ELECTRONIC SIGNATURE - APPLICATION INTEGRATION GUIDELINES

Version 1.0

21-OCT-2022

Controller of Certifying Authorities

Ministry of Electronics and Information Technology

Document Control

Document Name	ELECTRONIC SIGNATURE -APPLICATION INTEGRATION GUIDELINES
Status	Release
Version	1.0
Release Date	21.OCT.2022
Last update	21.OCT.2022
Document Owner	Controller of Certifying Authorities, India

Contents

1	**GENERAL**
1.	The scope of this document is to provide information on the essential steps to be followed for planning and implementation of electronic signatures in organizational applications and having a registered user base.
2.	In the case of the scope of the electronic signature is limited to implementation within an organisational application, the organisation has a role in maintaining the information related to the signature keys and digital signature certificate held by the organisational persons. This document also provides a procedure to be followed for custody and record keeping requirements of encryption certificates. The PDF signature related aspects are covered in this document; the same principles can be applied to XML, CMS, and other signature formats also.
3.	An overview of the electronic signature framework as it exists under the provisions of the IT Act may be found in the Electronic Signature Framework document ESF.PDF.
4.	As per Information Technology Act, the Digital Signature Certificate means the DSC issued by a Licenced CA. The Application Owners should allow only the use of Digital Signature Certificates issued by Licensed CAs in their application.
5.	An electronic Signature is to be created using the private key corresponding to the public key certified by a Licensed Certifying Authority. The safe custody of the crypto token containing the signature keys is the responsibility of the subscriber.
6.	The signature to be affixed to a document should be created in a manner as specified in the End Entity Signature Rules.
7.	In an Electronic Signature enabled application, the Application Owner should accept DSCs issued by any of the Licensed CAs as long as they belong to the specified class or higher. If the application has specified any specific services associated with DSC, the same should be satisfied.
8.	The validity of the signature is determined based on the time of affixing an electronic signature on the electronic document. Hence the certificate should be valid, not expired, and not revoked at the 'time of affixing the signature'.
9.	The non-availability of a token or revocation or expiry of the certificate after affixing the electronic signature does not affect an already signed document
10.	For tender-related requirements, Application Owners should not impose any additional requirements of DSC fields or private key storage requirements other than those mentioned in the Guidelines issued by CCA. The certificates issued by Licensed CAs should be compliant with Interoperability guidelines issued by the CCA, and no deviations should be imposed in such certificates.
11.	Application Owners should also accept higher class certificates if lower class certificates of the same were specified by them for their application. The DSCs issued by Licensed CAs hold the same assurance level for the same class of certificates.
1.1	**SIGNATURE REQUIREMENTS SCENARIOS**
1.	The signature requirements of the applications broadly fall under the following scenarios
	(a) The creation and verification of electronic signatures are under the control of the same application and there are no additional requirements.

	(b) The creation and verification of electronic signatures are under the control of the same application but the signatures are verifiable by any relying party.
	(c) Only verification of the electronic signature is carried out by the application.
	(d) The combination of one or more of the above.
2.	The planning relating to verification information like (CRL/OCSP), the signature type, rendering mechanism, etc. should be based on the above categorization.
1.2	**TYPES OF CERTIFICATES**
1.	Certificates issued by CAs are used for an Individual's Signature, encryption, web server authentication, device authentication, bulk document signature, etc. The individual Signature Certificates are referred to as Signature Certificates in this document. • The Signature Certificates are issued for affixing a signature on an electronic document which is equivalent to an ink signature in the paper world. • Encryption certificates are used to encrypt electronic documents. • Webserver certificates, commonly known as SSL certificates, are used to secure websites. • The device certificates are used for confirming the authenticity of the device. • The document signer certificates are issued to Organisational software for bulk signature (e.g. receipt generation, where no individual's signature is required). The Signature Certificates contain the name & address of the applicant. The certificate usage in the organization requires the office address to be present in the certificate, such certificates being known as organisational person Signature Certificates. The Digital Signature Certificates issued by CAs to individuals with residential addresses are known as personal Signature Certificates.
1.3	**DIGITAL SIGNATURE CERTIFICATES**
1.	The signature keys associated with signature certificates are to be generated and stored in a crypto token. As per the provisions of the IT Act, the signature keys should always be in the custody of the DSC applicant. The DSC applicant should request for revocation of DSC to Issuer CA in the case of transfer or missing token or superannuation or any other. In case, the officer is not available (death, illness, etc), the department/Organization should request to CA for revocation of DSC. The issuer CA should revoke the signature certificate on receipt of an authorised request from the concerned department.
1.4	**DIGITAL SIGNATURE - CLASS OF CERTIFICATES**
1.	Based on risk analysis and security requirements for the applications and relying parties, Application Owners should decide the Assurance Level (Class) of the Digital Signature Certificate suitable for them.
2.	CAs are issuing Class 3 individual digital signature certificates in a crypto token which automatically carries the assurance of Class 2 & Class 1 certificates also.
3.	As the Class 3 individual digital signature certificate covers the requirement of the Class 2 certificate also, there is no need of obtaining the Class 2 individual certificate separately.
1.5	**DIGITAL SIGNATURE CERTIFICATES - LEGAL VALIDITY OF SIGNATURE**
1.	The validity of the electronic signature under the IT Act is ensured only when the signature is

	applied in the manner specified in the End Entity Signature Rules and also the associated certificate is issued by a Licenced Certifying Authority.
1.6	**DIGITAL SIGNATURE CERTIFICATES - CA SERVICES**
1.	The crypto tokens holding the signature keys of subscribers may become unavailable for signature due to damage, loss, or other unforeseen reasons during the certificate validity period. CAs are liable for the re-issuance of such certificates at least once free of cost during the certificate validity period. If Application Owners, to have a smooth operation, desires to have an unlimited number of re-issuances by CA, the same may be specified as a condition of purchase.
2.	The Application Owners should determine the requirements of local storage of CRLs or Online Status Service Protocol (OCSP) responses offered by CAs or both in their applications. CRL and OCSP services are provided by all licensed CAs.
3.	To time-stamp electronic records, Timestamping services offered by Licenced CAs should be availed.
4.	As the signature-related software components and functions require core expertise in PKI development and security, the same can also be availed from third-party PKI tools & service providers in that area and integrated with the applications.
1.7	**DIGITAL SIGNATURE CERTIFICATES - ROLES & RESPONSIBILITIES OF APPLICATION**
1.	To get a digital signature certificate from a CA, the applicants are required to create a KYC account with CA. In cases of organisational application usage of organisational person certificates, the details required for the revocation of the certificates should be preserved by the organisation. To meet exigencies, such details should include the certificate serial number, validity, and authorization of the organisation by the subscriber for revocation.
2.	The organisation should put a procedure in place for revocation of certificates when the organisational persons holding the certificate have a status change concerning the organisational details mentioned in the certificate.
3.	The organisation should not mandate the transfer of signature keys & certificates to any other person. The Signature Certificate should be used only by the subscriber.
4.	The application should not have any requirements for custody of crypto tokens containing signature certificates by anyone other than the subscriber.
5.	The Application Owners should identify the operating systems and browsers likely to access their application and accordingly provide support to the client components for a smooth operation.
1.8	**DIGITAL SIGNATURE CERTIFICATES - APPLICATION FUNCTIONAL REQUIREMENTS**
1.	Considering the sensitive nature and potential misuse related to electronic signatures, it is recommended that the application may implement two-factor authentication.
2.	In the case of occasional use of electronic signature requirements in the application, the application should send an SMS message & email to the signer on the registered mobile no & email. The application may keep track of the identity of the system used by the subscriber for applying signature and in the case of first use in a new system, an alert should be sent to the user via SMS/email. This may help in the early identification of fraudulent activities concerning electronic signatures.

3.	The application should synchronize their time with the National source of time. For signatures, the server time should be used rather than the local client time.
4.	It is recommended that the Application Owner should carry out a Vulnerability Assessment and Penetration Test of their electronic signature-enabled applications
1.9	**ROOT CERTIFICATE**
1.	The root certificates required for signature verifications may be downloaded from the website, https://cca.gov.in and stored locally in the application/database. The present certificates are CCA India 2014 &, CCA India 2022. The local storage of Root CA certificates should be controlled only by authorised persons. The organisation should implement procedures in place to ensure no root certificates will be trusted without due authorization and authentication.
1.10	**CA CERTIFICATES**
1.	The CA certificates may also be downloaded from https://cca.gov.in and locally stored after path validation, and revocation status (CRL/OCSP response) checking.
1.11	**REVOCATION INFORMATION**
1.	Revocation status can be verified using CRLs or OCSP responses. CCA provides revocation information of CA certificates and CAs provide revocation information of their subCA and subscriber certificates. The corresponding revocation information link is available in the certificate also.
2.	For signature verification, the revocation status of the signer certificate, subCA certificate & CA certificate should be carried out.
3.	In the case of OCSP response for revocation status, CAs generally provide OCSP response with a validity time (8 hours for subCAs & CAs) as a part of the OCSP response data, and the same can be relied on. Applications can use the OCSP responses locally during the validity time of such responses.
4.	To validate the certificate used for signature, the corresponding revocation information, relevant to the time of signature, should be available. In case the verification requirements are external to the application, OCSP responses may be used. The OCSP response, if included in the signature, satisfies the requirements of revocation information. In case of the verification of a signed document is limited to the same application, the application may use CRLs. The CRLs are generally not included in the signature as they are large; however, they may be archived & available in the application for verification.
5.	In the case of CRL usage in applications, the application should periodically download CRLs from the CAs and store them. The download of the CRL should not be later than the expiry date (next update date) of the CRL. It is, however, recommended to download and cache CRLs, at least once every 24 hours.
1.12	**REGISTRATION OF DSC**
1.	To enable digital signatures in the application having a user base, a registration process should be followed. The application should implement measures to ensure the DSC belongs to the registered user and also maintain the integrity of the registered details subsequently. This can be implemented by cross-verifying the details in their database with the information included in the certificate like Name, address, PAN, mobile, email ID, Aadhaar Number (last

	four digits), etc.
1.13	**REGISTRATION -CERTIFICATE VALIDITY CHECKING**
1.	The validity of the certificate should be checked at the time of registration. The certificate should be valid at the time of registration.
1.14	**REGISTRATION -CERTIFICATE PATH VALIDATION**
1.	The application should perform the path validation up to the Root certificate and the genuineness of the root certificate to be reconfirmed.
1.15	**REGISTRATION- CERTIFICATE REVOCATION STATUS**
1.	The revocation status of the signer certificate and all the issuer certificate up to Root is to be verified to ensure none of the certificates are revoked.
1.16	**REGISTRATION -KEY USAGE CONFIRMATION**
1.	The application should ensure that the key usage includes “Digital Signature” & “Non-Repudiation” if the intended use of the certificate is for affixing the signature of the registrant.
1.17	**REGISTRATION -TESTING AND CERTIFICATE ACCEPTANCE**
1.	To confirm the possession of the private key with the registrant, the registrant shall send a signed random challenge text, and the signature verification using the corresponding public key of the registrant shall be carried out by the Application Owner.
2.	The proof of verification at the time of registration should be archived by the Application.
1.18	**SIGNATURE FORMATS**
1.	The signed documents are subject to verification by the organisational application or external relying parties at a later point in time. In both cases, the information required for verification of a signature certificate such as issuer certificates and corresponding revocation information should be available. The standard or extended signature formats are used to address these scenarios.
2.	In case the signature creation and verification are internal to the same application, a standard signature format can be used where the current and historic issuer certificates & revocation information are available within the application. However extended signature formats can be used to enable portability even if the immediate requirements are internal to the application.
3.	The extended signature format enables signature verification to happen externally to the control of the signer’s application by including signature verification information such as issuer certificates and revocation information as a part of the signature. The PDF(LTV) format mentioned in this document could address these requirements
1.19	**SIGNATURE -PDF REQUIREMENTS**
1.	The signature affixed on a PDF document is often shown as invalid due to the unavailability of all the issuer certificates or corresponding CRL/OCSP responses. To have a consistent signature validation in a different environment it is necessary to make available all the validation information (issuer certificates & revocation information) along with the signature to eliminate external dependencies.
2.	The PKCS#7 signature to be created in the PDF document should include (LTV Format) with all the issuer certificates up to the Root certificate and corresponding Revocation Information (CRLs/OCSP responses).

3.	For PDF signature, where the number of CRL entries is more than 5, it is recommended to use OCSP responses to reduce the size of the signature. The revocation information should be included as a signed attribute under pdfRevocationInfoArchival (1.2.840.113583.1.1.8).
1.20	**SIGNATURE CREATION**
1.	The signature should be created as per the formats and standards specified under provisions of the Information Technology Act.
2.	To make signatures interoperable and compatible 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 part of the signature.
1.21	**SIGNATURE VALIDATION**
1.	The signature validation should include the validation of the signer certificate and all issuer certificates including root. The following should be carried out for each certificate
	(a) The signer certificate and issuer certificates should be valid at the time of the creation of the signature.
	(b) The signer certificate and issuer certificates should not have been revoked at the time of the creation of the signature.
	(c) If the signature is LTV enabled (embedded with Revocation Info), then the same should be given priority to validate the certificate status. The OCSP Response /CRL embedded in the signature should be valid at the time of signature creation.
	(d) The signature on each certificate should be verified with its issuer certificate. The root key certificate is self-signed. The thumbprint of the Root certificate may be verified using a locally stored thumbprint.
	(e) The key usage of the signer certificate should be checked to confirm the presence of "Digital Signature" and "Non-Repudiation" in the key usage field of the certificate.
	(f) If the Revocation Information checking is based on OCSP Response, the signature of the OCSP responder certificate should be verified with the Issuer CA certificate. There is no need of checking the revocation status of the OCSP responder certificate.
1.22	**CRYPTO TOKENS**
1.	The individual signature certificates are issued to subscribers by CAs in a crypto token. As per the guidelines issued by CCA, CAs empanel the specific crypto token product and identifies the token details before issuance of DSC. As a part of empanelment, the crypto token providers are required to make available token management software, and OEM-specific drivers supporting Windows, Linux, Android, and Mac in a downloadable form at their locations.
2.	To enable signers to perform the signature functions, provided by the organisational application, using the crypto token, in their local system, the token drivers are required to be installed. These drivers are provided by OEM of crypto tokens.
3.	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.
1.23	**PRECAUTIONARY MEASURES**
1.	The replacement of the registered DSC in the application should be communicated to the

	registrant via mobile (SMS)/email registered in the application.
2.	The Application Owner should implement strict internal accountability and authentication of the registrant for replacement of the registrant's certificates in their application/database. The logs of such replacements should be protected
3.	The revocation information evidencing the validity of the certificate at the time of registration should be archived as proof to safeguard the interest of the Application Owner to produce in the case of any dispute. In the case of CRL-based revocation information, it should be made available for verification and if OCSP response is used, it should be stored along with registration information.
1.24	**TIMESTAMPING**
1.	The term "date and time" as used in the application is different from timestamping service of CA. With timestamping services of Licensed CA, a document is cryptographically signed with the national source of time embedded.
2.	The timestamping service of the CA may be used to make the document authentic with proof of time.
3.	The Timestamping Service should be availed from the Licensed CA. The service shall be used as per RFC 3161 specifications and implement the request and response in an interoperable manner.
4.	The Time Stamp responses should be LTV Enabled, which means, it should include all the chain certificates (till root), as well as revocation info for the same. The verification application should use such embedded revocation information to validate the time stamping information.
1.25	**LONG TERM VALIDATION (LTV) & LONG TERM ARCHIVAL (LTA)**
1.	Long Term Validation (LTV) enabled signature means the signature containing embedded information of the Signer's certificate (End-entity) and all its trust chain certificates until CCA Root Certificate, along with revocation information (OCSP response / CRL data valid at the time of signature creation) for each of those certificates. These LTV-enabled signatures help the applications to validate the signature without any online connectivity to the CA or any other external resource, hence making it easier for verification over a longer period.
2.	Long Term Archival (LTA) enabled signature means the signature enable with LTV and additionally Time Stamped via a trusted time-stamping authority (TSA) operated by a Licensed CA, along with an embedded TSA Certificate, its trust chain until CCA Root certificate, and the revocation information (OCSP response / CRL data valid at the time of signature creation) for each of those certificates. This information should be part of the signature to help the applications validate and trust the time of the signature at any time in the future. In addition to the benefits of LTV, LTA assures time for the document signature.
3.	The technical compliances of the electronic signature structure for LTV and LTA should be met in line with interoperable standards (eg: RFC 3126), to facilitate validation of the signature through any application.

4.	Application owner should assess documents of the organization and identify the requirement of archiving a document for long-term and time stamping
1.26	**ENCRYPTION CERTIFICATE (EC)**
1.	The encryption keys and certificates are to be managed in a manner different from the signature keys. A backup of encryption keys and certificates should be available.
1.27	**ENCRYPTION CERTIFICATE- BACKUP REQUIREMENTS**
1.	The encryption key backup by the applicant should be carried out at the time of issuance of the certificate by CA. The CA software generates encryption keys on the system and transfers them to a token. The DSC applicant is required to keep a copy of the encryption keys and certificate.
2.	For organisational person encryption certificates, It is recommended to keep a backup copy along with a PIN by a designated Officer preferably in a sealed envelope, under lock & key.
1.28	**ENCRYPTION CERTIFICATE- ORGANISATIONAL ROLE**
1.	In the case of encryption, the token having an encryption certificate & keys may be required for decryption by the organization at a later point in time.
2.	The encryption certificates are issued to the organization person and the custody of keys is the duty of the corresponding subscribers. In case of the non-availability of keys, the already encrypted documents cannot be decrypted. The backup of encryption keys is very important for continued operation.
3.	The backup copy along with the PIN of encryption keys and certificates are to be kept by the applicant as well as by the organization. In the case of loss/damage/unavailability, the encryption keys & certificates are to be retrieved from the backup.
4.	An office procedure should be in place and to be followed for handling the non-availability of encryption certificates and corresponding keys. In case of the non-availability of an organizational person, to whom the encryption certificate was issued by the CA, the encryption certificate & corresponding keys should be used only for decryption by the organization; no further encryption should be carried out by those keys.
1.29	**ENCRYPTION CERTIFICATE - CA ROLE**
1.	From 2022 January onwards, CAs escrow encryption keys, however, it is recommended to keep a backup copy of the keys with the organization also.
1.30	**AUDIT**
1.	The audit of the application concerning the signature function may be carried out by Cert-in empanelled auditors in compliance with this document
1.31	**ESIGN-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 eSign API specifications.

****