

Office of the CCA

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

Callaway

[Handwritten signature]

at

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

Document Approval

Name	Role	Date	Signature

Distribution List


Name	Role

Document Control

Classification	Public
Document Status	
Document Location	
Maintenance Owner	
Approval owner	
Release Date	
Next Review Date	

Table of Contents

Document Change Control	2
Document Approval.....	2
Distribution List.....	2
Document Control.....	2
1. Executive Summary	4
2. Definition	5
3. Background.....	5
4. Objective	6
5. Scope	6
6. e-Sign Overview	7
7. e-Sign Classification & Applicability	7
8. e-Sign Service Framework.....	9
8.1 Subscribere-KYC/Enrolment process.....	10
8.2 Certificate issuance process.....	10
8.3 e-Sign Subscriber authorization device set-up process.....	11
8.4 Remote Signing Process	12
9. Role of e-Sign Service Provider.....	13
10. e-KYC service.....	13
11. Role of Business Application Owner.....	14
12. Role of e-Sign Subscriber	15
13. e-Sign Security	15
14. Certificate and Key Lifecycle Management.....	17
15. e-Sign Interoperability	17
16. Standard & Compliance	17
17. Event Logging Procedure	17
17.1 ESP event logging	18
17.2 Business application Event Logging	18
17.3 e-KYC Event Logging	18
18. Audit Procedure.....	19
19. Guideline Governance	19
20. Abbreviations	19
21. References.....	20

Allauca 



1. Executive Summary

If a nation has a dream, the dream itself can guide the nation and help materialize the dream. In 2008, Bangladesh started to believe in a dream, the whole nation started to envisage a vision to become “Digital Bangladesh”. Digital Bangladesh vision is not about digitizing information and automating the system with technology, it is about transforming the nation from Low Income Country to Middle Income Country by 2021, it is about raising all economic, social, and other key indicators of the country to a desired level by 2021. Controller of Certifying Authorities (CCA) is working as one of the key organizations in this journey since 2011. CCA has developed necessary Rules, Guidelines for Public Key Infrastructure (PKI), established the Root CA infrastructure, and completed the license issuance process of a Certifying Authority (CA). All Licensed CAs of Bangladesh are working to create awareness about the importance and benefits of electronic transactions and digital signature. While creating awareness on PKI enablement with other agencies, most of the time the challenges all CA have encountered with is the complexity to use digital signature in applications, complexity to enroll for digital signature certificate, no mobility, signing is hardly possible from anywhere, and from any device.

To overcome this complexity, the global phenomena is to use PKI based remote signing solution. It became widely accepted considering the simplicity, ease of use, and security. It is also known as e-Sign, or Cloud Sign, or Remote Signature. In Bangladesh Information and Communication Technology Act 2006 (ICT Act 2006) has made Electronic Signature legally valid. Subsequently, as per ICT Act 2006 and IT (CA) Rules 2010, CCA issued Certifying Authority (CA) licenses to credible organizations for implementation of Electronic signature certificate & relevant activities. The ICT Act 2006 or IT (CA) Rules 2010 does not define type of electronic signature or the processes. It gives the outline that the Electronic signature and digital signature type, process of issue, application and total life cycle management will be defined though the CCA approved CPS of the CA. E-Sign is a form of Electronic Signature and shall be implemented following the CCA approved CPS of CA. All operational issues related to e-Sign life cycle management would be included in the CCA approved CPS of the CA.

Considering the huge necessity of easy to use electronic signature under the existing legal framework, the CCA intended to set the guideline for CAs for providing e-Sign to the Subscribers.

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

2. Definition

e-Sign: A form of electronic signature or digital signature provided and certified by CAs as per ICT Act 2006 clause 2(1) and IT (CA) Rules 2010 where the user's private key is kept on e-Sign Service Provider CA's end, where the user has sole control of it through appropriate ecosystem.

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

Business Application Owner: The owner of the business application software or application where e-sign will be integrated into the workflow

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

e-KYC Service: Identity Verification service provided by CAs as per Rule 24 (e) of IT (CA) Rules 2010.

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 ICT Act 2006 and as per the Rule 21 of IT (CA) Rules 2010.

Controller of Certifying Authorities (CCA): Organization established under ICT Act 2006 to govern the certificate authorities and regulate the electronic signature landscape of Bangladesh.

Certifying Authority (CA): CCA Licensed Body/Bodies working under section 2(32) of ICT Act 2006 and providing electronic signature, digital signature, e-Sign Certificate & related services under section 36 of ICT Act 2006.

Certification Practice Statement (CPS): Certification Practice Statement submitted by the Licensed CAs under Rule 21(a) of IT (CA) Rules 2010 and approved by CCA.

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

Biometric Personal Information: Physical & biological Information of any person such as fingerprints, retina, and particle of the eye, voice pattern, etc.

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.

3. Background

Bangladesh has taken a great number of digital initiatives in recent years. Many e-government and e-business applications have been built to ease the life

of the customers. Digital signature is an essential government initiative which electronically bridges the Government with private individual and effectively bridges the Government agencies and bodies.

To regulate digital signatures system in Bangladesh, the office of CCA (Controller of Certifying Authorities) was established in 2011. It was established under the ICT Act 2006, in May 2011 within the ICT Division of the Ministry of Posts, Telecommunications & IT. The Section-8 of the ICT Act 2006 mandates that the usage of Electronic Signature and Records shall be recognized in all Government offices. Currently, there are multiple licensed Certifying Authority (CA) in Bangladesh, which have been providing digital signatures since 2013.

CAs operating under the regulatory body CCA, provide PKI enabled electronic signature and digital Signature for organizations and private individuals. But the current scheme of digital-signature of in-person physical presence, paper document-based identity & address verification, and issuance of hardware cryptographic tokens, along with custom driver-software- does not scale to a hundred million plus people in Bangladesh. But for offering fully paperless and secured citizen services, mass adoption of digital signature is necessary. A simple to use online service is required to allow everyone to have the ability to digitally sign electronic documents.

4. Objective

Objective of this guideline is to:

- a) Introduce e-Sign service in Bangladesh under the applicable laws and regulations;
- b) Provide the outline of e-Sign framework for Bangladesh;
- c) Guide licensed CA to implement e-Sign Service as e-Sign Service Provider (ESP);
- d) Assist licensed CA to establish the e-KYC platform for e-Sign;
- e) Provide the necessary information in regards to e-Sign certificate
- f) Provide necessary guidance to ESP (CA), business application owners, e-KYC, e-Sign Users, and relying parties to comply with regulatory requirements;
- g) Create awareness, build confidence and promote the use of PKI based e-Sign in business transactions.

5. Scope

This guideline is issued by the Office of the CCA, and it applies to all the Licensed CAs under ICT Act 2006, owner of business applications, e-Sign users, e-KYC provider, Empaneled Auditor of 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 that can be integrated with service delivery applications via an API to facilitate users to digitally sign a electronic content, record, file, application or document instantaneously. In e-Sign, the cryptographic key-pair is generated and stored securely on the ESP's server-side, and it is kept under the "Sole control" of the signer using multifactor authentication, encryption, and tamper-resistant hardware. And the signing happens completely remotely after the user gives consent and authenticates through OTP/QR/PIN/Biometric triggers.

Since all the complexities of securely storing keys and signing are pushed to the server-side of ESP, the proposed solution does not require any additional device in user side except a computer/ mobile/ tab with any browser. e-Sign can be easily integrated with many service delivery applications via an API to facilitate a user to digitally sign a document.

CAs shall provide a detailed description of their e-Sign Service, in their respective CPS.

7. e-Sign Classification & Applicability

As mentioned earlier, there could be different variants of e-Sign depending on mainly 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
- b) certificate validity,
 - i. Basic E-sign: Short validity (destroyed after first use)
 - ii. Advance 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) Basic e-Sign

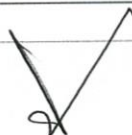
Basic e-Sign will be of short validity certificate and the identity verification shall be only Mobile (MSISDN) or E-mail OTP and Face matching based. The e-Sign subscriber can choose any of the authorization methods available. The face identified for verification

shall be 80% matched with the NID photo whereas other demographic information (e.g. name) has to 100% matched with NID database.

b) Advance e-Sign

Advance e-Sign can be of long/short validity certificate and the identity verification must be completed through biometric and Mobile (MSISDN) or email OTP. The e-Sign subscriber can choose any of the authorization methods available. In this case, the registration of the user will be done through certain registration booth/kiosk of ESP or Office of the CCA. The fingerprint identified for verification shall be 80% matched with NID or CCA fingerprint data.

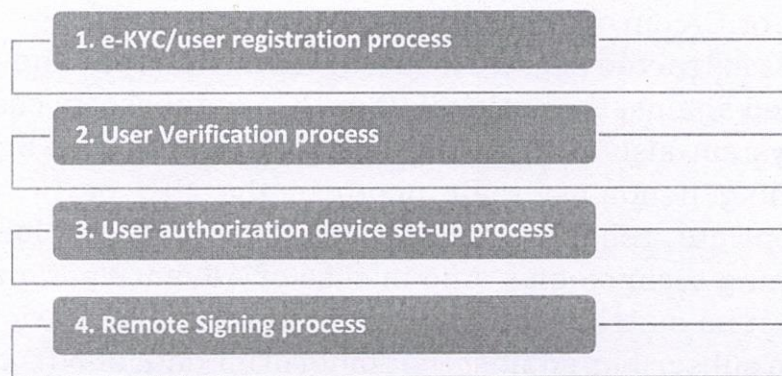
Property	Basic e-Sign	Advance e-Sign
Required Data from E-Sign subscriber	<ul style="list-style-type: none"> • Front and Rear part of NID Card • Live Photo • Mobile Number • Email Address 	<ul style="list-style-type: none"> • Front and Rear part of NID Card • Fingerprint • Mobile Number • Email Address
Identity Verification Method	<ul style="list-style-type: none"> • Face Recognition (>80%) • Demographic Data Verification (>80%) • NID number and Date of Birth matching (100%) • Mobile Number or email (with OTP) 	<ul style="list-style-type: none"> • Fingerprint Matching (>80%) • Demographic Data Verification (>80%) • NID number and 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	PIN and OTP or with Authorized Device
Enrollment Platform	<ul style="list-style-type: none"> • Mobile Apps • Web based Application • Physical CA enrollment center direct e-Sign portal or interface 	<ul style="list-style-type: none"> • Mobile Apps supporting fingerprint reader • Web based Application supporting fingerprint reader (provided customer has the fingerprint scanner) • KIOSK/Enrollment Center (to be established by CA)



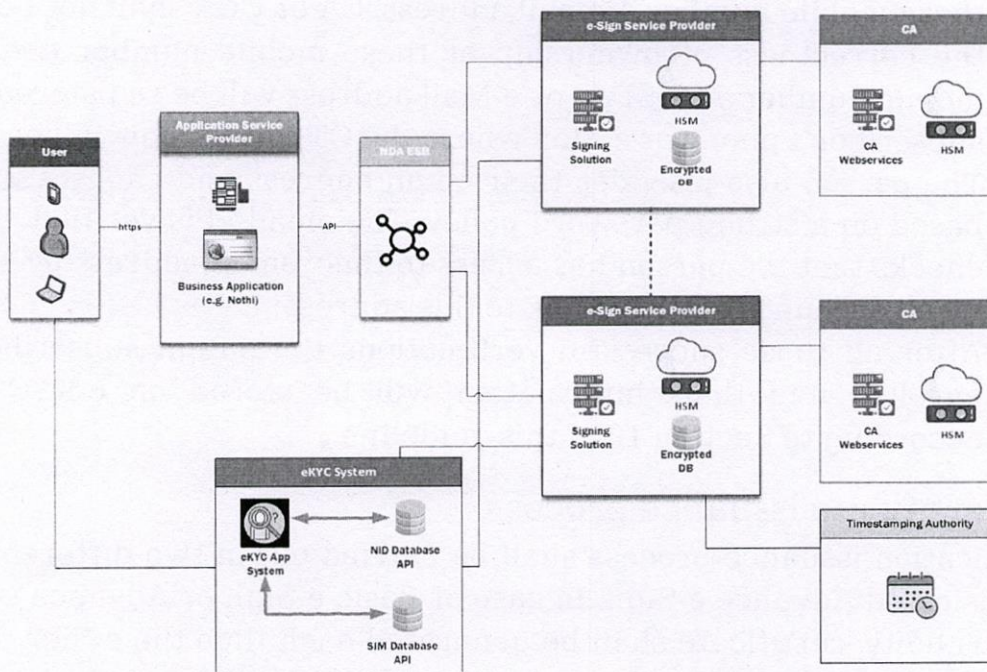
Depending on these types Office of the CCA will publish notification about the application area of e-Sign from time to time. Initially, all CA can start with Basic e-Sign immediately, later they can start rolling out Advance e-Sign version. However, there is no restriction by Office of the CCA on starting 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 download and open the e-Sign mobile app or access 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 and upload it through e-Sign mobile app/web based application or through direct CA interface;
- 3) For Basic e-Sign with face-matching, the e-Sign subscriber takes a selfie photo for App or a photo for the browser or Enrolment centre having a webcam. For Advance e-Sign the e-Sign subscriber gives fingerprint input through authorized standard fingerprint reader- which may be facilitated by ESP (or CCA) by deploying self-service kiosk or through agent or CA enrolment centres;
- 4) Data is extracted (e.g. OCR based) from NID front and rear side and it is verified against the national ID or CCA database. In case of Basic e-Sign, the system also verifies the live selfie photo of e-Sign subscriber by matching it against their photo in the NID or CCA database using appropriate reliable technologies like machine learning and face-matching technologies. And in case of Advance e-Sign (long/short time) the system matches the fingerprint or other Biometric data provided by e-Sign subscriber against the fingerprint data of NID or CCA database;
- 5) The user is prompted to give his/her mobile number & e-Mail. Mobile number & e-Mail address verification will be done through OTP and optionally through the SIM registration database; the e-Sign subscriber or user shall be fully liable for the validity, authenticity & ownership of these mobile number & email address, CA or CCA shall not be liable for the correctness of ownership of these mobile number & email. This mobile number (MSISDN) or e-Mail address will be registered as e-Sign subscriber's phone or e-Mail where the OTP for e-Sign will be sent.
- 6) The person also provides their email address and chooses a password based on a strong password policy. The email id is verified, the system checks that the person has access to their email address by sending an email account activation link to this address;
- 7) After all these successful verifications the e-Sign subscriber will be enrolled and their information will be stored on e-KYC database according to Section 10 of this guideline.

8.2 Certificate issuance process

Certification issuance process shall be carried out in two different methods for Basic and Advance e-Sign. In case of Basic e-Sign or Advance e-Sign with short validity, certificate shall be generated each time the e-Sign subscriber requests for signing a electronic record, content or document through business application. Whereas in case of Advance e-Sign with long validity,

certificate of an e-Sign Subscriber shall be generated prior to using it in any business application and then stored for issue period in a safe way where only the e-Sign subscriber will have sole access to use it. The process is described below:

1. e-KYC system will send necessary information (Name, Mobile number, Email, and other information) to e-Sign Service Provider (ESP) CA's system;
2. CA ESP system will request the HSM to create a key pair and return the pkcs#10 CSR or applicable format as per CA Rules 2010 & CA CPS;
3. The private key is exported from the HSM using an HSM Key Encrypting Key (KEK) and stored as encrypted blob (binary large object) in the CA database or in appropriate suitable system in sole control of e-Sign subscriber. They will remain encrypted when not in use;
4. e-Sign Service Provider (ESP) part of CA then sends the CSR to CA system for issuing certificate for this CSR;
5. The CA system then issues electronic certificate or digital certificate for the user and sends it back to the ESP system of the CA;
6. ESP system will store it in the database for that corresponding user in appropriate manner as per CA Rules 2010 & CA CPS;

8.3 e-Sign Subscriber authorization device set-up process

e-Sign subscriber can authorize their mobile device with the help of an App belonging to CA (ESP of CA), so that authorization response from that mobile device will only allow CA ESP system to create signature on behalf of the e-Sign subscriber. This is an optional process, e-Sign subscriber may wish to use it or opt for other process. The other convenient way is to send OTP from CA ESP before signature creation to the e-Sign subscriber's mobile number (MSISDN) or email address and e-Sign subscriber will give secure PIN and OTP to authorize (In that case authorization device setup is redundant). Following is the process if the e-Sign subscriber wants mobile device to be used as authorization device:

1. In the mobile app when the e-Sign subscriber will first try to login using their email address and password (set-up during the initial user registration process). The app detects this is the first time it is being used and asks the e-Sign subscriber to confirm they wish to register this device for remote signing purposes. If the e-Sign subscriber confirms, the app sends a device registration request to the e-Sign Service Provider's backend. On the other hand, e-Sign subscribers can also enable device authorization anytime they want.
2. e-Sign Service Provider CA sends OTP to the email address and mobile phone number (MSISDN) provided by the e-Sign subscriber;

3. After e-Sign subscriber authentication with OTP, ESP Mobile App will create an authorization key pair in the mobile device's tamper-protected Secure Element/ Secure Enclave hardware chip.
4. The e-Sign Mobile app creates a CSR for the authorization public key and sends this to the ESP's backend, along with the device's hardware fingerprint.
5. ESP CA certifies this authorization key using its internal/ external CA and stores the authorization certificate.
6. ESP links the person's authorization certificate& device-fingerprints with their Qualified Certificate and stores this information in the e-Sign subscriber's account information. This is protected using cryptographic checksums.
7. ESP notifies the e-Sign mobile app that it is now registered for signing authorization purposes.

8.4 Remote Signing Process

The following steps happen during the remote signing process:

1. Enrolled e-sign subscriber can access the business application from any device supported by that application;
2. e-Sign subscriber sends signing request to business application;
3. Business application will forward the signing request along with the unique information of e-Sign subscriber, hash of document/data, and application ID and other required information;
4. CA ESP system shall create signature for the e-Sign subscriber
 - a. For signing with Advance e-Sign with long validity, CA ESP will create signature with confirmation from user through tamper-proof device authorization or OTP and PIN;
 - b. For Basic or Advance e-Sign with short validity -
 - i. CA ESP will generate the appropriate key pair and return the pkcs#10 CSR to CA system;
 - ii. CA system shall issue certificate for this CSR and sends it back to the ESP system;
 - iii. ESP system will create signature with confirmation from user through tamper-proof device authorization or OTP and PIN;
5. CA ESP will forward the signature to business application;
6. Business application owner will attach signature with the data/document;



9. The Role of CA as e-Sign Service Provider (ESP)

Following are the roles of CA as the ESP:

1. CCA Licensed CAs shall automatically operate as ESP;
2. Licensed CAs shall apply for CPS approval to Office of the CCA by including e-Sign related practice information in the existing CPS;
3. According to the e-Sign guideline and other relevant guidelines or directives from the Office of the CCA, and the approved CPS, the Licensed CA will operate as ESP;
4. Licensed CA shall implement the e-Sign Service facility according to the prescribed e-Sign framework in this guideline;
5. Licensed CA shall develop an e-KYC platform which shall be integrated with their e-Sign platform to onboard the e-Sign user;
6. Licensed CA shall assist business application owner to integrate their business application with the e-Sign Platform through API and other applicable means;
7. Licensed CA shall comply with all the regulatory requirement of Office of the CCA as CA and ESP; and
8. Licensed CA shall be abiding by any other directives issued from the Office of the CCA time to time.

10. e-KYC service

Licensed CA shall develop their own e-KYC front-end platform to provide authentication service for the e-Sign subscriber. The front-end e-KYC system developed by each CA shall not store any personal sensitive data (e.g. biometric data). Only the following demographic data can be stored by Licensed CA to issue certificate and provide authorization service 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 ESP, Licensed CA can also store the following information of the user in the ESP database securely as prescribed by 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

Allama

J

Q

Any sensitive information (e.g. fingerprint) captured while on-boarding the e-Sign subscriber through the e-KYC system, must not be stored by CA. Sensitive information shall only be used only during the identity verification process whether it is a successful or failed verification. e-KYC system must comply with the event logging and storing procedure described in section 16.

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

The e-Sign Service provider can choose any of the verification service provider from the following to verify an e-Sign subscriber:

- a) National Identity Registration Wing, Election Commission;
- b) CCA DB
- c) Any other entity authorized by CCA with formal written permission
- d) Any other trusted database where identity verification has been done with reasonable assurance and confidence (e.g. specific bank's customer database, BTRC DB, BNDA Service bus BCC, Porichoy platform, , Mobile operator's DB, MFS DB, PSP DB etc.) with formal approval of CCA

While choosing the e-KYC verification service provider, CA ESP must ensure that the connectivity between the e-KYC verification service provider and CA ESP is private and encrypted. Moreover, the e-KYC verification service provider must keep a record of all transactional requests from each ESP and provide this information to the Office of the CCA as and when required. CCA may update this list of trusted verification service provider 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 needs to have a legal agreement with the CA according to this guideline before on-boarding for e-Sign service. Following are the responsibilities of a Business application owner:

- a) Complete the on-boarding process to use e-Sign in their business application according to this guideline;
- b) Assist to integrate their business application with CA's ESP system through API;
- c) Ensure security of back and forth communication with CA's ESP system;
- d) Ensure showing document/data to be signed to the e-Sign subscriber (e.g. WYSIWYS feature for e-Sign user or other suitable systems)

- e) All request sent to CA's ESP system has to be signed with digital certificate issued by Licensed CA;
- f) Provide the facility to verify the signature at any point of time through CA's system;
- g) Securely store and maintain all e-Sign related event logs and information required for audit purpose;
- h) Any other responsibility provided 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 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 natural identity and register mobile (MSISDN) and/ or email address for subsequent use. e-Sign subscriber has the following role (not limited):

- a) E-Sign subscriber must choose the e-Sign type, verification process, and authorization process;
- b) E-Sign subscriber must agree with the terms and condition of having e-Sign service;
- c) E-Sign subscriber must abide by all the regulatory requirement and relevant laws, regulation, and guidelines;
- d) E-Sign subscriber must verify each document represented to them by Business application before giving final consent for signing;
- e) E-Sign subscriber must keep his confidential information (Pin/Passphrase/Password etc.) only within their custody and must not impersonate as another e-Sign subscriber;
- f) Must comply with other regulatory directives provided by the Office of the CCA.
- g) E-Sign subscriber must keep the registered mobile phone number (PSISDN) and email address in his own possession. CA or CCA does not have any control over e-Sign subscriber mobile or email address and shall not be liable for any miss use in any form.
- h) E-Sign subscriber must report to CA in case of loss or registered mobile number (MSISDN) or hacked email account or address as per the CPS policy of the CA. They must register new mobile (MSISDN) and e-mail though 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:

Alana

[Signature]

[Signature]

- 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 CA 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-time 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
 - iii) Other suitable system as approved by CCA

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

- (1) Sole Control Assurance Level 1 (SCAL1) for Basic e-Sign
- (2) Sole Control Assurance Level 2 (SCAL2) for Advance 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.

Collana

✓

at

14. Certificate and Key Lifecycle Management

If the ESP chooses to implement longer time validity for certificate and key-then the validity of the certificate shall not be more than 2year and keys will be preserved for 2 year. 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 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. And certificate profile for e-Sign will be according to interoperability guidelines.

15. e-Sign Interoperability

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

16. Standard & Compliance

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

- a) ICT Act 2006
- b) IT (CA) Rules 2010
- c) Digital Certificate Interoperability Guideline(IOG)
- d) Respective Certification Practice Statement (CPS)
- e) PKI Audit Guideline
- f) Digital Security Act 2018
- g) Data Privacy & Protection Rules
- h) Time stamping Services Guideline
- i) And any other laws/rules/directives/notification published by the Office of the CCA or by the Government of Bangladesh.

17. Event Logging Procedure

ESP, Business application, and e-KYC system have to maintain event logging as per ISO 27001 standard. In addition to that, there are certain e-Sign specific events that all these parties have to keep an event log of. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

1. The type of event,
2. The date and time the event occurred,
3. Success or failure where appropriate, 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 Signing Key Pair for e-Sign subscriber;
- b) Deletion of key pair;
- c) Retrieval of e-Sign subscriber signing private key for usage;
- d) Transfer of e-Sign subscriber signing private key to encrypted storage
- e) All e-KYC requests sent to the e-KYC system and response received from the e-KYC system
- f) All e-Sign requests received from business application
- g) Proof of e-Sign subscriber's consent for signing (OTP or signature by authorization key)
- h) Generated CSR based on the information received from e-KYC
- i) Signature generation of the hash/document submitted
- j) All communication to 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

Allhane

[Signature]

[Signature]

specified above. Audit logs should be made tamper-proof so that no one can easily change it.

18. Audit Procedure

Section 13 defines quite a few security controls. These controls will be checked at the time of audit. And section 16 defines the types of events to be logged. These need to be checked at the time of the audit. Vulnerability Assessment and Penetration Testing (VAPT) has to be done every year and this report needs to be submitted to yearly external audit. Apart from these, ESP, Business application, e-KYC system- has to comply with ISO 27001 standard, PKI Auditing guideline 2013, Digital Certificate Interoperability Guideline 2013, IT (CA) rules 2010, empanelment terms and conditions, etc. The office of the CCA will publish a full checklist for ESP Audit. Audit for ESP, business application & e-KYC system needs to be done every year by external auditor empaneled by CCA.

19. Governance Guideline

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 preserve 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
PKI	Public Key Infrastructure
OCSP	Online Certificate Status Protocol
CRL	Certificate Revocation List

Alhama

[Signature]

[Signature]

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 esign
<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/jan082020bfui25.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-0e94902d329b/IT-CA-Rules-2010>
8. ICT ACT 2006
<https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/97cc59c38f514d39a84b8c0b39ae3f62/ICTACT2006.pdf>
9. PKI Audit Guideline
<http://www.cca.gov.bd/sites/default/files/files/cca.portal.gov.bd/policies/ee75c95850a9408f8ac84f6703c73b88/PKI%20Auditing%20Guideline,%202012.pdf>



মোঃ খালেদ হোসেন চৌধুরী
আইন কর্মকর্তা
ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী
কর্তৃপক্ষের নিয়ন্ত্রক-এর কার্যালয়
তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ



সেগম
(উপ-সচিব)
স্বাক্ষর সার্টিফিকেট প্রদানকারী
কর্তৃপক্ষের নিয়ন্ত্রক (সিসিএ)-এর কার্যালয়
তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ



আব্দুল সাব্বির চৌধুরী
নিয়ন্ত্রক (স্বাক্ষর-সচিব)
ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী
কর্তৃপক্ষের নিয়ন্ত্রক-এর কার্যালয়
তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ।