
- Make a reasonable effort to ensure that discontinuing its certification services will cause minimal disruption to its Subscribers and to persons duly needing to verify Digital Signatures by reference to the public keys contained in outstanding Certificates.
- Make reasonable arrangements for preserving the records for 10 years.

Before ceasing the operations, the Partner for whom Sub-CA has been created:

- Notifies Dohatec–CA of its intention to cease acting as a Partner for whom Sub-CA has been created. Such notice will be made at least ninety (90) days before ceasing to act as the Partner for whom Sub-CA has been created or ninety days before the date of expiry of license. Dohatec–CA may require additional statements in order to verify compliance with this provision.
- Provides a sixty (60) day notice to the Subscriber of each unrevoked or unexpired Certificate of its intention to cease acting as the Partner for whom Sub-CA has been created.
- Initiates revocation of all Certificates through its RA that remain unrevoked or unexpired at the end of the sixty (60) day notice period, whether or not the

Subscribers have requested revocation. This is to enable the Subscribers to find alternate means of certification and thereby prevent undue disruption to their business.

- Give notice of the revocation to each affected Subscriber.
- Make a reasonable effort to ensure that discontinuing its certification services will cause minimal disruption to its Subscribers and to persons duly needing to verify Digital Signatures by reference to the public keys contained in outstanding Certificates.
- Make reasonable arrangements for preserving the records for 10 years.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key Pair Generation

The private-public key pairs of Dohatec-CA and the Partner for whom Sub-CA has been created will be generated by Dohatec-CA confidentially using the standards specified in the Bangladesh Information and Communication Technology Act 2006 (Amended in 2013), IT (CA) Rules 2010 and Interoperability Guidelines published by CCA. RA's key pair generation follows the same process as key generation for subscribers under Class 3 certificates. The key generation will be conducted in a secure and trustworthy environment. The Certificate and key generation shall be documented and witnessed for authentication purpose. The size of the Key pair for RA will be the same as that of the subscriber.

Subscribers will be required to generate private/public key pairs generated on a secure medium. The key pair size will be as prescribed in the section 3.3.1 of the Interoperability Guidelines published by CCA.

The Dohatec-CA and the Partner for whom Sub-CA has been created will generate encryption private-public RSA key pairs for Subscribers. The key size of the encryption certificate of the subscriber will be equivalent to the Subscriber's Signing Certificate as per section 3.3.1 of the Interoperability Guidelines published by CCA.

6.1.2 Private Key delivery to subscriber

The Dohatec-CA will generate the private key of the encryption key pair for the Subscriber, and the private key will be delivered to the Subscriber as a PKCS #12 file which is password protected. The password will be securely communicated to the subscriber. To download the encryption certificate the Subscriber has to possess a Signing Certificate from Dohatec-CA. During download, Dohatec-CA will validate the Subscriber by verifying the Subscriber's signature produced by Subscriber's signing private key before delivering the encryption private key.

The private key for all other types of certificates are generated by the Subscriber / Applicant in a secure medium. The private key for these types of certificates will not be shared with Dohatec-CA and will remain with the Subscriber.

6.1.3 Public key delivery to certificate issuer

The Subscriber / Applicant of a Digital Certificate from Dohatec-CA will produce supporting documents along with the filled in application form to the RA. The request is standards based PKCS#10 form. The Public Key is communicated to the Dohatec - CA as part of the PKCS#10 requests. The RA verifies the request details against the application form and the submitted Identity/Address Proofs.

The RA digitally signs and forwards the request to the CA only after establishing the proof of possession of the private key of the Subscriber.

The public key for the Encryption Certificate will be generated by the Dohatec-CA

6.1.4 CA public key delivery to relying parties

The Digital Certificate of the Dohatec-CA or the Partner for whom Sub-CA has been created will be published in the Dohatec-CA repository. The relying parties can connect to the Dohatec-CA repository and fetch the Digital Certificate of Dohatec-CA or the Partner for whom Sub-CA has been created.

6.1.5 Key sizes

The key length of the Dohatec-CA or the Partner for whom Sub-CA has been created or Subscriber/Applicant will be according to Section 3.1.1 Root CA Certificate Profile of the Interoperability Guidelines published by CCA.RA's key size will be same as that of subscriber.

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

The key usage for the various types of certificates supported by Dohatec-CA is tabulated below:

Certificate Type	Key Usage	Extended Key Usage
Signing Certificate	digitalSignature, nonRepudiation	clientAuth
Encryption Certificate	keyEncipherment	
SSL Certificate	digitalSignature, keyEncipherment	serverAuth

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The Dohatec-CA or RA under the Dohatec-CA Trust Network will utilize hardware cryptographic modules to perform all Digital signing operations that are rated FIPS 140-2 Level 2 of security.

The private key of Dohatec-CA and the Partner for whom the Sub-CA has been created will be stored in Hardware Security Module that is rated FIPS 140-2 Level 3of security.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The Digital Certificates issued by Dohatec-CA or the Partner for whom the Sub-CA has been created will be retained and archived by the Dohatec-CA for the Certificate life-cycle management.

6.3.2 Certificate operational periods and key pair usage periods

The Digital Certificate issued by Dohatec-CA or the Partner for whom the Sub-CA has been created is valid for the period specified in the Dohatec-CA Trust Portal and can neither be extended nor renewed thereafter. After expiry of the existing Digital Certificate, the Subscriber/Applicant must apply for and obtain a new Digital Certificate, including submitting details for verification as before.

6.4 Activation data

The private keys of Dohatec-CA and the Partner for whom the Sub-CA has been created are used for performing activities like Certificate generation, suspension, activation or revocation and CRL generation. The private keys will be stored in FIPS 140-2 Level 3 compliant hardware device, which is activated using tokens.

6.5 Computer security controls

The Dohatec-CA Digital Certificate generation system provides reasonable assurance that the system software and the data files used to issue, suspend, activate and revoke Digital Certificates shall be secured from unauthorized access. The access to the production systems is strictly limited to those individuals who are identified to perform the concerned activities. Remote access will not be permitted to Certificate Generation Module. Remote access for other management functions will be restricted to authorized users who authenticate themselves to the system. The systems will be monitored regularly and appropriate action will be taken when any security event is noticed.

The Dohatec-CA Digital Certification services and corresponding system utilizes a wide variety of hardware and software to perform various functions in a secure and timely manner.

6.6 Life cycle technical controls

6.6.1 Security management controls

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

Dohatec-CA will conduct Vulnerability Assessments and Network Penetration Testing to ensure that the Operational Systems and networks are secure.

Dohatec-CA in its operation maintains configuration management system to keep track of changes to the CA software.

6.7 Network security controls

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

6.8 Time-stamping

All servers used in the Dohatec–CA Trust Network set-up use the NTP suite of programs to keep themselves synchronized with timeservers with CCA Bangladesh.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate profile

Digital Certificates issued by the Dohatec–CA under this CPS will contain public keys used for authenticating the sender of the electronic message and verifying the integrity of such messages.

The Digital Certificate created will conform to International Telecommunication Union X.509 version 3 standards. The Digital Certificates produced under this CPS will contain the fields and indicated prescribed values or constraints described in Interoperability Guidelines published by CCA. The latest version published on the CCA website http://www.cca.gov.bd/

Certificate Profiles are as stated in the latest version of Interoperability guidelines published on the CCA website http://www.cca.gov.bd/

7.2 CRL profile

Certificate Revocation List issued by the Dohatec–CA will contain the list of the Revoked and Suspended Certificates.

The CRL created will conform to International Telecommunication Union version 2 standards. The CRL produced under this CPS will contain the field and indicated prescribed values or value constraints described in Interoperability Guidelines published by CCA. The latest version of which, is made published on the CCA website http://www.cca.gov.bd/

CRL Profile is as stated in the latest version of Interoperability guidelines published on the CCA website http://www.cca.gov.bd/

7.3 OCSP Profile

Dohatec-CA supports on-line revocation status check through its OCSP service. Any relying party application intending to make use of this service sends an OCSP Request to the responder. The response given out by the Dohatec-CA OCSP Responder shall be digitally signed using the certificate whose profile will be as per section 3.3.5 of the Interoperability Guidelines issued by the CCA Bangladesh.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The Dohatec-CA and the RAs under the Dohatec-CA Trust Network will implement and preserve an audit trail of all material events, such as key generation and Digital Certificate application, validation, suspension, and revocation and other audit records for the relevant time period as specified in this CPS

The Dohatec-CA will be audited by empaneled external auditors who are recognized by CCA. The audit will be carried out for compliance with the procedures specified in this CPS as well as the provisions of section 32(1) of IT (CA) Rules 2010.

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

8.1 Frequency or circumstances of assessment

The compliance audit of the Dohatec-CA will be done annually by the CCA empanelled auditors and the scope of the audit will be as per the section 32 (1)of IT (CA) Rules 2010.

In addition, Dohatec-CA shall also conduct two internal audits:

- A half yearly audit to ensure compliance with documented processes, security policy, physical security and planning of its operation
- A quarterly audit of its repository

8.2 Identity/qualifications of assessor

The annual audit will be performed by the empaneled external auditor, who is recognized by the Controller of Certifying Authorities.

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

8.3 Assessor's relationship to assessed entity

The auditing firm involved in the preparing the audit reports will be independent of the party being audited and will not be a software or hardware vendor which is, or has been providing services or supplying equipment to the party being audited. The auditing firm

and the party being audited will not have any current or planned financial, legal or other relationship, other than that of an auditor and the audited party.

8.4 Topics covered by assessment

The auditor will examine all procedures and operations of the Dohatec–CA performing the Certification Services for compliance with the Bangladesh Information and Communication Technology Act 2006 (Amended in 2013), IT (CA) Rules 2010 and Audit Guidelines given by CCA and prepare audit reports.

Dohatec–CA will conduct half yearly internal audit of the security policy, physical security, planning of its operations and quarterly audit of the repository. The annual audit will include the following:

- Security policy and planning
- Physical security
- Technology evaluation
- Certifying Authority's services administration
- Relevant Dohatec–CA CPS
- Compliance with the relevant Dohatec–CA CPS
- Contracts/Agreements
- Regulations prescribed by the controller
- Policy in according to the requirement of Dohatec-CA
- The audited party will follow approved procedures to ensure that its activities are recorded and made available during audits.

8.5 Actions taken as a result of deficiency

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

8.6 Communication of results

After commencement of the operations by the Dohatec-CA, Dohatec-CA will communicate the results of the periodic audits by the empaneled auditors concerning the state of practices and procedures in the audited party, to the CCA within 4 weeks of receiving the audit report.

9. OTHER BUSNESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Dohatec-CA is entitled to charge Subscribers for issuance and renewal of certificates accordingly the fees will be set as per the guideline provided by the CCA, Bangladesh.

9.1.2 Certificate access fees

Dohatec-CA does not charge any fees for accessing Digital Certificate in a repository or making it available to the Relying Parties.

9.1.3 Revocation or status information access fees

Dohatec does not charge any fees for making the CRLs available in a repository or making it available to the Relying Parties. However Dohatec can charge for providing OCSP service for checking the revocation status instead of a CRL. In such cases, the relying parties would need to procure OCSP client from Dohatec-CA.

9.1.4 Fees for other services

Dohatec does not charge a fee for access to this CPS. However, Dohatec is entitled to charge a fee for a printed version of CPS.

9.1.5 Refund policy

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

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

9.2 Financial responsibility

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

9.3 Confidentiality of business information

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

- Is posted to Dohatec-CA's website/ Trust Portal

- Is in the possession of Subscriber, except information which has been received under an obligation of confidentiality agreed to by the Dohatec-CA and/or RA in a written agreement, or
- Is or becomes publicly available.
- The Dohatec-CA and the RAs under the Dohatec-CA Trust Network and PKI Services shall take reasonable care in protecting the information from being disclosed or used for purposes other than specified in this Dohatec-CA CPS.
- Access to confidential information by operational staff of the Dohatec-CA shall be on a need-to-know and a need-to-use basis. Paper-based records, documents and backup data containing confidential information shall be kept safely and securely, and away from other (non-confidential) data.
- The confidential information shall not be taken out of the country except where a properly constitutional warrant or other legally enforceable document is produced to the Controller and only after the CCA permits Dohatec-CA to do so.
- The Dohatec-CA and the RAs under the Dohatec-CA Trust Network and PKI Services shall not disclose the information provided by the Applicant/Subscriber, unless otherwise specified elsewhere within this Section 9.3 of the CPS.

9.3.1 Scope of confidential information

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

- CA application records, whether approved or disapproved.
- Certificate Application records
- Encryption Private keys held by Dohatec-CA and information needed to recover such Private Keys
- Executed Subscriber Agreement
- Transactional records (both full records and the audit trail of transactions), Audit trail records of the Dohatec-CA, Sub-CA and RA operations.
- Audit reports created by Dohatec (to the extent such reports are maintained), or their respective auditors (whether internal or public).
- Contingency planning and disaster recovery plans.
- Security measures controlling the operations of the Dohatec-CA, Sub-CA and the RAs

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

9.3.2 Information not within the scope of confidential information

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

- Digital Certificate.
- CRL.
- Dohatec-CA public Repositories
- Information not expressly deemed Confidential/Private Information under Section 9.3.1 shall be considered neither confidential nor private.

9.3.3 Responsibility to protect confidential information

Dohatec-CA secures private information from compromise and disclosure to third parties.

9.4 Privacy of personal information

9.4.1 Privacy plan

None

9.4.2 Information treated as private

Any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private

9.4.3 Information not deemed private

All information made public in a certificate is deemed not private. This is subject to applicable local laws.

9.4.4 Responsibility to protect private information

Participants receiving private information shall secure it from compromise and disclosure to third parties and shall comply with applicable privacy laws in their jurisdiction.

9.4.5 Notice and consent to use private information

Unless otherwise stated in this CPS the private information will not be used without the consent of the party to whom the information applies. This is subject to applicable privacy laws.

9.4.6 Disclosure pursuant to judicial or administrative process

Dohatec-CA shall be entitled to disclose Confidential/Private Information if:

- Disclosure is necessary in response to search warrants.
- Disclosure is necessary in response to judicial, administrative, or other legal process.

This is subject to applicable privacy laws.

9.4.7 Other information disclosure circumstances

No stipulation

9.5 Intellectual property rights

The allocation of Intellectual Property Rights to participants other than Subscribers and Relying Parties is governed by the applicable agreements among the participants. The following subsections of Section 9.5 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information

Dohatec-CA retains all Intellectual Property Rights in and to the Certificates and CRLs issued by them. Dohatec-CA grants non-exclusive, non-transferable permission to its Subscribers and the Relying Parties to:

- Reproduce and distribute Certificates provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate.
- Use revocation information to perform Relying Party functions subject to the applicable Relying Party Agreement, or any other applicable agreements.

9.5.2 Property Rights in the CPS

Dohatec-CA retains all Intellectual Property Rights in and to this CPS.

9.5.3 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to certificates of Dohatec-CA and the Partner for whom the Sub-CA has been created regardless of the physical medium within which they are stored and protected are the property of Dohatec–CA.

Key pairs corresponding to certificates of the Subscribers are the property of the Subscribers regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs.

9.6 Representations and warranties

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

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

9.6.1 CA representations and warranties

Dohatec-CA warrants:

- To provide the Digital Certification services such as Dohatec-CA Repository.
- To provide the PKI architecture for operating as CA as specified in this CPS.
- That the RAs established by Dohatec-CA shall perform the validation of the Digital Certificate management as per the CPS.
- That the RAs appointed by Dohatec-CA or by any Partner for whom Sub-CA has been created shall perform the validation of the Digital Certificate application as per the CPS.
- The issuance of Digital Certificates to the validated Applicants as specified in this CPS.
- A Digital Certificate will be revoked by close of business day for revocations placed online by subscriber from his/her user login and if the request for revocation is received vide email/letter, verification of a revocation request is made and the revocation will be done on the following business day, but action on a revocation request made over a weekend or holiday may be delayed until the following business day of the RA.
- To activate the Subscriber's Digital Certificate within 1 week of receipt of valid request from the RA to activate a particular Digital Certificate of a Subscriber.
- To publish the user accepted Digital Certificates in the Dohatec-CA Repository.
- To put the revoked/suspended Digital Certificates in the Repository.
- To generate a Dohatec-CA CRL with suspended, activated and revoked Digital Certificates and publish the updated CRL to the Dohatec-CA

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

- Forward the verified Applicant's request for issuing a Digital Certificate to the Dohatec-CA.
- Send a request to the Dohatec-CA to suspend, activate or revoke a Digital Certificate.
- Activate the Subscriber's Suspended Digital Certificate within 1 week of receipt of valid request from the RA to activate a particular Digital Certificate of a Subscriber.

9.6.2 RA representations and warranties

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

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

9.6.3 Subscriber representations and warranties

The following are the responsibilities of the Subscriber who intends to procure a Digital Certificate from the Dohatec – CA. The Subscriber

- Generates his/her Certificate Request as per the requirements mentioned in this CPS under section – 3.2 Initial Identity Validation , based on the Class of Certificate being requested.
- Accepts and abides by the terms and conditions specified in the Subscriber Agreement given by the Dohatec – CA.
- Will be solely responsible for his/her Private Key associated with his/her Digital Certificate and will not subject the Digital Certificate to mis-use.
- Will ensure that the private key is protected and that no unauthorized person has any access to the private key
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS

9.6.4 Relying party representations and warranties

Relying Parties are bound by the Relying Party agreements to acknowledge that:

- they have sufficient information to decide the extent to which they choose to rely on the information in a Certificate

- they are solely responsible for deciding whether or not to rely on such information
- they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CPS.

9.6.5 Representations and warranties of other participants

None

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages.

Under no event will the aggregate liability of any RA, partner for whom Sub-CA has been created, Relying Parties and Dohatec-CA exceed the applicable liability cap for such certificate. Below are given the Liability Caps for the different classes of certificates.

Class	Liability Caps
Class 0	No liability
Class 1	No liability
Class 2	BDT 5000
Class 3	BDT 10000

The liability of Subscribers shall be as set forth in the applicable Subscriber agreements.

The liability of RAs, partner for whom Sub-CA is created shall be set out in the applicable Dohatec – CA and the RA/ Sub-CA partner agreements.

The liability of Relying Parties shall be as set forth in the applicable Relying Party agreements

9.9 Indemnities

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

9.9.1 Indemnification by the Subscriber

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

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

9.9.2 Indemnification by the Relying Parties

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

- Lack of proper validation of the Digital Certificates done by the relying parties before using the Certificates.
- Relying on Digital Certificates that have expired or revoked and are no longer valid.
- Using Digital Certificates for purposes other than those permitted for the corresponding classes of Certificates.

9.9.3 Fiduciary Relationships

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

9.10 Term and termination

9.10.1 Term

This CPS and its subsequent amendments become effective upon publication to Dohatec-CA Trust Network portal.

9.10.2 Termination

This CPS shall remain in force until it is replaced by a new version.

9.10.3 Effect of termination and survival

Upon termination of this CPS, the Dohatec-CA RAs and the partner for whom the Sub-CA is created under the Dohatec-CA Trust Network remain bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual notices and communications with participants

Parties under the Dohatec-CA Trust Network shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication unless otherwise specified in the agreement.

9.12 Amendments

9.12.1 Procedure for amendment

Dohatec – CA reserves all rights to make amendments to this CPS. Amended versions of the CPS on approval by CCA, Bangladesh will be published on the Dohatec- CA Trust Network portal. Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

9.12.2 Notification mechanism and period

Dohatec – CA reserves the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. Such amendments will be effective immediately upon publication.

9.12.3 Circumstances under which OID must be changed

In the event of CCA Bangladesh, indicating a change in the object identifier corresponding to a Certificate policy, the amendment shall contain new object identifiers for the Certificate policies corresponding to each Class of Certificate.

- OID of Dohatec-Certifying-Authority (2.16.50.1.7)
- CPS of Dohatec-Certifying-Authority (2.16.50.1.7.1)
- CP of Dohatec-Certifying-Authority (2.16.50.1.7.2)

9.13 Dispute resolution provisions

Any dispute arising among Dohatec–CA, RAs or, partner for whom Sub-CA has been created; Subscribers and Relying Parties shall be resolved pursuant to provisions in the applicable agreements. The agreements shall contain a dispute resolution clause.

9.14 Governing law

The laws of the Peoples' Republic of Bangladesh shall govern the enforceability, construction, interpretation, and validity of this CPS. This is in accordance with the Information and Communication Technology Act, 2006 (Amended in 2013).

9.15 Compliance with applicable law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations in accordance with the Information and Communication Technology Act, 2006 (Amended in 2013) and IT (CA) Rules 2010.

9.16 Miscellaneous provisions

All agreements drawn up by Dohatec-CA with its RAs, partners for whom Sub-CA is created, Subscribers and Relying Parties shall include a force majeure clause protecting Dohatec – CA.

10. Dohatec-CA Subscriber Agreement (Sample)

DOHATEC – CERTIFYING AUTHORITY
[DIGITAL CERTIFICATION SERVICES]

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

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

DOHATEC Digital Certification Services are governed by DOHATEC - CERTIFYING AUTHORITY Trust Network Certificate Practice Statement (the "Dohatec-CA CPS") as amended from time to time, which is incorporated by reference into this Subscriber Agreement. The Dohatec-CA CPS is published on DOHATEC - CERTIFYING AUTHORITY repository at http://www.dohatec-ca.com.bd. Amendments to the Dohatec-CA CPS are also posted in DOHATEC - CERTIFYING AUTHORITY repository at http://www.dohatec-ca.com.bd.

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

YOU CERTIFY THAT THE INFORMATION PROVIDED BY YOU IS ACCURATE, CURRENT AND COMPLETE. YOU CONSENT TO THIRD PARTY, INDEPENDENT VERIFICATION OF THE PROVIDED INFORMATION. SHOULD THERE BE ANY MATERIAL CHANGES IN THE INFORMATION PROVIDED IN YOUR APPLICATION AFTER A DIGITAL CERTIFICATE HAS BEEN ISSUED TO YOU, THE CERTIFICATE WILL BE RENDERED INVALID AND YOU WILL HAVE TO APPLY FOR A NEW CERTIFICATE. YOU SHALL NOT SEND ANY DATA IN ENCRYPTED FORMAT THAT MAY DIRECTLY OR INDIRECTLY COMPROMISE THE NATION'S SECURITY AND INTEREST. YOU AGREE AND ACKNOWLEDGE THAT DOHATEC-CA HAS AUTHORITY AND POWER TO REVOKE THE DIGITAL CERTIFICATE ISSUED TO YOU IF AT ANY POINT IT IS DETERMENT THAT THE INFORMATION PROVIDED IS INCOMPLETE OR INCORRECT

YOU SHALL SUBMIT YOUR PRIVATE KEY (S) TO DOHATEC-CA OR CCA ON THEIR DIRECTION OF ANY COMPETENT AUTHORITY UNDER VARIOUS LAWS AND ACTS INCLUDING THE INFORMATION AND COMMUNICATION TECHNOLOGY ACT 2006 (Amended in 2013), BECAUSE OF A DISPUTE ARISING DUE TO THE ISSUE OF A DIGITAL CERTIFICATE ISSUED BY DOHATEC-CA AND USED FOR ENCRYPTION OF ANY MATERIAL

.

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

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

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

11. Dohatec-CA Relying Party Agreement (Sample)

DOHATEC - CERTIFYING AUTHORITY
[DIGITAL CERTIFICATION SERVICES]

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

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

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

Agreement

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

Definitions

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

Certificate Practice Statement

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

Certificate Validation

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

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

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

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

You may rely upon a digital signature binding the Subscriber if

- the digital signature was created during the operational period of valid Certificate and it can be verified by cross checking a validated Certificate chain and
- such reliance is responsible under the circumstances. If the circumstances indicate a need for additional assurance, you may obtain such assurance for such reliance to be reasonable.

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

You acknowledge and accept that in providing the services as contained in the CPS, neither Dohatec-CA, Partner for whom Sub-CA has been created (Sub-CA) or Registration Authorities (RAs) shall become a party to any of the dealings or transactions entered into between yourself and the Subscriber and that the services shall be limited to certifying the digital signature of the Subscriber in accordance with the Dohatec-CA

CPS. All claims, of contractual nature or otherwise, resulting from or connected to the dealings or transactions shall be entirely between you and the Subscriber and you shall not hold Dohatec-CA or any Partner for whom Sub-CA has been created or Registration Authorities or any of their employees and representatives liable.

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

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

Exclusion of Certain Elements of Damage

IN NO EVENT SHALL ANY PARTNER FOR WHOM SUB-CA HAS BEEN CREATED OR REGISTRATION AUTHORITIES OR DOHATEC-CA BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA, OR OTHER INDIRECT, CONSEQUENTIAL, PUNITIVE DAMAGES, WHETHER OR NOT REASONABLY FORESEEABLE, ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE, NON-PERFORMANCE OR UNAVAILABILITY OF THE CERTIFICATES, DIGITAL SIGNATURES, OR ANY OTHER TRANSACTION OR SERVICES OFFERED OR CONTEMPLATED HEREIN, EVEN IF SUCH REGISTRATION AUTHORITIES , PARTNER FOR WHOM SUB-CA HAS BEEN CREATED OR DOHATEC OR BOTH HAVE BEEN ADVISED OF SUCH DAMAGES.

Damages and Loss Limitations

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

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

Liability Caps

CLASS-0 - No liability

CLASS-1 - No liability

CLASS-2 - BDT 5000<>

CLASS-3 -BDT 10000<>

Private Key Protection

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

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

Governing Laws

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

Dispute Resolution

All disputes between DOHATEC-CA/ PARTNER FOR WHOM SUB-CA HAS BEEN CREATED /RA, the Subscriber and the relying party shall be settled by negotiation failing that it will be referred for Arbitration. The Arbitration shall be guided by the laws of Bangladesh and it will be conducted by 1(one) Arbitrator to be appointed by mutual agreement.

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

Dohatec New Media ★ 43, Purana Paltan Line, Dhaka-1000 ★ Dohatec

12. Application Forms (Sample)

GLOSSARY

ACCEPT (A DIGITAL CERTIFICATE)

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

ACCESS

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

ACCESS CONTROL

Access control is the process or mechanism of limiting access to the resources of a computer system only to authorized users, programs or other computer systems.

ADDRESSEE

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

AFFIRM / AFFIRMATION

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

AFFIXING DIGITAL SIGNATURE

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

ALIAS

A pseudonym.

APPLICANT (See CA Applicant; Certificate Applicant)

APPLICATION SOFTWARE

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

APPLICATION SYSTEM

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

ARCHIVE

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

ASSURANCES

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

ASYMMETRIC CRYPTO SYSTEM

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

AUDIT

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

AUDIT TRAIL

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

AUTHENTICATED RECORD

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

AUTHENTICATION

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

AUTHORITY REVOCATION LIST (ARL)

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

AUTHORIZATION

Authorization is the process of granting of rights, including the ability to access specific information or resources.

AVAILABILITY

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

BACKUP

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

BINDING

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

CERTIFICATE

A Digital Certificate issued by Certifying Authority.

CERTIFICATE CHAIN

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

CERTIFICATE EXPIRATION

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

CERTIFICATE EXTENSION

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

CERTIFICATE ISSUANCE

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

CERTIFICATE MANAGEMENT [Management of Digital Certificate]

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

CERTIFICATE POLICY

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

CERTIFICATE REVOCATION (See Revoke a Certificate)

CERTIFICATE REVOCATION LIST (CRL)

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

CERTIFICATE SERIAL NUMBER

Certificate Serial Number is a value that unambiguously identifies a Digital Certificate generated by a Certifying Authority.

CERTIFICATE SIGNING REQUEST (CSR)

Certificate Signing Request (CSR) is a machine-readable form of a Digital Certificate application.

CERTIFICATE SUSPENSION (See SUSPEND A CERTIFICATE)

CERTIFICATION / CERTIFY

Certification is the process of issuing a Digital Certificate by a Certifying Authority.

CERTIFYING AUTHORITY (CA)

Certifying Authority (CA) is a person who has been granted a license to issue a Digital Certificate under section 25 of Information and Communication Technology Act, 2006 (Amended in 2013).

CERTIFYING AUTHORITY SOFTWARE

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

CERTIFYING AUTHORITY SYSTEM

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

CERTIFICATEPRACTICE STATEMENT (CPS)

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

CHALLENGE PHRASE

Challenge Phrase is a set of numbers and/or letters that are chosen by a Digital Certificate Applicant, communicated to the Certifying Authority with a Digital Certificate application, and used by the Certifying Authority to authenticate the Subscriber for

various purposes as required by the Certificate Practice Statement. A challenge phrase is also used by a secret shareholder to authenticate himself, herself, or itself to a secret share issuer.

CERTIFICATE CLASS

A Digital Certificate of a specified level of trust.

CLIENT APPLICATION

Client Application is an application that runs on a personal computer or workstation and relies on a server to perform some operation.

COMMON KEY

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

COMMUNICATION/NETWORK SYSTEM

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

COMPROMISE

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

COMPUTER

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

COMPUTER CENTRE (SEE DATA CENTRE)

COMPUTER DATA BASE

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

COMPUTER NETWORK

Interconnection of one or more computers through:

The use of satellite, microwave, terrestrial line or other communication media; and

terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.

COMPUTER PERIPHERAL

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

COMPUTER RESOURCE

Computer Resource means computer, computer system, computer network, data, computer database or software.

COMPUTER SYSTEM

A device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions.

COMPUTER VIRUS (SEE VIRUS)

CONFIDENTIALITY

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

CONFIRM

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

CONFIRMATION OF DIGITAL CERTIFICATE CHAIN

Confirmation of Digital Certificate Chain is the process of validating a Digital Certificate chain and subsequently validating an end-user Subscriber Digital Certificate.

CONTINGENCY PLANS

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

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

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

CONTROLS

Controls are measures taken to ensure the integrity and quality of a process.

CORRESPOND

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

CRITICAL INFORMATION

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

CROSS-CERTIFICATE

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

CRYPTOGRAPHIC ALGORITHM

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

CRYPTOGRAPHY (*See also* public key cryptography)

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

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

DAMAGE

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

DATA

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

DATA BASE (See Computer Database)

DATA CENTRE (as also Computer Centre)

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

DATA CONFIDENTIALITY (See confidentiality)

DATA INTEGRITY

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

DATA SECURITY

Data Security is the practice of protecting data from accidental or malicious modification, destruction, or disclosure.

DEMO CERTIFICATE

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

DIGITAL CERTIFICATE

Means a Digital Certificate issued under sub-section *(1)* of section 36 of the Information and Communication Technology Act, 2006 (Amended in 2013).

DIGITAL CERTIFICATE APPLICANT

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

DIGITAL CERTIFICATE APPLICATION

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

DIGITAL SIGNATURE

Digital Signature is one of the mechanisms of creating Electronic Signature. Digital Signature is a mechanism of authenticating an electronic record by a Subscriber using an electronic method or procedure in accordance with the provisions of section 4 of the Information and Communication Technology Act, 2006 (Amended in 2013).

DISTINGUISHED NAME

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

DOCUMENT

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

ELECTRONIC FORM

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

ELECTRONIC MAIL ("E-mail")

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

ELECTRONIC RECORD

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

ELECTRONIC SIGNATURE (see digital signature)

Electronic Signature means authentication of any electronic record by a Subscriber by means of an electronic method or procedure in accordance with the provisions of section 4 of the Information and Communication Technology Act, 2006 (Amended in 2013). For the sake of this CPS, Electronic Signature is referred to as Digital Signature.

ELECTRONIC SIGNATURE CERTIFICATE (see DIGITAL CERTIFICATE)

Means a certificate issued under sub-section *(1)* of section 36 of the Information and Communication Technology Act, 2006 (Amended in 2013). For the sake of this CPS, Electronic Signature Certificate is equivalent to Digital Certificate.

ENCRYPTION

Encryption is the process of transforming plaintext data into an unintelligible form (cipher text) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).

EXTENSIONS

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

FIREWALL/DOUBLE FIREWALL

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

FILE TRANSFER PROTOCOL (FTP)

File Transfer Protocol (FTP) is the application protocol that offers file system access from the Internet suite of protocols.

FUNCTION

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

GATEWAY

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

GENERATE A KEY PAIR

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

HARD COPY

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

HASH (hash function)

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

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

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

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

HIGH-SECURITY ZONE

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

IDENTIFICATION / IDENTIFY

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

IDENTITY

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

INFORMATION

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

INFORMATION ASSETS

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

INTERMEDIARY

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

INFORMATION TECHNOLOGY SECURITY

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

INFORMATION TECHNOLOGY SECURITY POLICY

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

KEY

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

KEY GENERATION

Key Generation is the trustworthy process of creating a private key/public key pair.

KEY MANAGEMENT

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

KEY PAIR

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

LICENCE

Means a license granted to a Certifying Authority.

LOCAL AREA NETWORK (LAN)

Local Area Network (LAN) is a geographically small network of computers and supporting components used by a group or department to share related software and hardware resources.

MANAGEMENT OF DIGITAL CERTIFICATE [See Certificate Management]

MEDIA

Media is the material or configuration on which data is recorded. Examples include magnetic tapes and disks.

MESSAGE

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

NAME

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

NETWORK

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

NETWORK ADMINISTRATOR

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

NODE

Node in a network is a point at which one or more functional units connect channels or data circuits.

NOMINATED WEBSITE

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

NON-REPUDIATION

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

NOTARY

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

ON-LINE

On-line is communications that provide a real-time connection.

OPERATIONS ZONE

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

OPERATIONAL CERTIFICATE

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

OPERATIONAL MANAGEMENT

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

OPERATIONAL FIELD

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

ORGANIZATION

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

ORIGINATOR

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

PASSWORD (pass phrase; pin number)

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

PC CARD (see also Smart Card)

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

PERSON

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

PERSONAL PRESENCE

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

PKI (Public Key Infrastructure) / PKI SERVER

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

PKI HIERARCHY

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

PLEDGE (See software publisher's pledge)

POLICY

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

- Introduction
- Definitions
- Policy Statement identifying the need for "something" (e.g. data security)
- Scope
- People playing a role and their responsibilities
- Statement of Enforcement, including responsibility

PRIVATE KEY

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

PROCEDURE

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

PROGRAM

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

PROXY SERVER

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

PUBLIC ACCESS ZONE

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

PUBLIC KEY

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

PUBLIC KEY CERTIFICATE (*See* Certificate)

PUBLIC KEY CRYPTOGRAPHY (*See* cryptography)

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

PUBLIC KEY INFRASTRUCTURE (PKI)

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

PUBLIC/PRIVATE KEY PAIR (See public key; private key; key pair)

RECIPIENT (of a Digital Signature)

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

RECORD

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

RE-ENROLLMENT (*See also* renewal)

RELYING PARTY

Relying Party is a recipient who acts in reliance on a Certificate and Digital Signature.

RENEWAL

The process of obtaining a new Digital Certificate of the same class and type for the same subject once an existing Digital Certificate has expired. Certificate renewal is always treated as re-key.

REPOSITORY

Repository is a database of Digital Certificates and other relevant information accessible on-line.

REPUDIATION (*See also* non-repudiation)

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

REVOKE A CERTIFICATE

Revoke a Certificate is the process of permanently ending the operational period of a Digital Certificate from a specified time forward.

RISK

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

RISK ANALYSIS

Risk Analysis is the process of identifying security risks, determining their magnitude, and identifying areas needing safeguards.

RISK ASSESSMENT

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

RISK MANAGEMENT

Risk Management is the total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect information technology system resources.

RSA

RSA is a public key cryptographic system invented by Rivest, Shamir & Adelman.

SECRET SHARE

Secret Share is a portion of a cryptographic secret split among a number of physical tokens.

SECRET SHARE HOLDER

Secret Share Holder is an authorized holder of a physical token containing a secret share.

SECURE CHANNEL

Secure Channel is a cryptographically enhanced communications path that protects messages against perceived security threats.

SECURE SYSTEM

Means computer hardware, software, and procedure that—

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

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

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

(d) Adhere to generally accepted security procedures.

SECURITY PROCEDURE

Means the security procedure prescribed under section 17 of the Information and Communication Technology Act, 2006 (Amended in 2013) for the purpose of:

verifying that an electronic record is that of a specific person;
detecting error or alteration in the communication, content or storage of an electronic record since a specific point of time, which may require the use of algorithms or codes, identifying words or numbers, encryption, answer back or acknowledgement procedures, or similar security devices;

SECURITY

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

SECURITY POLICY

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

SECURITY SERVICES

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

SECURITY ZONE

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

SERIAL NUMBER (*See* Certificate serial number)

SERVER

Server is a computer system that responds to requests from client systems.

SIGN

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

SIGNATURE (*See* Digital Signature)

SIGNER

Signer is a person who creates a Digital Signature for a message or a Signature for a document.

SMART CARD

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

S/MIME

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

SUBJECT (of a Certificate)

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

SUBJECT NAME

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

SUBSCRIBER

A person in whose name the Digital Certificate is issued.

SUBSCRIBER AGREEMENT

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

SUBSCRIBER INFORMATION

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

SUSPEND A CERTIFICATE

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

SYSTEM ADMINISTRATOR

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

SYSTEM SECURITY

System Security is a system function that restricts the use of objects to certain users.

SYSTEM SOFTWARE

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

TEST CERTIFICATE

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

THREAT

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

TIME-OUT

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

TIME STAMP

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

TOKEN

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

TRANSACTION

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

TRUST

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

TRUSTED POSITION

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

TRUSTED ROLES

Trusted role is assigned to a person holding a trusted position. The following are the trusted roles in Dohatec-CA Trust Network:

- Certifying Authority – Senior Management of Dohatec New Media who is recognized as the CA.
- CA Administrator – The CA Administrator is the manager of the CA operations
- CA Operator – Appointed by CA Administrator to perform delegated operations of CA Administrator (This is an optional role and may be used when required).
- Sub-CA Administrator – Manages the operations for the Partner for whom the Sub-CA has been created.
- RA Administrator – Appointed by the RA to perform the RA Operations as defined in this CPS.
- RA Operator – Appointed by the RA to perform delegated operations of RA Administrator (This is an optional role and may be used when required).

TRUSTED THIRD PARTY

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

TRUSTWORTHY SYSTEM

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

TYPE (of Certificate)

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

UNAMBIGUOUS NAME (*See* distinguished name)

UNIFORM RESOURCE LOCATOR (URL)

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

USER

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

VALID CERTIFICATE

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

VALIDATE A CERTIFICATE (*i.e.,* of an end-user Subscriber Certificate)

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

VALIDATION (of Certificate application)

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

VALIDATION (of Software) (*See* software validation)

VERIFY (A Digital Signature)

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

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

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

VIRUS

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

VULNERABILITY

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

WEB BROWSER

A software application used to locate and display web pages.

WORLD WIDE WEB (WWW)

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

WRITING

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

X.509

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

DOHATEC NEW MEDIA

DOHA HOUSE 43, PURANA PALTAN LINE

DHAKA – 1000, BANGLADESH

PHONE: +880 2 934 8119, 934 1003

CELL: +880 1678 625336

FAX : +880-2-956 9326

EMAIL: dohatec@bol-online.com

WEBSITE: www.dohatec.com

www.dohatec-ca.com.bd

Dohatec