e-KYC Guideline
for
CA Operator

June 2021
Version 1.0

Contents

1.1 Background

The Office of the Controller of Certifying Authorities was established in 2012 to issue of electronic signature certificate as per Information and Communication Technology Act 2006 (amended 2013). By taking this initiative, Government intends to introduce digital signatures to achieve the target of developing information technology and to introduce secure e-governance. Under the Information and Communication Technology Act, 2006 and the Information Technology (Certifying Authorities) Rules, 2010 made thereunder, the Digital Signature Certificates (DSCs) are being issued by CA on successful verification of the identity and address credentials of the applicant. To begin e-sign service through e-KYC, CA may also use the same physical infrastructure and manpower resources for verification purposes. Security requirements for this service should be at the same level as being currently maintained by the CA.

The concept of Know Your Customer (KYC) started only few decades back. KYC had been emerged as one of the main preventive measures or tools to ensure users identity and to protect any abutment from criminal activities. However, KYC has gone one sept forward and emerged as Electronic Know Your Customer (eKYC).

In Bangladesh, Election Commission of Bangladesh holds the citizens (18 years and above) identity data with their biometrics has higher level of assurance and authenticity, where,"CCA or Certifying Authority (CA) " can have access to check the authenticity of customer provided identity data and bio-metrics by using this database. Therefore, this e-KYC Guideline is based on the national ID card and the bio-metrics data stored against each NID card.

This e-KYC guideline contains a set of instructions for the Certifying Authorities (CA) to enable them to conduct customer due diligence in a digital means.

Definitions:

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.

It also means

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information;

b) Identifying and taking reasonable measures to verify the identity of the user, as such that the Certifying Authority (CA) is satisfied and meets the guideline.

1.2 Scope

This Guideline shall be known as Electronic Know Your Customer (e-KYC) Guidelines which deals with electronic customer onboarding, identification and verification of customer identity, creating of customer digital KYC profile customer in a digital means. The scope of this Guideline will be as follows:

a) The provisions of this Guideline shall be applicable only for natural person;

b) The requirements of this guideline shall be applicable based on the risk exposures of the users. The user shall be required to conduct e-KYC which includes electronic customer onboarding, verify customer identity and preserve customer profile digitally;

c) The e-KYC requirement of this Guideline is based on the OTP and biometric verification;

d) Where e-KYC attempts failed due to any technical reason, the traditional KYC approach should be followed in case of emergency.

1.3 Objectives

The key objective of e-KYC is that it can provide an sample scope of quick onboarding of users by verifying user's identity through digital means which can leverage saving of time and provide ease both for the client and service providers.

Additionally, e-KYC can save institutional cost as well as foster growth of user base compare to the traditional growth. Therefore, the basic objectives of implementing e-KYC are as follows:

- Establish good governance within digital signing process.
- Protect digital signing sector from abuse of criminal activities.
- Ensure authenticity, integrity and stability.

- Reduction of time and cost related to customer on boarding and managing.
- Participate in the national level well-being.

2.0 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	• Front and Rear part of NID Card • Live Photo • Mobile Number • Email Address	• Front and Rear part of NID Card • Fingerprint • Mobile Number • Email Address
Identity Verification Method	• Face Recognition • Demographic Data Verification (>80%) • NID number and Date of Birth matching (100%) • Mobile Number or email (with OTP)	• Fingerprint Matching • 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	• Mobile Apps • Web based Application • Physical CA enrollment center direct e-Sign portal or interface	• 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.

3.0 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.

4.0 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:

a) NID Number
b) Full Name of the e-Sign user
c) Date of birth
d) Mobile Number (MSISDN)
e) Email Address
f) 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

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.

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

5.0 e-KYC Event logging:

The following event 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

6.0 Security measures

The CAs may use additional security measures in the onboarding process which may contains checking the phone number by generating pin codes and other measures as deemed necessary. Additionally, security of the data recorded and preserved under this e-KYC should be maintained properly by the CAs so that no user data to be hacked or compromised. This Guideline also suggest to preserved customer data locally hosted server or cloud sever and put in place necessary data protection and data security measures as prescribed by the prudential and self-regulators and/or by the government of Bangladesh.

7.0 Abbreviations

CA	Certifying Authority
CCA	Controller of Certifying Authorities
CSR	Certificate Signing Request
DB	Database
DSC	Digital Signature Certificates
e-KYC	Electronic Know your customer
ESP	e-sign Service Provider
FIPS	Federal Information Processing Standards
HSM	Hardware Secure Module
MSISDN	Mobile Station International Subscriber Directory Number
OTP	One Time Password