e-Sign Guideline for the Certifying Authorities (CAs), 2020

Version 2.0

10.06.2026

CCA

নিয়ন্ত্রক সনদ কর্তৃপক্ষের প্রধানকার্যালয় কর্তৃপক্ষের নিয়ন্ত্রক-এর কার্যালয়

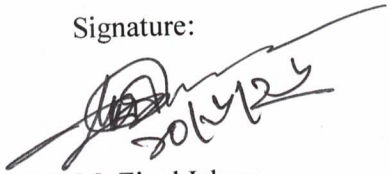
Office of the Controller of Certifying Authorities
Information & Communication Technology Division
Ministry of Posts, Telecommunications and Information Technology

Classification: Public

Document Reference

Document Title	**e-Sign Guideline for the Certifying Authorities (CAs), 2020**
Document Type	**Public**
Previous Version	**1.0.1**
Previous Version Revise Date	**24 November 2020**
Release Date	**10 June 2026**
Version	**2.0**
Pages	**39**
Status	**Approved**
Document Owner	**Controller, Office of the Controller of Certifying Authorities (CCA), Bangladesh.**

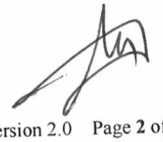
Signature:



A.T.M. Ziaul Islam

Controller

Controller of Certifying Authorities



Document Change Control

Version	Date	Reason for issue	Issued By	Reviewed by
1.0	20/10/2020	To introduce e-Sign Service in Bangladesh	Office of the CCA	CA
1.0.1	24/11/2020	To implement e-Sign in Bangladesh	Office of the CCA	CCA
2.0	10/06/2026	To implement e-Sign in Bangladesh	Office of the CCA	CCA

Table of Contents

1. Executive Summary

If a nation holds a clear vision, that vision can guide its path and drive its realization. In Bangladesh, this aspiration has translated into a sustained journey toward a technology-driven society, with digital transformation at the core of national development. This journey formally began with the adoption of the National ICT Policy, 2002, which established a comprehensive framework for developing skilled human resources, expanding ICT infrastructure, promoting e-governance, encouraging private sector participation, strengthening the legal and regulatory environment, boosting ICT exports, and ensuring broader access to information. Building on this policy foundation, the government enacted the Information and Communication Technology Act, 2006 to legitimize digital activities, enhance cybersecurity, and institutionalize the country's digital transformation agenda through proactive leadership in policy formulation, legislative development, and regulatory implementation. In furtherance of this legal framework, the Office of the Controller of Certifying Authorities (CCA) was instituted in 2011 as an attached office under the Information and Communication Technology Division of the Ministry of Posts, Telecommunications and Information Technology, Government of the People's Republic of Bangladesh, to operationalize and oversee the nation's digital certification infrastructure.

Since its inception, the Office of the Controller of Certifying Authorities (CCA) has played a key role in this journey by developing the necessary rules and guidelines for Public Key Infrastructure (PKI), establishing the Root CA infrastructure, and completing the license issuance process for Certifying Authorities (CAs). All licensed CAs in Bangladesh are working to create awareness about the importance and benefits of electronic transactions and digital signatures. While collaborating with other agencies to promote PKI adoption, most CAs have identified several important opportunities for improvement, including simplifying the use of digital signatures in applications, streamlining the digital signature certificate enrollment process, enhancing mobility, and enabling secure signing capabilities from anywhere and on any device.

To overcome this complexity, the global phenomenon is to use PKI-based remote signing solutions. They have become widely accepted due to their simplicity, ease of use, and security. They are also known as e-Sign or Cloud Sign, or Remote Signature. In Bangladesh, the Information and Communication Technology Act, 2006 has made electronic signatures legally valid. Subsequently, as per the ICT Act, 2006 and the Information Technology (Certifying Authorities) Rules, 2010, the CCA issued Certifying Authority (CA) licenses to credible organizations for the implementation of electronic signature certificates and related activities. The Information and Communication Technology Act, 2006 and the Information Technology (Certifying Authorities) Rules, 2010 do not define the types of electronic signatures or the processes. They provide an outline stating that the types of electronic and digital signatures, the process of issuance, application, and total lifecycle management will be defined through the CCA-approved Certification Practice Statement (CPS) of the CA. e-Sign is a form of electronic signature and shall be implemented following the CCA-approved CPS of the CA. All operational issues related to the e-Sign lifecycle management would be included in the CCA-approved CPS of the CA.

Considering the huge necessity of easy-to-use electronic signatures under the existing legal framework, the CCA intends to set guidelines for CAs to provide e-Sign to subscribers.

This document is issued under Section 19(b) and 19(d) of the Information and Communication Technology Act, 2006 and Rule 7 of the Information Technology (Certifying Authorities) Rules, 2010. It lays down the standards to be adhered to by all licensed CAs in providing e-Sign services to subscribers.

2. Definition

API: An application programming interface (API) is a computing interface that defines interactions between multiple software intermediaries. It defines the kinds of calls or requests that can be made, how to make them, the data formats that should be used, the conventions to follow, etc.

Biometric Personal Information: Physical and biological information of any person, such as fingerprints, eye retinas and irises, voice patterns, etc.

Business Application Owner: The owner of the business application software or application who is contractually obliged to let the CAs to use the platform provide e-Sign services to the e-Sign Subscribers as per law.

Certification Practice Statement (CPS): Certification Practice Statement (CPS) is submitted by the licensed Certifying Authorities (CAs) under Rule 21(a) of the Information Technology (Certifying Authorities) Rules, 2010 and approved by CCA.

Certifying Authority (CA): "Certifying authority" means a person or authority who has been granted a license under section 18 of the Information and Communication Technology Act, 2006 to be read with section 22 of this Act to issue an Electronic Signature Certificate:

Controller of Certifying Authorities (CCA): Controller of Certifying Authorities (CCA) means the Controller of Certifying Authorities appointed under sub-section (1) of section 18 of the Information and Communication Technology Act, 2006.

e-KYC: Electronic Know Your Customer (e-KYC) is an electronic automated method used to verify and authenticate the identity of an e-Sign Subscriber as defined in Rule 2(j) of the Information Technology (Certifying Authorities), Rules 2010.

e-KYC Service: Identity Verification service provided by CAs as per Rule 24 (e) of the Information Technology (Certifying Authorities) Rules, 2010.

e-Seal: Digital equivalent of a physical seal, applied by a legal entity (such as a company or organization) to a document to assert its origin, integrity, and legal identity.

e-Sign: A form of electronic or digital signature provided and certified by Certifying Authorities (CAs) in accordance with Clause 2(1) of the Information and Communication Technology Act, 2006, and the Information Technology (Certifying Authorities) Rules, 2010, where the user's private key is stored on the e-Sign Service Provider CA's end, while the user retains sole control over it through an appropriate ecosystem.

e-Sign Service Provider (ESP): The CAs and their Sub-CAs Licensed by CCA can provide e-Sign Service under section 2 (32) and 2(34) of Information and Communication Technology Act, 2006 and as per the Rule 21 of Information Technology (Certifying Authorities) Rules, 2010.

e-Sign Subscriber: A person or individual who uses e-sign to sign any electronic record, electronic content & electronic document.

KYC: Know Your Customer (KYC) refers to the regulatory and procedural framework established for verifying and authenticating the identity of a customer, in accordance with applicable financial, legal and compliance standards. The process encompasses the collection and validation of identification details, documents, and background information of the customer, as may be prescribed by relevant regulatory authorities from time to time.

Person: "person" shall include an individual; or a company or association or body of individuals: whether incorporated or not and shall also include any governmental authority having knowledge of the issuance of an electronic signature certificate.

Personal Information: Information relating to any person, by which he or she may be directly or indirectly identified (e.g., biometric information).

Relying Party: Relying Party refers to an individual, organization, or system that relies on a digital certificate or electronic credential issued by a Certifying Authority (CA) to verify the identity of a user, system, or entity in digital transactions.

X-509 Certificate: An X. 509 certificate binds an identity to a public key using digital signature. A certificate contains an identity (a hostname, or an organization, or an individual) and public key (RSA, DSA, ECDSA, ed25519. etc.), and is signed by a certificate authority.

3. Background

Bangladesh has taken a large number of digital initiatives in recent years. Many e-government and e-business applications have been built to make customer's lives easier. Digital signatures are an essential government initiative that electronically bridges the government with private individuals and connects government agencies and bodies.

To regulate the digital signature system in Bangladesh, the Office of the Controller of Certifying Authorities (CCA) was established in May 2011 under the Information and Communication Technology Act, 2006, within the Information and Communication Technology Division under the Ministry of Posts, Telecommunications & Information Technology. Section 8 of the Information and Communication Technology Act, 2006 mandates that the use of electronic signatures and records shall be recognized in all government offices. Currently, there are

multiple licensed Certifying Authorities (CAs) in Bangladesh, which have been providing digital signature services since 2013.

The existing digital signature framework in Bangladesh, operated by licensed Certifying Authorities under the Office of the Controller of Certifying Authorities, has established a foundational Public Key Infrastructure for secure electronic transactions. However, the current digital signature scheme, which relies on in-person physical presence, paper-based identity and address verification, the issuance of hardware-based cryptographic tokens, and custom driver software, does not scale to a hundred million plus people in Bangladesh. But for offering fully paperless and secure citizen services, mass adoption of digital signatures is necessary. A simple-to-use online service is required to allow everyone to digitally sign electronic documents.

4. Objectives

The objectives of these guidelines are to:

a) Introduce e-Sign service in Bangladesh under the applicable laws and regulations;

b) Provide an outline of e-Sign framework for Bangladesh;

c) Guide and set Standard for the licensed CAs to implement e-Sign Service as e-Sign Service Provider (ESP);

d) Assist licensed CAs to establish the e-KYC platform for e-Sign;

e) Assist licensed CAs to establish KYC procedure for organizations;

f) Provide necessary information regarding e-Sign (X.509) certificates;

g) Provide necessary guidance to ESP (CAs), business application owners, e-KYC service providers, e-Sign Users, and relying parties to comply with regulatory requirements;

h) Create awareness, build confidence, and promote the use of PKI-based e-Sign in business transactions;

i) Define the scope and take effective steps to incorporate e-Seal within PKI framework.

5. Scope

This guideline is issued by the Office of the CCA and applies to all licensed CAs under the Information and Communication Technology Act, 2006, owners of business applications, e-Sign users, e-KYC providers, Empaneled Auditors of the Office of the CCA, and other relying parties involved in the process.

6. e-Sign Overview

e-Sign is an easy-to-use online electronic signature and digital signature service that can be integrated with service delivery applications via an API to facilitate users to digitally sign electronic content, records, files, applications, or documents instantaneously. In e-Sign, the cryptographic key pair is generated and stored securely on the ESP's server side and is kept under the 'sole control' of the signer using multifactor authentication, encryption, and tamper-resistant hardware. The signing process happens completely remotely after the user gives consent and authenticates through OTP/QR/PIN/biometric triggers.

Since all complexities of securely storing keys and performing signing operations are handled on the server side of the ESP, the proposed solution does not require any additional device on the user's side except a computer,

mobile phone, or tablet with a web browser. e-Sign can be integrated with service delivery applications via an API to facilitate users to digitally sign documents. Anything in this document in contradiction with the Information and Communication Technology Act, 2006 and Information Technology (Certifying Authorities) Rules, 2010 or/and any Laws of the Land, shall have no legal effect.

7. e-Sign Classification & Applicability

As mentioned earlier, there could be different variants of e-Sign depending mainly on the following properties:

a) The verification method (any combination, multifactor authentication)

i. Mobile (MSISDN) OTP or E-mail OTP with Face matching

ii. Mobile (MSISDN) OTP or E-mail OTP with Biometric (Fingerprint or other) matching

iii. Mobile (MSISDN) OTP or E-mail OTP with Biometric (Face/Fingerprint/Iris) matching or live e-KYC session

b) Certificate validity:

i. Short validity e-Sign: Short validity (destroyed after first use)

ii. Long validity e-Sign: Long validity (1-2) Years)

c) Authorization method:

i. PIN & OTP (MSISDN & email based)

ii. Mobile or other applicable Device Authorization Key

Depending on these different parameters, there will be two classes of e-Sign certificate in Bangladesh, which can be modified as and when needed by the Office of the CCA:

a) Short validity **e-Sign**

Short validity e-Sign will be of short validity certificate and the identity verification shall be only Mobile (MSISDN) or E-mail OTP and Face matching based. The e-Sign subscriber can choose any of the authorization methods available. The face identified for verification shall be 80% matched with the NID photo whereas other demographic information (e.g. name) has to be 100% matched with NID database.

b) Long validity **e-Sign**

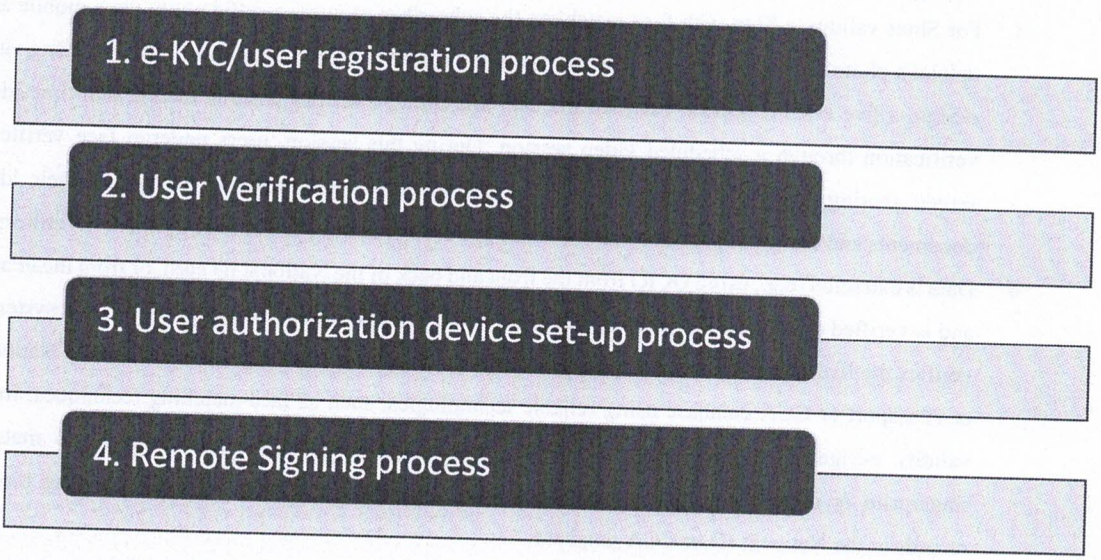
Long validity e-Sign can be of long/short validity certificate, and the identity verification must be completed through live e-KYC session, biometric verification, and Mobile (MSISDN) or email OTP. The e-Sign subscriber can choose any of the authorization methods available.

Property	Short validity e-Sign	Long validity **e-Sign**
Required Data from E-Sign subscriber	· Front and Rear part of NID Card · Live Photo · Mobile Number · Email Address	· Front and Rear part of NID Card · live e-KYC session · Mobile Number · Email Address
Identity Verification Method	· Face Recognition (>80%) · Demographic Data Verification (>80%) · NID number and Date of Birth matching (100%) · Mobile Number or email (with OTP)	· Biometric (Face/Fingerprint/Iris) · Demographic Data Verification (>80%) · NID number or ePassport number or Date of Birth matching (100%) · Mobile Number or email (with OTP)
Certificate Validity	Short (one time use)	Long (1-2) Years)
Signature Authorization Method	PIN and OTP or with Authorized Device	PIN and OTP or with Authorized Device
Enrollment Platform	· Mobile Apps · Web based application · Physical CA enrollment center direct e-Sign portal or interface	Mobile Apps or Web based platform supporting live e-KYC session

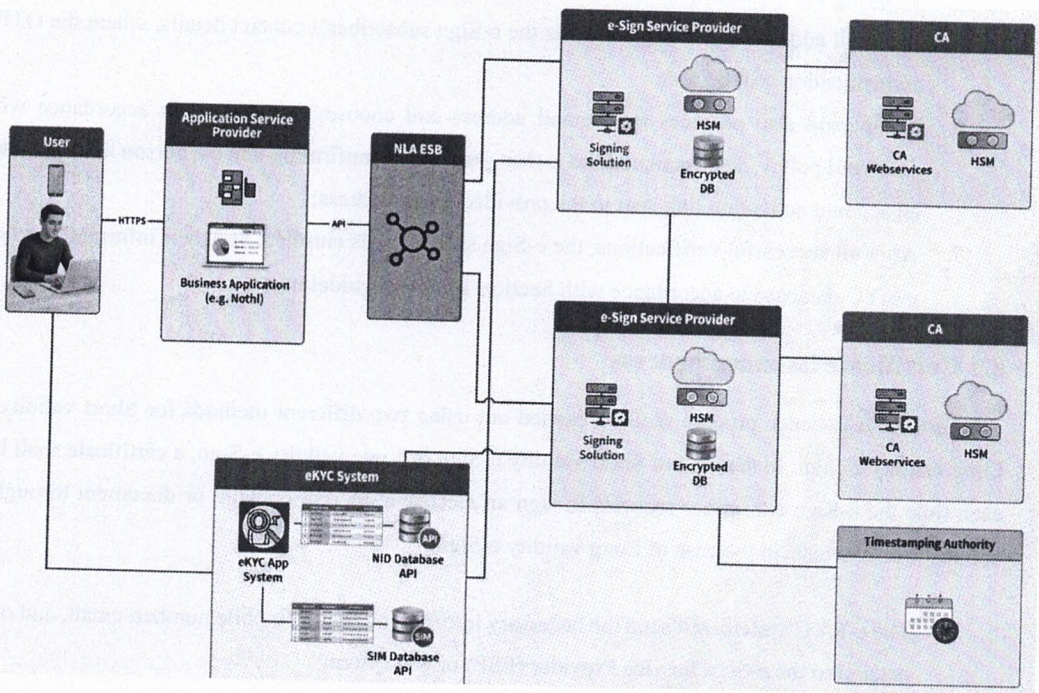
Depending on these types Office of the CCA will publish notification about the application area of e-Sign from time to time. Initially, all CA can start with Short validity e-Sign immediately, later they can start rolling out Long validity e-Sign version. However, there is no restriction by Office of the CCA on starting both from the beginning or providing only any of these e-Sign types.

8. e-Sign Service Framework

The whole e-Sign process flow can be broken down into 4(four) parts, they are described in more detail in the following sections of this document. The major 4 parts are:



These 4 parts follow the below process flow which is described in the later section of this document, this process flow is applicable for all type of e-Sign certificates/profile:



8.1 e-Sign subscriber e-KYC/enrolment process

1. e-Sign subscriber downloads and open the e-Sign mobile app or accesses e-KYC portal from any browser or following from CA enrolment centre using direct e-Sign interface;
2. e-Sign subscriber captures the front and rear part of the National ID card or ePassport and upload it through e-Sign mobile app/web based application or through direct CA interface;
3. For Short validity e-Sign with face matching, the subscriber captures a selfie photo via a mobile app or upload a photo through a browser or at an enrolment center equipped with a webcam. For Long validity e-Sign, a live e-KYC session between the user and the CA verifier ensures secure, real-time identity verification through a scheduled video session. During this session, users undergo face verification, screen sharing, and OTP validation. e-Sign subscribers are also required to upload their identity documents and complete profile creation, which are cross-checked in real time by the CA verifier;
4. Data is extracted (e.g., using OCR) from the front and back of the National ID card, or from the ePassport and is verified against the National ID database or the CCA database. In case of e-Sign, the system also verifies the live selfie of the subscriber by matching it against the photograph stored in the National ID or ePassport or CCA database using reliable technologies, such as face-matching techniques. In Long validity e-Sign, the system may additionally use machine learning–based methods to match the fingerprint or other biometric data provided by the subscriber against the corresponding biometric records in the National ID or CCA database;
5. The user is prompted to provide their mobile number and e-mail address. Mobile number and e-mail address verification will be performed through OTP and, optionally, through the SIM registration database. The e-Sign subscriber or user shall be fully responsible for the validity, authenticity, and ownership of the provided mobile number and e-mail address. The CA or CCA shall not be liable for verifying the ownership of these mobile numbers or e-mail addresses. This mobile number (MSISDN) or e-mail address will be registered as the e-Sign subscriber's contact details, where the OTP for e-Sign authentication will be sent;
6. The person also provides their email address and chooses a password in accordance with a strong password policy. The email address is then verified by confirming that the person has access to it through an account activation link sent to the provided email address;
7. After all successful verifications, the e-Sign subscriber is enrolled, and their information is stored in the e-KYC database in accordance with Section 10 of this guideline.

8.2 Certificate issuance process

The certificate issuance process shall be carried out using two different methods for Short validity e-Sign and Long validity e-Sign. In the case of Short validity e-Sign or Long validity e-Sign, a certificate shall be generated each time the e-Sign subscriber requests to sign an electronic record, content, or document through a business application. Whereas, in the case of Long validity e-Sign,

1. The e-KYC system will send the necessary information (name, mobile number, email, and other relevant details) to the e-Sign Service Provider (ESP) or CA system.

2. The CA/ESP system will request the HSM to generate a key pair and return a PKCS#10 CSR or any applicable format in accordance with the CA Rules 2010 and the CA CPS.
3. The private key is exported from the HSM using an HSM Key Encryption Key (KEK) and stored as an encrypted Binary Large Object (BLOB) in the CA database or in another appropriate secure system under the sole control of the e-Sign subscriber. It shall remain encrypted when not in use.
4. The e-Sign Service Provider (ESP), as part of the CA system, then sends the CSR to the CA system for issuance of the certificate for the respective CSR.
5. The CA system then issues an electronic certificate or digital certificate for the user and sends it back to the ESP system of the CA.
6. The ESP system stores the certificate in the database for the corresponding user in an appropriate manner, in accordance with the Information Technology (Certifying Authorities) Rules, 2010 and the CA CPS.

8.3 e-Sign Subscriber authorization device set-up process

The e-Sign subscriber may authorize their mobile device using an application provided by the CA (ESP of the CA), such that authorization responses only from that device will permit the CA/ESP system to create signatures on behalf of the e-Sign subscriber. This is an optional process; the e-Sign subscriber may choose to use it or opt for an alternative method. Another convenient approach is for the CA/ESP system to send an OTP to the subscriber's registered mobile number (MSISDN) or email address prior to signature creation. The e-Sign subscriber then provides a secure PIN and OTP to authorize the transaction. In such cases, setting up a dedicated authorization device becomes unnecessary. The following process applies if the e-Sign subscriber chooses to use a mobile device as the authorization device:

1. In the mobile app, when the e-Sign subscriber first attempts to log in using their email address and password (set up during the initial user registration process), the app detects that it is being used for the first time and prompts the subscriber to confirm that they wish to register the device for remote signing purposes. If the subscriber confirms, the app sends a device registration request to the e-Sign Service Provider's backend. Alternatively, e-Sign subscribers may enable device authorization at any time;
2. The e-Sign Service Provider ESP/CA sends an OTP to the email address and mobile phone number (MSISDN) provided by the e-Sign subscriber;
3. After OTP-based authentication by the e-Sign subscriber, the ESP mobile app creates an authorization key pair within the mobile device's tamper-protected Secure Element or Secure Enclave hardware chip;
4. The e-Sign mobile app creates a CSR for the authorization public key and sends it to the ESP backend, along with the device's hardware fingerprint;
5. The ESP/CA certifies the authorization key using its internal or external CA and stores the authorization certificate;
6. The ESP links the subscriber's authorization certificate and device fingerprint with their qualified certificate and stores this information in the e-Sign subscriber's account. This information is protected using cryptographic checksums;

7. The ESP notifies the e-Sign mobile app that the device is now registered for signing authorization purposes.

8.4 Remote Signing Process

The following steps happen during the remote signing process:

1. . An enrolled e-Sign subscriber can access the business application from any device supported by the application;
2. The e-Sign subscriber sends signing request to business application;
3. The business application shall forward the signing request to the CA/ESP system, along with the subscriber's unique identification information, the hash of the document or data to be signed, the application ID, and any other required information;
4. The CA/ESP system shall create a signature on behalf of the e-Sign subscriber as follows:
   a. For signing with Long validity e-Sign, the CA/ESP shall create the signature upon confirmation from the user through a tamperproof device authorization mechanism or through OTP and PIN authentication;

   b. For signing with Short validity e-Sign:

   i. The CA/ESP system shall generate the appropriate key pair and submit a PKCS#10 Certificate Signing Request (CSR) to the CA system;
   ii. The CA system shall issue a certificate for the CSR and return it to the ESP system;
   iii. The ESP system shall create the signature upon obtaining user confirmation through a tamper-proof device authorization mechanism or via OTP and PIN authentication;

5. The CA/ESP system shall forward the generated signature to the business application;
6. The business application owner shall attach the signature to the respective data or document.

9. The Role of the Certifying Authority (CA) acting as a e-Sign Service Provider (ESP)

The following are the roles of CA as the e-Sign Service Provider (ESP):

1. CCA-licensed CAs shall automatically operate as ESP;
2. Licensed CAs shall apply for CPS approval to the Office of the CCA by incorporating e-Sign-related practice information into their existing CPS.
3. In accordance with the e-Sign Guidelines, other relevant guidelines or directives issued by the Office of the CCA, and the approved CPS, the licensed CA shall operate as an ESP;
4. Licensed CAs shall implement the e-Sign service facility in accordance with the prescribed e-Sign framework outlined in this guideline;
5. Licensed CAs shall develop an e-KYC platform, which shall be integrated with their e-Sign platform to onboard e-Sign subscribers;
6. Licensed CAs shall enter into an agreement with the Business Application Owners describing the nature of the business application and the services the Business Application Owners provide to facilitate CAS in performing its role as an ESP;
7. Licensed CAs shall assist business application owners in integrating their applications with the e-Sign platform through APIs and other applicable means;

8. Licensed CAs shall comply with all regulatory requirements of the Office of the CCA in their capacity as both a CA and an ESP; and
9. Licensed CAs shall comply with any other directives issued by the Office of the CCA from time to time.

10. e-KYC service

Licensed CA shall develop its own e-KYC front-end platform to provide authentication services for e-Sign subscribers. The front-end e-KYC system developed by each CA shall not store any sensitive personal data (e.g., biometric data). Only the following demographic data may be stored by a Licensed CA to issue certificates and provide authorization services for e-Sign:

1. NID Number
2. Full Name of the e-Sign user
3. Date of birth
4. Mobile Number (MSISDN)
5. Email Address
6. Hash of the Password/PIN

As an ESP, a licensed CA may also securely store the following user information in the ESP database, as prescribed by the Office of the CCA:

1. Device Fingerprint (if device authorization is chosen)
2. Public Certificate of the device (if device authorization is chosen)
3. Generated Key pair of the e-Sign subscriber
4. e-Sign Certificate of the e-Sign subscriber
5. Video of the live e-KYC session

Any sensitive information (e.g., fingerprint) captured during the onboarding of an e-Sign subscriber through the e-KYC system must not be stored by the CA. Such sensitive information shall be used only during the identity verification process, regardless of whether the verification is successful or unsuccessful.

The e-KYC system must comply with the event logging and storage procedures described in Section 16.

The ESP and the front-end e-KYC system must take reasonable security measures to protect user data and shall comply with the relevant laws and regulations of the Government of Bangladesh.

The e-Sign service provider may choose any of the following verification service providers to verify an e-Sign subscriber:

a) National Identity Registration Wing, Election Commission;
b) CCA database;
c) Any other trusted database authorized by the CCA, where identity verification has been conducted with

reasonable assurance and confidence (e.g., bank customer databases, BTRC database, BNDA Service Bus, BCC, etc.);

d) Any other entity authorized by the CCA with formal written permission.

While selecting an e-KYC verification service provider, the CA ESP must ensure that the connectivity between the provider and the CA ESP is private and encrypted. Furthermore, the e-KYC verification service provider must maintain a record of all transactional requests from each ESP and provide this information to the Office of the CCA as required. The CCA may update the list of trusted verification service providers from time to time.

11. The Role of Business Application Owner

The business application owner is the owner of the business application who intends to integrate their business application (s) with the e-Sign platform to enable e-Sign in their business transactions and documents. The Business Application Owner shall enter into a legal agreement with the e-Sign service provider, in accordance with this guideline, prior to onboarding for the e-Sign service. The prescribed format of the agreement is set forth in Annexure A. The following are the responsibilities of a Business Application Owner:

a) Complete the onboarding process to use e-Sign in their business application in accordance with this guideline.

b) Assist in integrating their business application with the CA's ESP system through APIs.

c) Ensure the security of all communications with the CA's ESP system.

d) Ensure that the document or data to be signed is displayed to the e-Sign subscriber (e.g., through a WYSIWYS feature or other suitable mechanisms).

e) Ensure that all requests sent to the CA's ESP system are digitally signed using a certificate issued by a licensed CA.

f) Provide a facility to verify the signature at any time through the CA's system.

g) Securely store and maintain all e-Sign-related event logs and information required for audit purposes.

h) Comply with any other responsibilities as prescribed by the Office of the CCA.

12. The Role of e-Sign Subscriber

e-Sign subscribers are the users of a business application integrated with a CA/e-Sign Service Provider (ESP). Before having the signing service capability, e-Sign subscribers have to go through the registration process to prove their identity and register a mobile number (MSISDN) and/or email address for subsequent use. e-Sign subscribers have the following roles (not limited to):

a) e-Sign subscribers must choose the e-Sign type, verification process, and authorization process;

b) e-Sign subscribers must agree with the terms and conditions of having the e-Sign service;

c) e-Sign subscribers must abide by all regulatory requirements and relevant laws, regulations, and guidelines;

d) E-Sign subscriber must check and confirm each document represented to them before giving final consent for signing;

e) e-Sign subscribers must keep their confidential information (PIN/Passphrase/Password etc.) within their custody and must not impersonate another e-Sign subscriber;

f) Must comply with other regulatory directives provided by the Office of the CCA;

g) e-Sign subscribers must keep the registered mobile phone number (MSISDN) and email address in their own possession. The CA or CCA does not have any control over the e-Sign subscribers' mobile or email address and shall not be liable for any misuse in any form;

h) e-Sign subscribers must report to the CA in case of loss of the registered mobile number (MSISDN) or a hacked email account or address as per the CPS policy of the CA. They must register a new mobile number (MSISDN) and email through the same formalities as registering and authenticating for the first time for their own safety.

13. e-Sign Security

ESP/CAs shall describe all the security practices in their respective CPS and get formal approval from CCA. Following are the security measures (not limited to) which shall be adopted by the different stakeholders of the e-Sign framework:

a) The communication between business application and CA/ ESP should be secured with reasonable security measures;

b) The communication between e-KYC DB and CA/ ESP should be secured with reasonable security measures;

c) Key pair shall be created inside a secured device as per the Information Technology (Certifying Authorities), Rules, 2010 and CCA approved CPA of the CA (for example, FIPS 140-2 level-3 certified HSM (Hardware Security Module));

d) The key pair, although held centrally by the e-Sign Service Provider (ESP), should be in the sole control of the user with a high degree of confidence. For long-validity certificate it is highly recommended and globally accepted to adopt the following two technical standards for achieving this:

i) EN 419241-1 (2018) Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements;

ii) EN 419241-2 (2017) Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing.

EN 419241-1 describes two levels of assurance for sole control

(1) Sole Control Assurance Level 1 (SCAL1) for short validity e-Sign

(2) Sole Control Assurance Level 2 (SCAL2) for long validity e-Sign

EN 419241-2 defines a detailed set of security requirements that must be implemented to meet the sole control assurance required for remote signatures.

e) CA\ ESP, business application & e-KYC system- should deploy trustworthy systems and employ trusted personnel;

f) There should be a system for revoking certificates through standard CRL and OCSP if the validity of the certificates is longer (1 year). If ESP implements shorter-lived certificate, there is no need to keep a system for revoking certificates through standard CRL and OCSP.

g) Audit logs should be made tamper-proof and its access should be made highly restricted.

h) To ensure long term validation of signature, ESP or Business Application Owner can use timestamp response from a trusted Time Stamping Authority according to the Time Stamping Service Guideline for Cas, 2020 issued by Office of the CCA;

i) The e-Sign user key generation and certificate management systems of CA ESP may be separate from existing CA systems for issuing e-Sign subscriber's certificates.

14. Certificate and Key Lifecycle Management

If the ESP chooses to implement longer time validity for the certificate and key, then the validity of the certificate shall not be more than 2 years, and keys will be preserved for 2 years. In this model, the ESP should adhere to EN 419241-1 & EN 419241-2 or other suitable standards for ensuring the security of the key.

If the ESP chooses to implement shorter time validity for the certificate and key, then the validity of the certificate shall not be more than 30 minutes, and keys shall be destroyed after one-time use. The certificate profile for e-Sign will be according to interoperability guidelines.

15. e-Sign Interoperability

To ensure interoperability of the e-Sign certificate, each CA shall prepare an e-Sign certificate profile according to the Digital Certificate Interoperability Guideline issued by the Office of the CCA. To make the business application interoperable, all CAs shall follow the same API specification to be issued by the Office of the CCA.

16. Standard & Compliance

The stakeholders under this guideline must comply with the following laws, rules, and regulations (not limited to):

a) Information and Communication Technology Act, 2006

b) Information Technology (Certifying Authorities) Rules, 2010

c) Digital Certificate Interoperability Guideline (IOG)

d) Respective Certification Practice Statement (CPS)

e) PKI Auditing Guidelines

f) Cyber Security Act, 2026

g) Data Privacy & Protection Rules

h) Time Stamping Services Guidelines for Certifying Authorities

i) And any other laws/rules/directives/notification published by the Office of the CCA or by the Government of the People's Republic of Bangladesh.

17. Event Logging Procedure

ESPs, Business Applications, and e-KYC systems must maintain event logs in accordance with the ISO 27001 standard. In addition, there are certain e-Sign–specific events for which all these parties must keep event logs. At a minimum, each audit record shall include the following information (either recorded automatically or manually for each auditable event):

1. The type of event,
2. The date and time the event occurred,
3. The success or failure of the event, where applicable, and
4. The identity of the entity and/or operator that caused the event.

The following events shall be audited:

17.1 CA ESP Event Logging

The following events shall be logged by the CA ESP:

a) Generation of a signing key pair for the e-Sign subscriber;

b) Deletion of the key pair;

c) Retrieval of the e-Sign subscriber's signing private key for use;

d) Transfer of the e-Sign subscriber's signing private key to encrypted storage;

e) All e-KYC requests sent to the e-KYC system and the responses received from the e-KYC system;

f) All e-Sign requests received from business applications;

g) Proof of the e-Sign subscriber's consent for signing (OTP or signature using an authorization key);

h) Generation of a CSR based on the information received from e-KYC;

i) Signature generation for the submitted hash/document;

j) All communications with the CA in respect of certification.

17.2 Business Application Event Logging

The following events/data shall be logged by business application:

a) Business application sending signing request to ESP

b) Business application receiving response of signing from ESP

c) Hash of the document to be signed

d) Signed hash of the document

e) Application ID

17.3 e-KYC Event Logging

The following events shall be logged by the e-KYC system:

a) ESP sending e-KYC request to e-KYC system

b) e-KYC system sending e-KYC response to ESP

The minimum retention period for ESP archive data shall be according to the ICT Act, 2006 and IT (CA) Rules, 2010. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined. Applications required to process the archive data shall also be maintained for the minimum retention period specified above. Audit logs should be made tamper-proof so that no one can easily change it.

18. Audit Procedure

The audit framework for the Electronic Signature Provider (ESP), Business Application, and e-KYC System shall encompass a comprehensive assessment of compliance with the security, operational, and regulatory requirements prescribed under the applicable laws, standards, and guidelines.

All security controls specified in **Section 13** shall be subject to detailed verification during the audit process to ensure their effective implementation and ongoing operational effectiveness. Similarly, the audit shall assess compliance with the event logging and monitoring requirements stipulated in **Section 16**, including the adequacy, integrity, retention, and protection of audit logs.

To maintain a robust security posture, the ESP shall conduct Vulnerability Assessments (VA) on a quarterly **basis** and Vulnerability Assessment and Penetration Testing (VAPT) annually through qualified and independent

assessors. The results, findings, remediation status, and supporting evidence of such assessments shall be made available for review during the annual external audit.

In addition to the above requirements, the ESP, Business Application, and e-KYC System shall demonstrate compliance with all relevant regulatory and technical frameworks, including but not limited to:

- ISO/IEC 27001 Information Security Management System (ISMS) Standard;
- PKI Auditing Guidelines;
- Digital Certificate Interoperability Guidelines;
- Information Technology (Certifying Authorities) Rules, 2010;
- Applicable empanelment terms and conditions issued by the Controller of Certifying Authorities (CCA); and
- Any other directives, standards, or guidelines issued by the CCA from time to time.

The **Office of the Controller of Certifying Authorities (CCA)** shall publish and maintain a detailed audit checklist to facilitate consistent and standardized assessment of ESP operations and associated systems.

An **annual external audit** of the ESP, Business Application, and e-KYC System shall be conducted by an auditor or audit firm empaneled by the CCA. The audit shall evaluate compliance with all applicable legal, regulatory, technical, and security requirements, and the audit report shall be submitted to the CCA within the prescribed timeframe.

Furthermore, both the **Certifying Authority (CA)** and the **Controller of Certifying Authorities (CCA)** shall ensure that audit activities are conducted in accordance with the audit provisions prescribed under **Rule 32 of the Information Technology (Certifying Authorities) Rules, 2010**, as amended from time to time.

19. Guideline Governance

The office of the CCA, on behalf of the Government of Bangladesh shall have ownership of this guideline. The office of the CCA shall monitor the implementation of this guideline. Licensed CAs in association with the Office of the CCA are responsible for the implementation of e-Sign and related technology according to this guideline. The owner of business applications and the end-users of business applications and other stakeholders shall adhere to this guideline regarding e-Sign adoption and usage. Any query regarding this document can be forwarded to the Office of the CCA. Office of the CCA reserves the right to review/update this guideline if and when necessary.

20. Abbreviations

API	Application Programming Interface
CA	Certifying Authority
CCA	Controller of Certifying Authorities
CSR	Certificate Signing Request
e-KYC	Electronic Know Your Customer
ESP	e-Sign Service Provider
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
OTP	One Time Password
PKCS	Public Key Cryptography Standard
OCSP	Online Certificate Status Protocol

CRL Certificate Revocation List

21. References

1. eIDAS regulations
   https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L.2014.257.01.0073.01.ENG
2. CCA India guideline for e-Sign
   http://cca.gov.in/eSign.html
3. e-Sign - An Online Digital Service: Evolving Trends & Use Cases:
   https://www.ijert.org/research/e-sign-an-online-digital-service-evolving-trends-use-cases-IJERTV9IS010038.pdf
4. Guidelines on Electronic Know Your Customer (e-KYC) of Bangladesh Financial Intelligence Unit
   https://www.bb.org.bd/mediaroom/circulars/aml/jan082020bfiu25.pdf
5. India Audit guidelines for CA, ESP, ASP
   http://cca.gov.in/sites/files/pdf/guidelines/CCA-CAAC.pdf
6. Time-Stamp Protocol for Time-Stamping Authority (rfc3161)
   https://tools.ietf.org/html/rfc3161
7. IT (CA) Rules, 2010
   https://www.bcc.gov.bd/site/page/a2f3c95c-8e75-48f7-a0ea-0e94902d329

Change History

The "Change History" section has been newly added to the guideline to provide a consolidated summary of all revisions made to the document over time. This section is intended to give readers a high-level overview of the changes introduced in the current and previous versions, while detailed comparative differences can be reviewed in the archived versions of the document.

Version	Date	Section/Topic	Changes Logs
		Executive Summary	The Executive Summary section has been revised by replacing the earlier "Digital Bangladesh 2021" vision–centric narrative with a broader and more formal description of Bangladesh's digital transformation journey. The updated version incorporates references to the National ICT Policy, 2002 and expands the description of the Information and Communication Technology Act, 2006.
		Definition	The "Definition" section has been updated to improve legal clarity, consistency, and standardization of terminology. Existing definitions such as e-Sign, CA, CCA, e-KYC, e-KYC Service, CPS, Business Application Owner, and Personal Information have been revised with clearer wording and updated references to the ICT Act, 2006 and IT (CA) Rules, 2010. Several definitions have been refined, including expanded scope for biometric data and more precise wording for e-Sign and related regulatory roles. New definitions such as e-Seal, KYC, Person, Relying

			Party, and X.509 Certificate have been added to enhance completeness and align the document with current technical and legal frameworks.
		Objectives	The "Objectives" section has been revised to improve clarity, structure, and scope by expanding existing objectives and adding new ones. Key additions include setting standards for licensed CAs, establishing KYC procedures for organizations, defining the scope for e-Seal within the PKI framework, and explicitly referencing e-Sign (X.509) certificates.
		e-Sign Overview	Updated the e-Sign Guidelines with enhanced regulatory, technical, operational, security, audit, interoperability, and legal compliance provisions for e-Sign implementation in Bangladesh.
		e-Sign Classification & Applicability	1. The classification names "Basic e-Sign" and "Advance e-Sign" have been changed to "Short validity e-Sign" and "Long validity e-Sign" to align the terminology with certificate validity periods. 2. The verification methods have been expanded to include biometric verification using Face, Fingerprint, and Iris, as well as live e-KYC sessions. 3. The long validity e-Sign onboarding process has been updated to incorporate live e-KYC–based identity verification. 4. The requirement for mandatory physical registration through kiosk/enrollment centers has been removed for long validity e-Sign. 5. Fingerprint-only verification has been replaced with broader biometric verification options including Face, Fingerprint, and Iris. 6. The required subscriber data for long validity e-Sign has been updated by replacing mandatory fingerprint submission with live e-KYC session requirements. 7. Identity verification criteria have been expanded to include e-Passport information in addition to NID and Date of Birth matching. 8. The signature authorization method for short validity e-Sign has been updated to allow authorized device–based authentication in addition to PIN and OTP. 9. Enrollment platform requirements for long validity e-Sign have been simplified by replacing fingerprint-reader–based enrollment with live e-KYC–enabled mobile or web platforms. 10. All references throughout the section have been updated to reflect the revised terminology of "Short validity e-Sign" and "Long validity e-Sign".
		e-Sign subscriber e-KYC/Enrolment process	The "e-Sign subscriber e-KYC/Enrolment process" section has been revised to include e-Passport as an identity document and align the process with the updated "Short validity e-Sign" and "Long validity e-Sign" model. A live e-KYC video-based verification process has been introduced for long validity e-Sign, along with improved

			biometric verification and clearer technical descriptions. The section also strengthens OTP-based authentication, email verification, data responsibility of subscribers, and overall clarity and consistency of the enrolment workflow.
		The Role of the Certification Authority (CA) acting as a e-Sign Service Provider (ESP)	The "Role of the CA as e-Sign Service Provider (ESP)" section has been revised to improve clarity, consistency, and legal wording. It introduces a new requirement for formal agreements between licensed CAs and Business Application Owners for e-Sign integration.
		e-KYC service	The "e-KYC service" section has been revised for improved clarity, consistency, and formal language. It introduces the storage of live e-KYC session video under ESP controls and further clarifies that sensitive biometric data must not be stored and may only be used for verification. The list of trusted verification service providers has been reorganized and streamlined, and compliance, security, and data protection requirements have been made more precise without changing the core regulatory intent.
		The Role of Business Application Owner	The "Role of Business Application Owner" section has been revised for improved clarity, structure, and legal precision. It introduces a mandatory legal agreement with the CA prior to onboarding, with the prescribed format specified in Annexure A. The responsibilities have been refined and standardized, including API-based integration, communication security, WYSIWYS requirement, digital signature usage, audit logging, and compliance obligations, without changing the core requirements.
		e-Sign Security	The "e-Sign Security" section has been revised to improve legal accuracy, technical alignment, and clarity without changing the core security framework. The reference to "CA Rules 2010" has been updated to the full legal title "Information Technology (Certifying Authorities), Rules, 2010," and terminology has been standardized throughout. The sole control assurance mapping has been refined by clearly aligning SCAL levels with e-Sign classifications, specifying SCAL1 for short validity e-Sign and SCAL2 for long validity e-Sign.
		Standard & Compliance	The legal reference to the "Digital Security Act, 2018" has been updated to the "Cyber Security Act, 2026" to reflect the current governing cybersecurity legislation.
		Audit Procedure	The "Audit Procedure" section has been revised to improve legal accuracy and standardize references to guidelines and regulations. It adds new requirements to comply with Rule 32 of the Information Technology (Certifying Authorities) Rules, 2010, strengthening the statutory audit framework. The ESP shall conduct Vulnerability Assessments (VA) on a quarterly basis and Vulnerability Assessment and Penetration Testing (VAPT) annually through qualified and independent assessors. All other requirements, including ISO 27001 compliance, and yearly external audits by CCA-empaneled auditors for ESP, business applications, and e-KYC systems, remain unchanged.
		Change History	The change history has been newly added to the document to systematically record, present, and track all revisions made across the guideline.

Annexure-A

Format of the agreement

Agreement for e-Sign Services

Between

e-Sign Service Provider (ESP)

And

Business Application Owner (BAO)

This Agreement for e-Sign Services (the **"Agreement"**) is made and entered into on this ___ day of _____, *20* (the **"Effective Date"**).

BY AND BETWEEN

[Name of Business Application Owner], which expression shall mean and include a company incorporated under the Companies Act, 1994/any Government Ministry/Division/Department **or** any statutory or autonomous body established under applicable law, acting through its duly authorized representative **[name, designation]**, having its office at **[address]** (hereinafter referred to as the "Business Application Owner" or "BAO", which expression shall, unless repugnant to the context, include its successors and permitted assigns), of the First Part;

AND

[Name of e-Sign Service Provider], which expression shall mean and include a company incorporated under the Companies Act, 1994 **or** any Government authority, agency, or department **or** any statutory or autonomous body duly authorized to provide e-sign services under applicable law, acting through its duly authorized representative **[name, designation]**, having its office at **[full address]** (hereinafter referred to as the "e-Sign Service Provider" or "ESP"), of the **Second Part**.

The BAO and ESP are hereinafter individually referred to as a "Party" and collectively as the "Parties".

WHEREAS

(a) The BAO is a legally constituted entity (which may be a company, Government entity, or autonomous/statutory body) and is engaged in lawful activities. The BAO intends to integrate and utilize the e-Sign platform and related services provided by the ESP.

(b) The ESP is a legally constituted entity (which may be a licensed Certifying Authority, Government entity, or autonomous/statutory body) authorized under applicable laws of Bangladesh, including the Information and Communication Technology Act, 2006 and the Information Technology (Certifying Authorities) Rules, 2010, and is duly licensed/authorized by the Controller of Certifying Authorities (CCA), Bangladesh, where applicable. Digital certificates and e-sign services provided by the ESP comply with applicable cryptographic, security, and interoperability standards and policies prescribed by the CCA.

(c) The BAO desires to obtain e-Sign services from the ESP for enabling secure electronic execution of documents and transactions for its internal use and/or for services provided to third parties or end users, as applicable.

(d) The ESP agrees to provide such e-Sign services to the BAO in accordance with the terms and conditions of this Agreement and all applicable laws, regulations, and regulatory guidelines.

NOW THEREFORE, IN CONSIDERATION OF THE FOREGOING AND MUTUAL COVENANTS AND PROMISES CONTAINED HEREIN AND OTHER GOOD AND VALUABLE CONSIDERATIONS, THE RECEIPT AND ADEQUACY OF WHICH IS HEREBY ACKNOWLEDGED, THE PARTIES HEREBY COVENANT AND AGREE AND THIS AGREEMENT WITNESSETH AS FOLLOWS:

1.1 Definitions and Interpretations

(a) **"Agreement"** means this e-Sign Service Agreement, including all schedules, annexures, appendices, exhibits, statements of work, service level agreements, and any amendments, modifications, supplements, or addenda executed by the Parties in writing from time to time;

(b) **"Business Day"** means any day other than Friday, Saturday, or any gazetted public holiday observed in the People's Republic of Bangladesh;

(c) **"Controller of Certifying Authorities (CCA)"** means the Controller of Certifying Authorities appointed under sub-section (1) of section 18 of the Information and Communication Technology Act, 2006;

(d) **"Digital Signature Certificate (DSC)"** shall have the same meaning as defined under the Information and Communication Technology Act, 2006 and rules and regulations made thereunder as amended from time to time;

(e) **"Electronic Know Your Customer (e-KYC)"** is an electronic automated method used to verify and authenticate the identity of an e-Sign Subscriber as defined in Rule 2(j) of the Information Technology (Certifying Authorities), Rules 2010;

(f) **"e-Sign' or 'e-Sign Service"** is an online Electronic Signature Service in which the key pair generation, certification of the public key by the CA and digital signature creation for electronic document are facilitated by the e-Sign online Electronic Signature Service provider instantaneously within a single online service based on successful authentication of individual using e-KYC services;

(g) **"e-Sign User"** means an individual or legally recognized entity acting through an authorized representative who requests or utilizes the e-Sign Service for executing a Document;

(h) **"Laws"** means all applicable laws, statutes, acts, ordinances, rules, regulations, notifications, orders, directives, circulars, guidelines, policies, licences, permits, judgments, decrees, governmental approvals, and other legally binding requirements issued by any competent governmental, regulatory, judicial, or statutory authority having jurisdiction over the Parties, the Services, or the subject matter of this Agreement, as amended, supplemented, replaced, or re-enacted from time to time.

(i) **"OTP"** shall mean 'one time password' sent to the e-Sign User's cell phone or email for the purpose of authentication;

(j) **"Party"** means individually either the Business Application Owner (BAO) or the e-Sign Service Provider (ESP), as the context may require;

(k) **"Parties"** means collectively the Business Application Owner (BAO) and the e-Sign Service Provider (ESP).

(l) 'Services' shall mean the services to be provided by the e-Sign Service Provider (ESP) to Business Application Owner (BAO) as agreed in this Agreement;

(m) 'Successful Transaction' means the event of receipt of an e-Sign by BAO from ESP for a particular Document in the case of BAO and the event of dispatch of a DSC to BAO by ESP for a particular document;

(n) 'Third Party' shall mean any party who is not BAO or ESP.

1.2 Interpretations

In this Agreement, unless the context requires otherwise:

(a) reference to singular includes a reference to the plural and vice versa;

(b) reference to any gender includes a reference to all other genders;

(c) reference to an individual shall include his legal representative, successor, legal heir, executor and administrator;

(d) reference to statutory provisions shall be construed as meaning and including references also to any amendment or re-enactment (whether before or after the date of this Agreement) for the time being in force and to all statutory instruments or orders made

pursuant to statutory provisions;

(e) references to any statute or regulation made using a commonly used abbreviation shall be construed as a reference to the title of the statute or regulation;

(f) references to any Article, Clause, Section, Schedule or Annexure, if any, shall be deemed to be a reference to an Article, Clause, Section, Schedule or Annexure of or to this Agreement;

(g) clause headings in this Agreement are inserted for convenience only and shall not be used in its interpretation;

(h) when any number of days is prescribed in this Agreement, the same shall be reckoned exclusively of the first and inclusively of the last day unless the last day does not fall on a Business Day, in which case the last day shall be the next succeeding day which is a Business Day;

(i) if any provision in this Agreement is a substantive provision conferring rights or imposing obligations on anyone, effect shall be given to it as if it were a substantive provision in the body of this Agreement;

(j) any word or phrase defined in the body of this Agreement shall have the meaning assigned to it in such definition throughout this Agreement unless the contrary is expressly stated or the contrary clearly appears from the context;

(k) the rule of construction, if any, that a contract shall be interpreted against the party responsible for the drafting and preparation thereof shall not apply;

(l) reference to days, months or years in this Agreement shall be a reference to calendar days, months or years, as the case may be, unless the contrary is expressly stated or clearly appears from the context;

(m) Reference to any agreement, deed, document, instrument, rule, regulation, notification, statute or the like shall mean a reference to the same, as may have been duly amended, modified or replaced. For the avoidance of doubt, a document shall be construed as amended, modified or replaced only if such amendment, modification or replacement is executed in compliance with the provisions of such document(s).

2.0 Agreement

(a) The Business Application Owner (BAO) agrees to avail the Services from the e-Sign Service Provider (ESP), and the ESP agrees to provide the Services to the BAO, in accordance with the terms and conditions of this Agreement.

(b) The ESP hereby authorizes the BAO to access and utilize the e-Sign Services through the ESP's platform, subject to the terms and conditions of this Agreement and applicable laws and regulatory requirements.

3.0 Representations

3.1 Representations of ESP: ESP represents to BAO that:

(a) the ESP is a duly incorporated and validly existing entity under the laws of Bangladesh and is in good standing under such laws;

(b) the ESP has full legal capacity, power, and authority to enter into this Agreement and has taken all necessary corporate and other actions required to authorize the execution, delivery, and performance of its obligations hereunder;

(c) this Agreement has been duly executed by the ESP and constitutes a legal, valid, and binding obligation of the ESP, enforceable against it in accordance with its terms under the laws of Bangladesh;

(d) the ESP has obtained, and shall maintain in full force and effect, all necessary licences, permits, approvals, authorizations, and consents from the relevant governmental, regulatory, or competent authorities required to perform its obligations and provide the Services under this Agreement;

(e) the representations and warranties set out in this Clause are true, accurate, and correct as of the Effective Date and shall be deemed to be continuing representations for the duration of this Agreement.

3.2 Representations of BAO: BAO represents to ESP that:

(a) BAO is an entity legally constituted and validly existing under the laws of Bangladesh;

(b) BAO has all requisite powers and authority and has taken all actions necessary to execute, deliver, and perform its obligations under this Agreement;

(c) this Agreement has been validly executed by BAO and constitutes a valid agreement binding on BAO and enforceable in accordance with the laws of Bangladesh.

4.0 Scope of Work

The ESP & BAO shall provide services ('Services') as per **'Annexure -1'** of this Agreement.

4.1 Obligations of ESP

(a) The ESP shall, during the Term of this Agreement, maintain necessary licences with CCA as required for issuance of DSC;

(b) The ESP shall, during the Term of this Agreement, maintain its empanelment with CCA

4.2 Obligations of BAO

(a) The Business Application Owner (BAO), being the entity utilizing e-Sign Services to enable specific services or business functions, shall be solely responsible for determining the type(s) of authentication mechanisms to be used for its e-Sign transactions. Such selection shall be at the sole discretion of the BAO, and neither the ESP nor any e-Sign User shall have any authority or involvement in such determination.

(b) The BAO shall be solely responsible for ensuring and maintaining adequate network connectivity, integration, and communication infrastructure with the ESP, including all associated configurations, security controls, and operational requirements necessary for the proper use of the Services.

(c) The BAO shall establish, implement, and maintain all necessary e-Sign related operational capabilities, including but not limited to systems, processes, infrastructure, technology, information security controls, and periodic audits, in compliance with the standards, specifications, guidelines, and directives issued by the Controller of Certifying Authorities (CCA) from time to time.

(d) The BAO shall, at all times, comply with the Information and Communication Technology Act, 2006, and all applicable rules, regulations, directives, and guidelines issued thereunder, as well as all other applicable laws, rules, and regulations in force or that may come into force from time to time, including those relating to data security, data protection, data storage, data sharing, and data management. The BAO shall further comply with the requirements of the National Identity Registration Authority legislation or any successor law, as and when enacted and brought into force, and shall ensure equivalent compliance standards are maintained in its operations under this Agreement.

(e) The BAO shall maintain complete and accurate logs of all e-Sign related transactions processed through its systems, capturing all relevant transaction details in accordance with applicable technical and regulatory requirements. The BAO shall ensure that such logs are securely stored, retained for the legally required retention period, and protected against unauthorized access, alteration, or destruction, in compliance with the Information and Communication Technology Act, 2006, the Evidence Act, 1872, and any other applicable laws and regulations.

(f) In case of any investigations around signature related fraud(s) or dispute (s), the BAO shall extend full cooperation to ESP/CCA and/or any agency appointed/authorized by it and/or any other authorized investigation agency, including, but not limited to, providing access to their premises, records, personnel and any other relevant resource / information, etc. of or pertaining to its e-Sign,

(g) BAO shall obtain consent from e-Sign users to use their e-KYC information for e-Sign for availing e-Sign Services from ESP for DSC application form, key-generation, certificate issuance signature creation and key destruction"

(h) BAO shall Indemnify both ESP and CA for integrity related discrepancies arising at BAO end.

5.0 Service Level Agreement of ESP

ESP shall provide services in accordance with the service levels ('Service Level Agreement') as specified in 'Schedule II' appended to this Agreement. In case of breach of such service levels, BAO shall be authorized to levy such penalty as specified in Service Level Agreement.

6.0 Fees & Payment Terms

(a) BAO shall be liable to pay ESP as per the pricing modality & payment schedule mutually agreed by both the parties mentioned in the '**Annexure-2**' of this agreement.

(b) ESP shall raise invoice for the Fees on BAO in arrears on monthly basis. Along with the invoices, ESP shall send transaction reference numbers certificate of Successful Transaction(s) for which the invoice has been raised. If requested by BAO, ESP shall also share with BAO either the complete list of transaction numbers or the specific log against requested transaction number, as the case may be. Notwithstanding the foregoing, BAO shall maintain the clear log of transactions for BAO's reconciliation purposes.

(c) The Fees shall be due and payable upon receipt of invoice by BAO. BAO shall pay ESP for all undisputed Successful Transactions mentioned in an invoice within 07 days of receipt of invoice by BAO. For the disputed Successful Transactions, the amount shall be paid with 07 days of the date on which such dispute is resolved by the Parties.

7.0 Taxes

The Fees is exclusive of applicable taxes & VAT. All applicable taxes and VAT on the Services shall be borne by BAO and shall be paid by BAO to ESP in addition to the Fees.

8.0 Force Majeure

(a) The Parties agree that neither of them shall be liable to the other for any loss, delay, damage or other casualty suffered or incurred by the other owing to earthquakes, floods, fires, explosions, acts of God, war, terrorism, or any other such cause, which is beyond the reasonable control of the Party and any failure or delay by any other Party in the Performance of any of its obligations under this Agreement owing to one or more of the foregoing causes shall not be considered as a breach of any of its obligations under this Agreement. The Parties however agree that any financial failure or non-performance of any financial obligations or covenants of the Parties shall not constitute Force Majeure.

(b) The Party claiming benefit of Force Majeure shall however not be entitled to the same unless it has intimated the other Party of the occurrence of such an event within a period of seventy hours from the occurrence of such Force Majeure event indicating therein the steps that it is

taking or intending to take to mitigate the effect of such Force Majeure on the performance of his obligations under this Agreement.

9.0 Confidentiality and data protection

(a) Each Party shall treat all information, which is disclosed to it as a result of the operation of this Agreement, as Confidential Information, and shall keep the same confidential, maintain secrecy of all such information of confidential nature and shall not, at any time, divulge such or any part thereof to any third party except as may be compelled by any court or agency of competent jurisdiction, or as otherwise required by law, and shall also ensure that same is not disclosed to any person voluntarily, accidentally or by mistake.

(b) Parties hereby unequivocally agrees to undertake all measures, including security safeguards, to ensure that the information in the possession or control of the Parties, as a result of operation of this Agreement, is secured and protected against any loss or unauthorized access or use or unauthorized disclosure thereof.

(c) Parties agree that information liable to be disclosed under the Right to Information Act, 2009 shall not be considered as confidential information.

(d) It is hereby mutually agreed that this Clause 13 shall survive the termination of this Agreement.

10.0 Intellectual Property Rights

Both parties shall have the exclusive Intellectual Property Rights to their respective products and services i.e. ESP shall have the intellectual Property Rights of their e-Sign Platform whereas, BAO shall have the intellectual Property Rights to their Business Application.

11.0 Limitation of Liability

The liability of ESP (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, shall be the payment of direct damages only which shall in no event in the aggregate exceed the percentage of payments made during the preceding months/years [Or the total value of the project]. Neither Party shall be liable to the other Party for any indirect, consequential or remote damages under this Agreement.

12.0 Audit rights

The BAO shall ensure that its operations and systems in terms of this Agreement are audited by Cert-IN empaneled auditor on an annual basis to ensure compliance with ESP and CCA standards and specifications and the audit report should be shared with ESP and CCA upon request. In addition to the above, ESP and/or CCA may choose to, in its/their sole discretion, audit the BAO's operations and systems in terms of this Agreement by itself or through an

auditor appointed by ESP/CCA, and the continuation of operations as the BAO shall, at all times, be dependent upon the said audit confirming the compliance by the BAO of the terms and conditions contained in this Agreement, and any failure in compliance of the same, if confirmed in the audit, may entail fine and/or penalties and termination of access to e-Sign Services. The BAO unequivocally agrees to provide full co-operation to ESP/CCA or any agency approved and/or appointed by ESP/CCA in the audit process, and to provide to ESP/CCA or any agency approved and/or appointed by ESP/CCA, complete access to its procedures, records and information pertaining to services availed. The audit rights of ESP/CCA shall be subject to such confidentiality undertaking as may be reasonably imposed by BAO to protect its confidential information.

13.0 Term

(a) This Agreement shall commence and come into force on the date first written above (the **"Effective Date"**).

(b) Unless terminated earlier in accordance with the provisions of this Agreement, this Agreement shall remain valid and in full force for an initial period of **[•] years** from the Effective Date (the **"Term"**).

(c) The Term may be extended for such further period(s) as may be mutually agreed in writing by the Parties, subject to such terms and conditions as may be agreed at the time of extension.

14.0 Termination

14.1 This Agreement shall be deemed to be automatically terminated (without any notice) if and when:

(a) the agreement between ESP and BAO is terminated;

(b) the license/authority provided by CCA/Certifying Authority to ESP for providing DSC related services is revoked/cancelled/suspended.

14.2 Either Party may terminate this Agreement by giving 30 days prior written notice to the other Party.

15.0 Consequences of termination

(a) In case of termination of this Agreement due to any reason, BAO shall, pay ESP all due and payable amounts of Fees for the Successful Transactions completed till the effective date of termination.

(b) In case of termination of this Agreement due to any reason or upon expiry of this Agreement, the ESP shall retain a copy of all logs, documents, artefacts etc. for a period of 7 years.

16.0 Dispute Resolution / Arbitration

(a) In the case of any dispute arising upon or in relation to or in connection with this Agreement

between the Parties, the disputes shall at the first instance be resolved through good faith negotiations, which negotiations shall begin promptly after a Party has delivered to the other Party a written request for such consultation.

(b) In the case of any dispute arising upon or in relation to or in connection with this Agreement between the Parties, which have not been settled in accordance with Clause 21.1, any Party can submit the dispute for arbitration under the Bangladesh Arbitration Act 2001.

(c) The decision of the arbitrator shall be final and binding upon both parties. The expenses of the arbitrator as determined by the arbitrator shall be shared equally by the Parties. However, the expenses incurred by each party in connection with the preparation, presentation shall be borne by the Party itself. All arbitration awards shall be in writing and shall state the reasons for the award.

(d) The Parties shall continue to be performing their respective obligations under this Agreement, despite the continuance of the arbitration proceedings, except for the disputed part under arbitration.

(e) The Parties shall use their best endeavors to procure that the decision of the Arbitrators shall be given within a period of six (6) months or soon thereafter as is possible after it has been demanded.

(f) This Clause 16.0 is severable from the rest of this Agreement.

(g) BAO may terminate this Agreement, by giving a written notice of termination of minimum 30 days to ESP, if ESP fails to comply with any decision reached consequent upon the arbitration proceedings.

17.0 Miscellaneous

17.1 Applicable law and jurisdiction

This Agreement shall, in all respects, be governed by, and construed in accordance with the laws of Bangladesh. The Courts in Dhaka, Bangladesh shall have exclusive jurisdiction in relation to this Agreement, including Clause 20.

17.2 Waiver

No failure by a Party to take any action with respect to a breach of this Agreement or a default by any other Party shall constitute a waiver of the former Party's right to enforce any provision of this Agreement or to take action with respect to such breach or default or any subsequent breach or default. Waiver by any Party of any breach or failure to comply with any provision of this Agreement by a Party shall not be construed as, or constitute, a continuing waiver of such provision, or a waiver of any other breach of or failure to comply with any other provision of this Agreement, unless any such waiver has been consented to by the other Party in writing.

17.3 Severability

If any Clause or part thereof, of this Agreement or any agreement or document appended hereto or made a part hereof is rendered invalid, ruled illegal by any court of competent jurisdiction, or unenforceable under present or future Laws effective during the term of this Agreement, then it is the intention of the Parties that the remainder of the Agreement, or any agreement or document appended hereto or made a part hereof, shall not be affected thereby unless the deletion of such provision shall cause this Agreement to become materially adverse to any Party in which case the Parties shall negotiate in good faith such changes to the Agreement, or enter into suitable amendatory or supplementary agreements, as will best preserve for the Parties the benefits and obligations under such provision.

17.4 **Notices**

Any notice, direction or other documentation required or remitted to be given hereunder shall be in writing and may only be given by personal delivery, international courier, electronic mail or facsimile (with confirmation received).

17.5 **Enurement**

This Agreement shall be binding upon and shall enure to the benefit of the Parties hereto and their respective successors and permitted assigns.

17.6 **Expenses**

Each of the Parties shall bear the fees and expenses of their respective counsels, accountants and experts and all other costs and expenses as may be incurred by them incidental to the negotiation, preparation, execution and delivery of this Agreement.

17.7 **Surviving provisions**

The provisions of this Agreement, which are intended to survive the term of this Agreement by their very nature, shall survive the termination of this Agreement. Notwithstanding the generality of the above, clauses related to indemnity, confidentiality, arbitration and applicable law and jurisdiction shall survive the termination/expiration of this Agreement.

17.8 **Assignment**

This Agreement shall not be assigned by either Party without obtaining a prior written consent from the other.

17.9 **Entire Agreement**

This Agreement constitutes the entire agreement between the Parties. There are not and will not be any verbal statements, agreements, assurances, representations and warranties or undertakings among the Parties and this Agreement may not be amended or modified in any respect except by written instrument signed by the Parties.

17.10 **Counterparts**

This Agreement may be executed in one or more counterparts, all of which shall be read and construed as one document and any facsimile signature hereto shall be deemed to be an original signature.

IN WITNESS WHEREOF the parties have each executed this Agreement by its duly authorized officer as of the day and year first above written

SIGNED AND DELIVERED FOR AND ON BEHALF OF BAO:

Name: _____
Title: _____
Designation: _____
Organization: _____

Signature: _____

Date: _____

SIGNED AND DELIVERED FOR AND ON BEHALF OF ESP:

Name: _____
Title: _____
Designation: _____
Organization: _____

Signature: _____

Date: _____

WITNESSES

Witness – 1 (BAO Side)

Name: _____
Father's Name: _____
Address: _____

Signature: _____
Date: _____

Witness – 2 (ESP Side)

Name: _____
Father's Name: _____
Address: _____

Signature: _____
Date: _____

Annexure – 1: Scope of Work

For e-Sign Service Provider (ESP)

The services which need to be performed by the e-Sign Service Provider include the following, but not limited to:

(a) e-Sign Service provider should facilitate the generation of the subscriber's key pair in accordance with the Information and Communication Technology Act 2006;

(b) The key generation process shall generate statistically random key values that are resistant to known attacks;

(c) Keys shall be transferred from the key generation system to the storage device (if the keys are not stored on the key generation system) using a secure mechanism that ensures confidentiality and integrity;

(d) The ESP should secure the key pairs in hardware security module which are in accordance with Information Technology Act;

(e) The ESP should generate application data for e-signature using e-KYC and send to the Certifying Authority for generation of digital signature certificate

(f) ESP shall provide signer's onboarding tool (e-KYC application) to onboard all the signers who will be signing through the application of BAO.

(g) The newly generated digital signature value should be attached to the hash of the document sent for signing

(h) Creates an audit trail for the transaction

(i) ESP shall provide necessary API and Middleware to integrate their platform to BAO's application.

For Business Application Owner (BAO)

The activities which the Business Application Owner needs to take care at its end include, but not limited to the following:

(a) Provide the end user with the required web interface to enable him to sign the document digitally.

(b) Creates a document hash (to be signed) on the client side to be sent to the ESP

(c) A connection needs to be established with the e-Sign Service Provider so that the request could be sent and received from the BAO's end

(d) Provide adequate security mechanism to ensure that the integrity, authenticity of data and resistant to all known attacks.

(e) The delegation of responsibilities of e-Sign related obligations should not be delegated other than to the application owned or operated by BAO

(f) Both the parties, that is, Business Application Owner and e-Sign Service Provider have to follow the guidelines and rules laid down by the Office of Controller of Certifying Authorities regarding the e-Sign service along with the Information and Communication Technology Act 2006.

Annexure – 2: Pricing & Payment Terms

Pricing Plan:

To Be Decided

Payment Terms

To Be Decided

A T M Ziaul Islam
Controller (Joint Secretary)
Office of the Controller of
Certifying Authorities
ICT Division