PKI Enable Application Guideline

Office of the Controller of Certifying Authorities

Government of Bangladesh

Document Control

Document Name	PKI ENABLE APPLICATION GUIDELINE
Status	Release
Version	1.0
Release Date	31 DEC 2024
Last update	31 DEC 2024
Document Owner	Office of the Controller of Certifying Authorities, Bangladesh

Contents

1. INTRODUCTION

Bangladesh emphasizes on digitization of work processes for timely decision and ensuring ease of doing business. This will require secured PKI enabled transaction, email, e-commerce etc. The Government has already established the Office of the Controller of Certifying Authority (CCA) to regulate, promote and encourage the use of PKI in the business and daily online e-commerce, e-payments, service delivery etc.

The Government of Bangladesh has already issued the following legislation, rules, guidelines to promote interoperable and secured digital transformation.

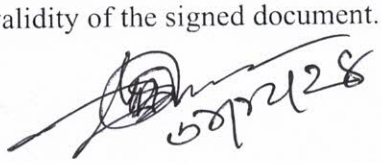
1. Information & Communication Technology Act, 2006
2. Information Technology (Certifying Authority) Rules, 2010
3. e-Sign Guideline for the Certifying Authorities (CAs)
4. PKI Auditing Guidelines
5. Time Stamping Services Guideline for Certifying Authorities (CAs)
6. e-KYC Guideline for CA Operators
7. CCA e-Sign API Specification Part 1: E-Signature for online e-KYC
8. Digital Signature Certificate Interoperability Guideline
9. Bangladesh National Digital Architecture Guideline, 2019
10. Certifying Authorities (CA) Licensing Guidelines, 2024
11. Certifying Authorities Personnel (Qualification & Experience) Guidelines, 2024

2. Objectives

This document outlines the key steps for planning and implementing electronic signatures in organizational applications, as well as managing a registered user base. If the scope of the electronic signature is confined to use within an internal application, the organization is responsible for maintaining the information related to the signature keys and digital signature certificates held by its personnel.

3. General

This document outlines the procedure for the custody and record-keeping requirements of encryption certificates. While it primarily addresses PDF signature-related aspects, the same principles are applicable to other signature formats such as XML, CMS, JSON and others. According to the Information and Communication Technology Act, 2006 a Digital Signature Certificate (DSC) refers to a certificate issued by a licensed Certifying Authority (CA). Application Owners must ensure that only DSCs issued by licensed CAs are used within their applications. An electronic signature is created using the private key corresponding to the public key certified by a licensed CA. In case of local signing, the subscriber is responsible for the secure custody of the private keys. In a Public Key Infrastructure (PKI) enabled application, Application Owners shall accept DSCs issued by any licensed CA, provided they belong to the specified class or higher. If the application requires specific services related to DSCs, these must be adhered to. The validity of an electronic signature is determined at the time it is applied to the document. Therefore, the certificate must be valid (not expired or revoked) at the time the signature is affixed. The unavailability of the token or the revocation or expiry of the certificate after the signature is applied does not affect the validity of the signed document.



For tender-related requirements, Application Owners should not impose additional fields or private key storage requirements for DSCs beyond those specified in the Guidelines issued by the Controller of Certifying Authorities (CCA). DSCs issued by licensed CAs must comply with the CCA's Interoperability Guidelines, and no deviations should be introduced. Application Owners should also accept higher-class certificates if lower-class certificates were initially specified for the application, as DSCs issued by licensed CAs offer the same level of assurance for certificates of the same class.

4. Requirements of Electronic Signature

1. The signature requirements for applications can be grouped into the following scenarios:
   (a) The application handles both creating and verifying electronic signatures, with no extra conditions.
   (b) The application handles both creating and verifying electronic signatures, but the signatures can also be verified by relying parties.
   (c) The application only verifies electronic signatures.
   (d) A combination of one or more of the above scenarios.
2. Planning for verification details, such as CRL/OCSP, signature type and rendering method, should be based on these categories.

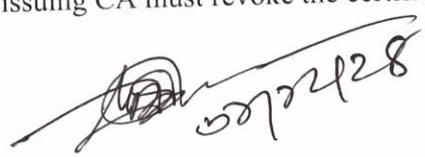
5. Types of Certificates

Certificates issued by CAs serve various purposes, such as individual signatures, encryption, web server authentication, device authentication and signing bulk documents. Here's an overview:

- **Individual Certificates:** These are issued for signing electronic documents, serving the same purpose as ink signatures on paper.
- **Encryption Certificates:** Used to encrypt electronic documents for secure communication.
- **Web Server Certificates (SSL Certificates):** Used to secure websites by ensuring safe communication between users and servers.
- **Device Certificates:** Verify the authenticity of devices.
- **Organizational Certificates:** Issued to organizational software for bulk document signing (e.g., generating receipts without requiring an individual's signature).

6. Digital Signature Certificates (DSCs)

According to the ICT Act, 2006 the signature keys linked to signature certificates must always remain under the control of the Digital Signature Certificate (DSC) applicant. The DSC applicant must request the issuing CA to revoke the certificate if the key is lost, transferred, or for organizational certificates in cases like retirement or other reasons. If the applicant is unavailable (due to death, illness, etc.), the department or organization should submit a revocation request to the CA. Upon receiving an authorized request from the relevant department, the issuing CA must revoke the certificate.



7. Digital Signature - Class of Certificates

Digital Signature Certificates (DSCs) are typically categorized into three classes based on their level of security and intended use. Here's an overview:

1. Class 1 DSC

- Purpose: Used for basic security and low-risk environments.
- Verification: Verifies the user's email address and name.
- Usage: Suitable for securing email communications or login credentials.
- Security Level: Provides basic assurance but is not suitable for high-security transactions.

2. Class 2 DSC

i. Local Sign

- Purpose: Used in environments that require a moderate level of security.
- Verification: Confirms the identity of individuals against a pre-verified database.
- Usage: Commonly used for e-filing tax returns, registration of companies, or signing documents in medium-risk scenarios.
- Security Level: Offers a good balance of security and usability.

ii. Remote Sign(e-Sign)

- Purpose: Used in environments that require a moderate level of security.
- Verification: Confirms the identity of individuals against a pre-verified database.
- Usage: Commonly used for e-filing tax returns, registration of companies, or signing documents in medium-risk scenarios.
- Security Level: Offers a good balance of security and usability.

3. Class 3 DSC

- Purpose: Designed for high-security transactions.
- Verification: Requires in-person verification of the individual or organization.
- Usage: Used for e-commerce, online banking, e-tendering, e-auctions, and other high-value or high-risk transactions.
- Security Level: Provides the highest level of security among all DSC classes.

Each class caters to different levels of trust and security needs, ensuring appropriate protection for various digital interactions.

8. Digital Signature Certificates - Legal Validity of Signature

Under the ICT Act, 2006 an electronic signature is considered valid only if it is applied following the procedures outlined in the IT (CA) Rules and is associated with a certificate issued by a Licensed Certifying Authority.

9. Digital Signature Certificates - CA Services

1. In case of local signing crypto tokens containing subscribers' signature keys might become unusable during the certificate validity period due to damage, loss, or other unforeseen circumstances. Certification Authorities (CAs) are obligated to provide at least one free re-issuance of such certificates within the validity period. If Application Owners require unlimited re-issuances for seamless operations, this condition should be explicitly included as part of the purchase agreement.
2. Application owners should assess whether their applications need local storage of Certificate Revocation Lists (CRLs), Online Certificate Status Protocol (OCSP) responses provided by Certifying Authorities (CAs) or both. All licensed CAs offer CRL and OCSP services.

07/2/28

3. Licensed CAs shall provide timestamping services to time-stamp electronic records.

4. Core expertise in PKI development and security required for signature-related software components and functions can also be provided by third-party PKI tools & service providers in that area.

10. Digital Signature Certificates - Roles & Responsibilities of Application Owner

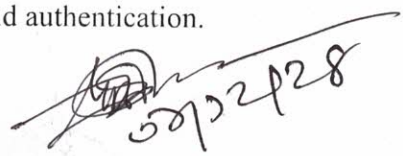
1. The applicants are required to create an e-KYC account with CA to get a digital signature certificate from a CA. For organizational application usage of organizational certificates, the details required for the revocation of the certificates should be preserved by the organization. To meet needs, such details should contain the certificate serial number, validity, and authorization of the organization by the subscriber for revocation.
2. The organization should set a process in place for revocation of certificates when the organizational personnel holding the certificate have a status transformation regarding the organizational details mentioned in the certificate.
3. The organization should not command the transfer of signature keys & certificates to any other person. The Certificate should be used only by the approved subscriber.
4. The application should not have any necessities for custody of the keys by anyone other than the subscriber.
5. The Application Owners should specify the operating systems and browsers likely to access their application and thus provide assistance to the client components for a seamless operation.

11. Digital Signature Certificates - Application Functional Requirements

1. Considering the sensitive nature and possible misuse linked to electronic signatures, it is suggested that the application may impose multi factor authentication.
2. For applications requiring occasional electronic signatures, the system should notify the signer via SMS and email on their registered mobile number and email address. The application should also track the identity of the system used by the subscriber to apply the signature. If the signature is applied from a new system for the first time, an alert should be sent to the user through SMS and email. These measures can help in the early detection of fraudulent activities related to electronic signatures.
3. It is suggested that the Application Owner should carry out a Vulnerability Assessment and Penetration Test of their PKI enabled applications

12. Root Certificate

Root certificates necessary for signature verification can be downloaded from the website rootcertificate.cca.gov.bd and stored locally within the application or database. The current certificates include Root CA Bangladesh 2018 and Root CA Bangladesh 2020. Organizations should establish procedures to ensure that no root certificates are trusted without proper authorization and authentication.



13. CA Certificates

The CA certificates may also be downloaded from the websites of the respective CAs and locally stored after path validation, and revocation status (CRL/OCSP response) checking.

14. Revocation Information

1. The revocation status of certificates can be verified using Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) responses. The Controller of Certifying Authorities (CCA) provides revocation information for CA certificates, while individual CAs provide revocation information for their sub-CA and subscriber certificates. The relevant revocation information link is also included within the certificate.
2. Application Owners should assess whether their applications require local storage of Certificate Revocation Lists (CRLs), Online Certificate Status Protocol (OCSP) responses, or both, as provided by Certifying Authorities (CAs). All licensed CAs offer CRL and OCSP services.
3. For revocation status verification using OCSP responses, Certifying Authorities (CAs) typically include a validity period in the response data (8 hours for sub-CAs and CAs). Applications can rely on these OCSP responses and utilize them locally within their specified validity period.
4. To validate the certificate used for a signature, the corresponding revocation information relevant to the time of signing must be accessible. If verification requirements extend beyond the application, OCSP responses can be used. An OCSP response included in the signature fulfills the need for revocation information. For verification limited to the same application, CRLs can be utilized. Although CRLs are typically not included in the signature due to their size, they can be archived and made available within the application for verification purposes.
5. When using CRLs in applications, the application should periodically download and store CRLs from the Certifying Authorities (CAs). CRLs must be downloaded before their expiry date (next update date). It is recommended to download and cache CRLs at least once every 24 hours to ensure up-to-date revocation information.

15. Registration of Digital Signature Certificate

To enable digital signatures in an application with a user base, a robust registration process should be implemented. The application must ensure that the Digital Signature Certificate (DSC) is associated with the registered user and maintain the integrity of the user details over time.

16. Registration -Certificate Validity Checking

The validity of the certificate should be checked at the time of registration.

17. Registration -Certificate Path Validation

The application should accomplish the path validation up to the Root certificate and the validity of the root certificate has to be reconfirmed.

18. Registration- Certificate Revocation Status

The revocation status of the signer certificate and all the issuer certificate up to Root has to be verified to guarantee that none of the certificates in the chain are revoked.

19. Registration -Key Usage Confirmation

The application must verify that the key usage includes "Digital Signature" and "Non-Repudiation" when the certificate is intended for affixing the registrant's signature.

20. Registration -Testing and Certificate Acceptance

1. To verify the registrant's possession of the private key, the registrant must send a signed random challenge text. The Application Owner will then perform signature verification using the registrant's corresponding public key.
2. The proof of verification during registration should be archived by the Application.

21. Signature -PDF Requirements

1. A signature on a PDF document may often appear invalid due to the absence of issuer certificates or corresponding CRL/OCSP responses. To ensure consistent signature validation across different environments, it is essential to include all necessary validation information (issuer certificates and revocation details) with the signature, eliminating reliance on external dependencies.
2. The PKCS#7 signature embedded in the PDF document should follow the LTV (Long-Term Validation) format, including all issuer certificates up to the Root certificate and the corresponding revocation information (CRLs/OCSP responses).

22. Signature Creation

1. The signature should be formed as per the formats and standards specified under provisions of the Information and Communication Technology Act, 2006.
2. To ensure the interoperability and compatibility of the signatures with standard signature verification tools, no proprietary techniques should be employed i.e. double hashing, etc.
3. The date and time should be a signed component of the signature.

23. Signature Validation

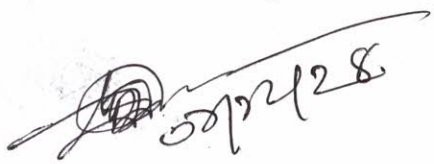
The signature validation should include the validation of the signer certificate and all issuer certificates up to the root. The following should be carried out for each certificate

(a) At the time of the creation of the signature both the signer and issuer certificates should be valid.

(b) At the time of the creation of the signature the signer and issuer certificates should not have been revoked.

(c) In cases when the signature is LTV enabled (embedded with Revocation Info), then the same should be given precedence to validate the certificate status. At the time of signature creation, the OCSP Response /CRL embedded in the signature should be valid.

(d) The signature of each certificate must be verified using its issuer's certificate. The root key certificate, being self-signed, can have its thumbprint validated against a locally stored thumbprint for verification.



(e) The key usage of the signer certificate must be verified to ensure that "Digital Signature" and "Non-Repudiation" are present in the key usage field

(f) Additionally, if revocation information is checked using an OCSP response, the signature of the OCSP responder certificate should be validated against the Issuer CA certificate.

24. Crypto Tokens

The application should support the usage of crypto tokens in all the latest versions of the client operating systems like Windows, Linux, Android, Mac, etc.

25. Precautionary Measures

The registrant must be notified of any replacement of their registered Digital Signature Certificate in the application through the mobile number (via SMS) or email registered in the application. The Business Application Owner must enforce strict internal controls, ensuring proper accountability and authenticating the registrant before replacing their certificates in the application or database. Logs of such replacements must be securely maintained. Revocation information confirming the certificate's validity at the time of registration must be archived as evidence to protect the Business Application Owner's interests in case of disputes. For CRL-based revocation information, it should be retained and made accessible for verification. If an OCSP response is used, it must be stored alongside the registration information.

26. Time Stamping

1. The term "date and time" as used in the application and the timestamping service of CA are different. In case of timestamping services of Licensed CA, a document is cryptographically signed with the national source of time embedded.
2. The timestamping service of the CA can be used to authenticate the document with proof of time.
3. The Licensed CA should provide the Timestamping Service. The service must conform to the standards of the RFC 3161 specifications and implement the request and response in an interoperable manner.

27. Long Term Validation (LTV) & Long Term Archival (LTA)

1. A Long-Term Validation (LTV) enabled signature is a signature that includes the embedded information of the signer's certificate (end-entity) along with all certificates in its trust chain, up to the CCA Root Certificate. It also contains revocation information (such as an OCSP response or CRL data valid at the time of signature creation) for each certificate in the chain. These LTV-enabled signatures allow applications to validate the signature without requiring online connectivity to the CA or other external resources, ensuring easier and more reliable verification over an extended period.
2. A Long-Term Archival (LTA) enabled signature includes all the features of an LTV-enabled signature and is additionally timestamped by a trusted Time-Stamping service operated by a Licensed CA. It also contains the embedded TS certificate, its trust chain up to the CCA Root Certificate, and the revocation information (such as an OCSP response or CRL data valid at the time of signature creation) for each certificate in the chain. This comprehensive

information is embedded within the signature to enable applications to validate and trust the timestamp of the signature at any point in the future. In addition to the benefits of LTV, LTA ensures the integrity of the signature's timestamp, providing assurance of the time of signing.

3. The technical compliances of the electronic signature structure for LTV and LTA should be in accordance with interoperable standards (e.g. RFC 3126), to ensure validation of the signature through any applications.
4. Application owner should assess documents of the organization and find the necessity of archiving a document for long-term and time stamping.

28. Audit

The audit of the application regarding the signature function may be carried out by the empaneled auditors of CCA Bangladesh in compliance with the PKI Auditing Guideline.

29. e-Sign-Based Signature Integration

1. The eSign-enabled application integration is as per the ASP-ESP agreement and this document is not applicable.

2. The eSign Service Provider (ESP) provides LTV-enabled signature responses in the case of PKCS#7 response formats, in line with CCA e-Sign API Specification Part 1: E-Signature for online e-KYC.

30. Miscellaneous

a) Government Paperwork Elimination-

1. Use And Acceptance of Electronic Signatures by Executive Agencies-

a) **Development of Procedures-** The CCA shall, in consultation with the relevant authorities, develop and implement procedures for the use and acceptance of electronic signatures by agencies.

b) Requirements for Procedures-

The procedures developed under sub-paragraph (A)--

I. shall be compatible with standards and technology for electronic signatures that are generally used in commerce and industry and by State governments;

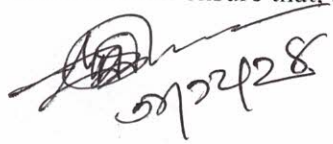
II. may not inappropriately favor one industry or technology;

III. shall ensure that electronic signatures are as reliable as is appropriate for the purpose in question and keep intact the information submitted;

IV. shall provide for the electronic acknowledgment of electronic forms that are successfully submitted; and

V. shall, to the extent feasible and appropriate, require an executive agency that anticipates receipt by electronic means of 50,000 or more submittals of a particular form to take all steps necessary to ensure that multiple methods of electronic signatures are available for the submittal of such form.

c) **Deadline For Use and Acceptance of Electronic Signatures-** The CCA in consultation with ICT Division shall ensure that agencies provide--



i. for the option of the electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper; and

ii. for the use and acceptance of electronic signatures, when practicable.

2. **Electronic Storage and Filing of Employment, Procurement, Tax Return, Service Request Forms**- The CCA shall, in consultation with the stakeholders, develop and implement procedures to permit public and private employers to store and file electronically with a forms containing information pertaining to the relevant activity.

3. **Study On Use of Electronic Signatures**- The CCA shall, in consultation with the licensed CAs and the relevant authorities, conduct an ongoing study of, and periodically report to ICT Division, the use of electronic signatures under this sub-section on--
   a) paperwork reduction and electronic commerce;
   b) individual privacy; and
   c) the security and authenticity of transactions.

4. **Enforceability and Legal Effect of Electronic Records**- Electronic records submitted or maintained in accordance with procedures developed under this sub-section, or electronic signatures or other forms of electronic authentication used in accordance with such procedures, shall not be denied legal effect, validity, or enforceability because such records are in electronic form as per the ICT Act 2006.

b) **Electronic Government**- The CCA shall, assisted by the PKI Implementation Committee and other interested persons as selected by the CCA with approval from ICT Division, monitor the implementation of the requirements of sub-section (b), the Electronic Signatures in relevant Act, and related laws to ensure that the Ministries/Divisions/Departments/Public and government Organizations--

   1. develops and maintains an efficient and effective information infrastructure for undertaking government operations using PKI;

   2. provides efficient and effective means for members of the public to interact with the public / private entities by means other than electronic information processes; and

c) manages its increasing reliance on information technology in a manner consistent with the purposes and requirements of Government of Bangladesh

d) **Establishment/Study of Standard Setting Process**- The CCA shall, in consultation with the CAs, establish a process for periodic review and study of the standards setting process and report to the ICT Division on the efficiency and effectiveness of the process and any recommendations for improving the process.

Acronyms

CCA	Controller of Certifying Authorities
CA	Certifying Authority
DSC	Digital Signature Certificate
CSR	Certificate Signing Request
e-KYC	Electronic Know Your Customer
ESP	e-Sign Service Provider
BA	Business Application
LTA	Long-Term Archival
LTV	Long-Term Validation
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
OCSP	Online Certificate Status Protocol
CRL	Certificate Revocation List