FRAMEWORK ON ESIGNATURE

Contents

Ministry of Electronics and Information Technology
6, CGO Complex, New Delhi, India

1 Legal Framework in India for Electronic Signature

The United Nations Commission on International Trade Law adopted the Model Law on Electronic Commerce in 1996. The General Assembly of United Nations by its Resolution No. 51/162, dated 30th January, 1997, recommended that all States should give favorable considerations to the said Model Law when they enact or revise their laws. India being signatory to it revised its laws as per the said Model Law. Keeping in view the urgent need to bring suitable amendments in the existing laws to facilitate e-commerce and with a view to facilitate Electronic Governance, the Information and Technology Bill was introduced in the Parliament.

Subsequent to the Introduction of Information Technology Act, consequential amendments in the Indian Penal Code and the Indian Evidence Act, 1872 were made to provide for necessary changes in the various provisions which deal with offences relating to documents and paper-based transactions. Also amended the Reserve Bank of India Act, 1934 to facilitate electronic fund transfers between the financial institutions and banks and the Bankers' Books Evidence Act, 1891 to give legal sanctity for books of account maintained in the electronic form by the banks

The Information Technology Act was enacted on 9th June 2000 and subsequently amended in 2008. The Act came in to force from 17th Oct 2000 and the Amendment to the Act came in to force from 27th Oct 2009. The jurisdiction of the Act extends to whole of India. The main purpose of the Act is to facilitate e-Commerce and e-Governance in the country and provide a legal frame work for recognition of electronic records and digital signatures.

The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities (CA). The following are some of the functions of CCA

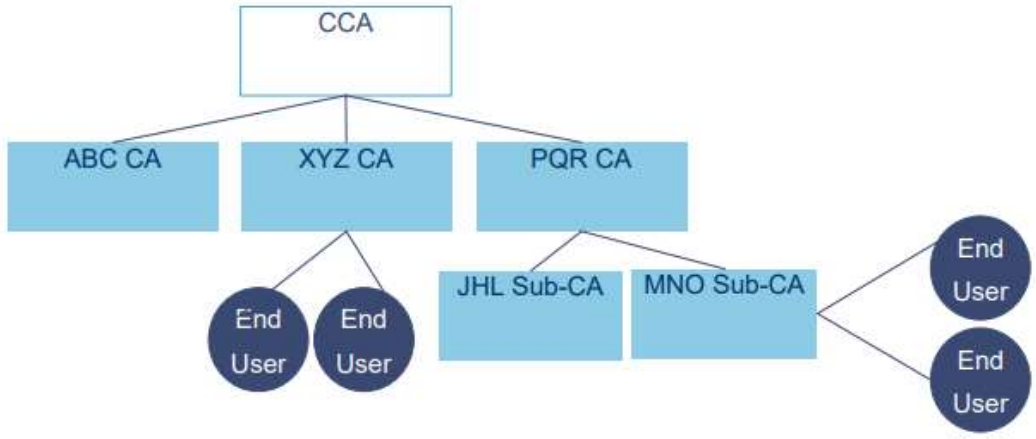
- Function as Root Certifying Authority of India
- Certifying the public keys of the CAs.
- Laying down the standards & Guidelines to be followed by the CAs,
- Licensing Certifying Authorities (CAs) and exercising supervision over their activities.
- Addressing the issues related to the licensing process
- Approving the Certification Practice Statement (CPS);
- Auditing the physical and technical infrastructure of the applicants through a panel of auditors maintained by the CCA.
- Resolving conflict of interest between CAs and subscribers

The Licence is issued for a period of 5 years. CAs are required to renew the licence after the expiry of Licence. The licence is subject to suspension, revocation and renewal. The terms and conditions for the renewal are same as fresh licence. The

licence is issued based on the eligibility criteria like net worth, paid up capital and compliance to technical and physical infrastructure in accordance with the provision under ACT.

2 Root CA

The model adopted by India is a hierarchical PKI with the trust chain starting from the Root Certifying Authority of India (RCAI). RCAI is operated by the CCA, Government of India. Below RCAI there are Certifying Authorities (CAs) licensed by CCA to issue Digital Signature Certificates under the IT Act.



There are two root hierarchy maintained by CCA. One for issuance of issuance of signature certificates and other for SSL. The root CA is operated completely in Offline mode.

3 Certifying Authorities

CAs can be private sector companies, Government departments, public sector companies, or Non-Government Organizations (NGOs). These are also called Licensed CAs. At present there are seventeen CAs licensed by Root CA and all of them are operating under same policy, standards, and verification methods, subjected to be audited by the criteria set by Root CA. The policy ids of certificates are also same for all CAs. CAs are required to provide CRL, OCSP and Timestamping Services. CAs are also not allowed to issue certificate other than that mentioned in the CPS which is approved by CCA. The certificates issued by Licensed CAs are legally valid in India.

A Certifying Authority can create sub-CAs to meet the business branding requirement. These sub-CAs, which will be part of the same legal entity as the CA, will issue certificates to the end entities or subscribers. The CAs are allowed to create ONE level of sub-CA only.

CAs are required to operate under the provisions of Act, Rules, Regulations and orders issued by CCA. The orders issued by CCA are published in the form of Guidelines

4 Electronic Signature Certificates

End user electronic signature certificates are strictly issued in a Hardware Crypto Token for a period of 1-3 years or through eSign service for creation of document signature where the validity of certificate is 30 minutes with an one-time use private key.

To obtain an Electronic Signature certificate from CA, the applicant needs to undergo a verification process as mentioned in the Identity verification Guidelines (IVG) issued by CCA and upon successful verification, CA create an eKYC account and issue electronic Signature certificate to applicant. As the verification process are online, the certificate can be obtained within 2-3 hours.

For all categories of applicants, email id, mobile number, photo, scanned copy of proof of identity and scanned copy of proof of address are required to be submitted to CA. The in-person verification is carried out by video verification or online Aadhar eKYC services.

The applicant can opt for different verification mode like Online/Offline Aadhaar, PAN, Banking and Organizational. The certificates are also issued to foreign nationals after similar verification carried out by CA on their identity, address and video.

Procedure followed for issuance of DSC to Foreign Nationals

DSCs are often required by foreign nationals to participate in the tender floated by Indian entities, or in Indian companies having foreign directors. eKYC for foreign national applicants are carried out by CAs and issue DSC to them.

An applicant is deemed as foreign applicant if the address (residential or organizational) provided in the DSC application form does not belong to India or identity document submitted is not issued by authorities under Government of India.

There are two types of certificates issued, namely:

i) Personal certificate
ii) Organizational person certificate

a) For Personal certificate, for identity proof, the scanned copy of Passport/Local Govt issued identity/PAN/OCI passport can be submitted. For the address proof, the scanned copy of passport/OCI passport/local government issued id having address/bank details having address/any utility bills in the name of applicant issued within three months/ document issued from embassy with residential address can be provided

b) For Organizational person certificate, scanned copy of Organizational id, Organizational email id, mobile number, Organizational address and letter of authorization from Organization are required. For the proof of Organizational existence, publicly verifiable and listed/recognized by local government reference of Organization in database/registry need to be provided.

CA carries out video verification, document verification (all the originals shall be verified during the video verification). Mobile number and Email verification. An eKYC account is created at CA up on successful verification and DSC is issued to applicant. The DSC issuance process 1-2 hour depending the applicant's availability for video and telephonic verification.

The options available for storage of applicant's signature keys are below

Sl	**Storage Medium (FIPS Level 2 or higher)**	**Details**
1	Crypto Token	Under the physical possession by applicant, valid for 2-3 years
2	HSM (CA)	held by CA HSM, activation only after subscriber authentication (still to be operational) valid for 2 years
3	HSM (CA)	eSign service, one-time key generation and deletion immediately after signature creation, certificate is valid for maximum of 30 minutes

Apart from Individual signature certificates, CAs issue other special types certificates for different usage scenarios. The following types of certificates are issued by CAs.

SL	**Type of certificate**	**Issued for**

1.	End User Certificate (issued for personal use)	Affixing individuals electronic Signature
2.	End User Certificate (issued for organization use)	Affixing individuals electronic Signature
3.	System Certificate	Machine to machine authentication
4.	Time Stamping Authority Certificate	Generating Timestamp Token
5.	Code Signing Certificate	Signing of software code
6.	OCSP Responder Certificate	OCSP response Signature
7.	Encryption Certificate	Key Encryption
8.	Document Signer Certificate	Organizational application signature
9.	SSL Certificate	Secure Communication

Depending on the level of assurance required, application owners can opt for different class of certificates for the use in their application. The following are the different Assurance level of Certificates

Assurance Level	**Assurance**	**Applicability**
Class 1	Class 1 certificates shall be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.	This provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance.
Class 2	These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial
Class 3	This certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value

	issued to individuals only on their personal (physical) appearance before the Certifying Authorities.	transactions or high levels of fraud risk.
eKYC-Single Factor	eKYC -Single Factor class of certificates shall be issued based on Single Factor authentication of subscriber to the applicable eKYC services. These certificates will confirm that the information in Digital Signature certificate provided by the subscriber is same as information retained in the eKYC databases pertaining to the subscriber	This level is relevant to environments where Single Factor authentication to eKYC service is acceptable method for credential verification prior to issuance of DSC. Certificate holder's private keys are created on hardware and destroyed immediately after one time usage at this assurance level.
eKYC-Multi Factor	eKYC -Multi Factor class of certificates shall be issued based on Multi Factor authentication of subscriber to the applicable eKYC services. These certificates will confirm that the information in Digital Signature certificate provided by the subscriber same as information retained in the eKYC databases pertaining to the subscriber.	This level is relevant to environments where Multi Factor authentication to eKYC service is acceptable method for credential verification prior to issuance of DSC. Certificate holder's private keys are created on hardware and destroyed immediately after one time usage at this assurance level

5 Electronic Signatures

Creating trust in electronic environment involves assuring the transacting parties about the integrity of the content of documents along with authentication of the sending and receiving parties in a manner that ensures that both the parties cannot repudiate the transaction. The paper-based concepts of identification; declaration and proof are carried forward in the electronic environment through the use of electronic signatures. For an electronic signature to be legally accepted reliable it shall possesses the following requirements:

1. The signature creation data or the authentication data are, within the context in which they are used, linked to signatory or, as the case may be, the authenticator and no other person
2. The signature creation data or the authentication data were, at the time of signing, under the control of signatory or, as the case may be, the authenticator and no other person
3. Any alteration to the electronic signature made after affixing such signature is detectable and

4. Any alteration to the information made after its authentication by electronic signature is detectable

Under the provision of Act, standards have been prescribed for affixing signature on document. The IT Act 2000 originally recognized only Public Key Cryptography based Digital signatures as legal. The Information Technology (Amendment) Act, 2008, technology-neutral and recognizes electronic signatures which are notified under the Rules. At present PKI is the only technology, which qualifies as an electronic signature under the IT Act. The electronic documents that have been digitally signed are treated at par with paper documents signed in the traditional way.

As per the IT Act, Section 5, for legal recognition, electronic record requires to be authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government. The manner of authenticating electronic records have been specified under Digital Signature (End entity) Rules, 2015

If electronic records are to be retained for a longer period, a timestamp shall be applied in such manner as specified under Digital Signature (End entity) Rules, 2015

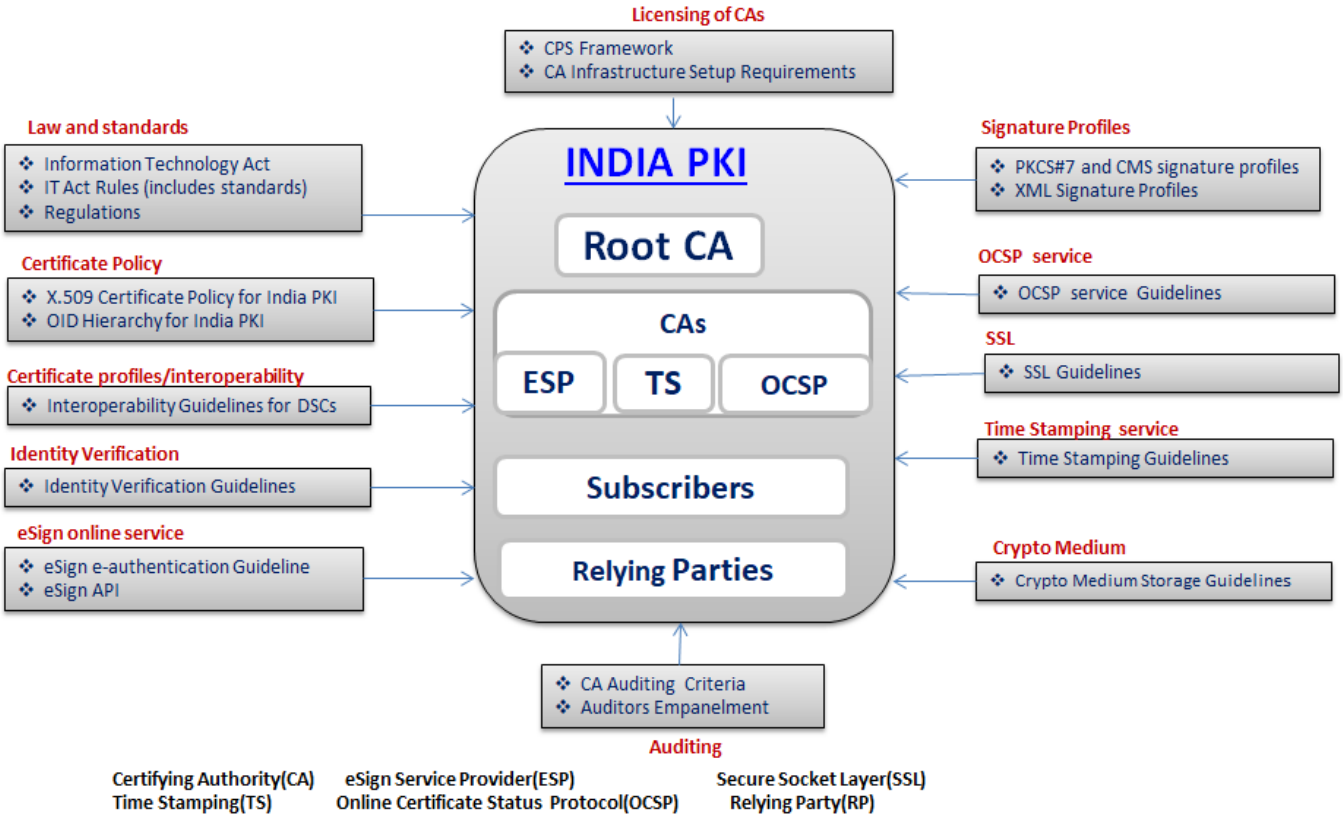
The application owners are required to determine the level of assurance required for their application with respect to the verification followed prior to issuance of Certificates

The standards to be followed for electronic signature certificates and Electronic signatures are given below

PKI Standards
Public Key Cryptography • RSA – Asymmetric Cryptosystem • Elliptic Curve Discrete Logarithm Cryptosystem
Digital Signature Standards • RSA and EC Signature Algorithms • SHA-2 – Hashing Algorithms
Directory Services (LDAP Ver 3) • X.500 for publication of Public Key Certificates and Certificate Revocation Lists • X.509 version 3 Public Key Certificates • X.509 version 2 Certificate Revocation Lists
PKCS family of standards for Public Key Cryptography from RSA • PKCS#1 – PKCS#15
Federal Information Processing Standards (FIPS) • FIPS 140- 1/2 Security Requirement of Cryptographic Modules

6 Electronic Signatures Policy Framework

A pictorial representation and a brief description of policies applicable to CA, electronic Signature Certificate and Electronic Signature are given below



1. In India PKI hierarchy, have two separate trust chains one for one end-entity certificates and one for SSL. There are seventeen Licensed CAs which are operated in the different parts of the country. The types of certificates issuance by CAs are given at https://cca.gov.in/CAServicesOverview.html
2. CAs are operated under single India PKI Policy. There is no separate policy for any of the licensed CA by Root CA. India PKI policy is published at https://cca.gov.in/sites/files/pdf/guidelines/CCA-CP.pdf
3. The verification requirements prior to issuance end-entity certificates are governed by Identity Verification Guidelines specified by Root CA. Licensed CAs are required to adhere to these Guidelines for issuance of any certificate. ref https://cca.gov.in/sites/files/pdf/guidelines/CCA-IVG.pdf
4. The certificate policy for India PKI covers the policy Id given to each class of certificates which are common across all CA and adhere to India PKI CP. The policy Ids are published at https://cca.gov.in/sites/files/pdf/guidelines/CCA-OID.pdf
5. To facilitate interoperability, Root CA has specified "DSC interoperability Guidelines for issuance certificates under the Root Chain. A detailed specification for end entity and SSL certificates are covered under DSC

interoperability Guidelines specified by Root CA and the same is followed by each sub-CA. DSC Interoperability, SSL, OCSP and Signature profiles can be seen on the following links, which are to be adhered by all the Licensed CAs.

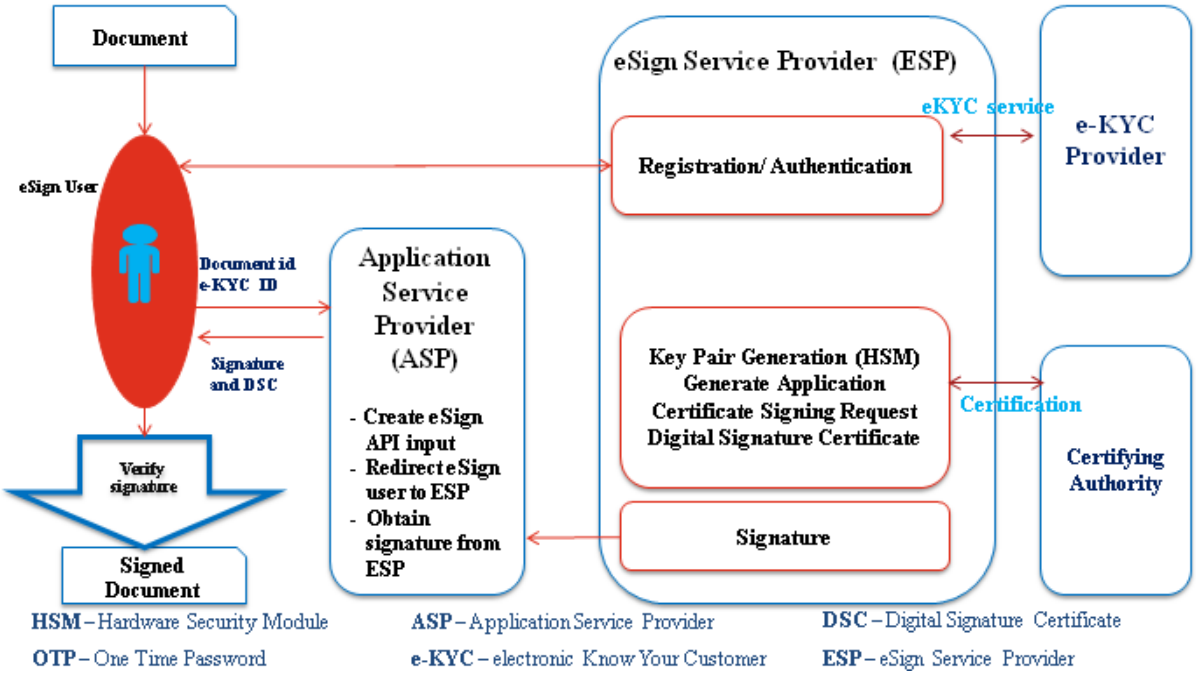
Cert profile: https://cca.gov.in/sites/files/pdf/guidelines/CCA-IOG.pdf
OCSP: https://cca.gov.in/sites/files/pdf/guidelines/CCA-OCSP.pdf
SSL https://cca.gov.in/sites/files/pdf/guidelines/CCA-SSL.pdf
Signature: https://cca.gov.in/sites/files/pdf/guidelines/CCA-SP.pdf

6. Under the provisions of IT Act Controller to license the Certifying Authorities and also to ensure that none of the provisions of the Act are violated. Audits are carried out to ensure the adherence to Information Technology Act 2000, the rules and regulations thereunder, and guidelines issued by the Controller from time-to-time. Auditing of the physical and technical infrastructure of CA is carried out through a panel of auditors maintained by the CCA. The audit reports are submitted to Root CA directly by auditors. The criteria for the audit include WebTrust and CAB requirements. The audit criteria specified by Root CA. is available at Audit Criteria: https://cca.gov.in/sites/files/pdf/guidelines/CCA-CAAC.pdf

7. In order to establish a single national policy, Root CA has already laid down common CPS template for sub-CAs. Each CA will have their own CPS and have provided links to policy, procedure, guidelines of Root CA. The CPS are available in the disclosure records of each CA published https://cca.gov.in/licensed_ca.html

7 eSign

eSign is an online Electronic Signature Service, based on successful authentication of individual using e-KYC services, the key pairs generation, the certification of the public key based on authenticated response received from e-KYC services, and digital signature of the electronic document are facilitated by the eSign online Electronic Signature Service provider instantaneously within a single online service. The key pairs are used only once and the private key is deleted after one time use. The Digital Signature Certificates are of 30 minutes validity, and this makes verification simple by eliminating the requirements of revocation checking. Document that is signed using eSign will contain a valid digital signature that can be easily verified using standard methods.



With eSign Service users are expected to submit the document hash and provide Aadhaar authentication or CA authentication. Upon success authentication CA generate a key pair for user, obtain certificate from CA, generate Certificate and send the signature and Electronic Signature Certificate to the signer for affixing in their document. The keys are deleted immediately after the signature creation. The signed information is packaged in a format as requested by user. CA include all the information required for verification of signature like CRL OCSP response along with Signature This enable relying parties to verify the signature without making external information provided that the Root certificate is locally available in the trusted store.

eSign was started with eKYC service provider as UIDAI where applicant provide OTP or Biometric authentication to UIDAI and in response eKYC information received by CA. Subsequently the enabling provision under IT was amended to include other eKYC services. Now CA can also verify the applicant and maintain eKYC information which is used by subscribers for subsequent eSign service or DSC issuance

1. Aadhaar Authentication

   The Unique Identification Authority of India (UIDAI) is a statutory authority established under the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (“Aadhaar Act 2016”) on 12 July 2016 by the Government of India, under the Ministry of Electronics and Information Technology (MeitY). UIDAI was created to issue Unique Identification numbers (UID), named as "Aadhaar", to all residents of India. The UID had to be (a) robust enough to eliminate duplicate and fake

identities, and (b) verifiable and authenticable in an easy, cost-effective way. As on 31st October 2021, the Authority has been issued 131.68 crore Aadhaar numbers to the residents of India.

UIDAI provides a mechanism to verify identity of an Aadhaar number holder through an online electronic KYC service. The e-KYC service provides an authenticated KYC details is in machine readable XML which is digitally signed by UIDAI allowing agency to verify its authenticity and detect any tampering. The agency can also authenticate the user through their own OTP/Face authentication mechanisms.

2. CA eKYC account creation and authentication

   One time registration of applicant and subsequent use for a period of 2 year is expected in this option. With this option, applicants are required to submit the information to CA and CA carryout a verification to establish the information submitted by the applicant is genuine. For verification CA may rely on the information received from the publicly trusted database like Income Tax database, Bank Database to cross verify the information submitted by the applicant. For in-person verification, a direct online video verification is used and also carryout face matching with the photo submitted or contained in the other supporting documents. CA may employ one or more of the following online verification mechanisms

   1. Offline Aadhaar authentication
   2. Online Aadhaar authentication
   3. PAN (Income tax)
   4. Bank KYC online
   5. CA direct verification for Foreign Nationals

   Upon successful verification of applicant, CA create an eKYC account for the user with user name and password with authentication option as one or more of the following

   1. PIN & SMS-OTP,
   2. PIN &T-OTP,
   3. PIN &Mobile Access Tokens (MAT),
   4. PIN & FIDO
   5. PIN &Public Key Authentication.

Once the eKYC account with CA is created, user can directly authenticate with CA and perform eSign or obtain DSC

eSign Electronic Signature Service is an innovative initiative for allowing easy, efficient, and secure signing of electronic documents by authenticating signer

using Aadhaar eKYC or other approved eKYC services. With this service, any Aadhaar holder can digitally sign an electronic document. Application Service Application Service providers can easily integrate eSign service and provide signature capability to their users.

The relevant Guidelines for eSign Services are given below

Sl	Guidelines/Link
1	Notification
2	e-authentication guidelines for eSign
3	eSign API 2.1 (Aadhaar based authentication)
4	eSign API 3.3 (CA eKYC based authentication)
5	eSignRemote 1.0 (Remote Key storage)
4	eSign Framework

8 Time stamping

The National Physical Laboratory, India (NPLI), is responsible for maintenance and development of the Indian Standard Time (IST). NPLI maintains the time scale of Indian Standard Time (IST) with the help of a commercial cesium atomic clock. The time scale maintained by NPL is designated as UTC.

CAs are required to derive time from national time source for their use in issuance of electronic signature certificate and eSign Service. Also, the time included in the time-stamp token shall be synchronized with Standard Time Source within the accuracy of ± 1 second

CA are providing time stamping service in compliance with RFC 3161.The time-stamp token include a representation (e.g., hash value) of the datum being time-stamped as provided by the time stamp requestor/subscriber. The guidelines issued by CCA to CAs are available at https://cca.gov.in/sites/files/pdf/guidelines/CCA-TSG.pdf

9 Foreign CA Regulations

For a Digital Signature Certificate issued by a Foreign Certifying Authority to be recognized in India, notification contains two sets of Regulations –

1. Foreign Certifying Authorities operating under a PKI Regulatory Authority comparable to that in India [G.S.R. 204(E) dated 6th April, 2013].
2. Foreign Certifying Authorities which are not operating under a PKI Regulatory Authority [G.S.R 205(E) dated 6th April, 2013]

The Intention is to provide seamless authentication, message integrity, non-repudiation, & accessibility across jurisdictions facilitating e-commerce* & e-Governance

The following are the highlights of two sets of Regulations

Recognition of CA operating under a Regulatory Authority
A foreign CA deemed as recognized if it has been authorized to issue DSCs by a recognized Regulatory Authority established under the laws of a country other than India. [Regulation 3A (2)]
Recognition of Foreign Certifying Authorities operating under a Regulatory Authority is based on Principle of reliability & reciprocity. Recognition of Foreign Certifying Authorities if the laws of the country under which such regulatory authority is established require a level of reliability at least equivalent to that required for issue of a Digital Signature Certificate under the Act and such regulatory The foreign regulatory authority accords similar recognition to the Controller and to certifying authorities licensed under the Act.
Controller of Certifying Authority (CCA – India) to enter into a Memorandum of Understanding (MoU) with each recognized Regulatory Authority
Reliability assessment for equivalence Factors to determine the level of reliability and equivalence, include-: (a) financial and human resources, including existence of assets within the country; (b) trustworthiness of hardware and software systems; (c) procedures for processing of certificates and applications for certificates and retention of records; (d) availability of information to subscribers identified in certificates and to potential relying parties; and (e) regularity and extent of audit by an independent body;
Recognized Foreign Certifying Authority not to issue certificates in India
Recognition of CA not operating under a Regulatory Authority
Any Foreign CA may apply to Controller for recognition; it may require to submit following details, including: ○ A Certificate Practice Statement (CPS) ○ A statement for the purpose & scope of anticipated DSC technology, management, or operations to be outsourced ○ Certified copies of the business registration & license of foreign certifying authority that intends to be recognized ○ Audit report of infrastructure

○ Maintenance of local office ○ Fee of USD 25,000 ○ Performance Bond USD 1crore ○ Issuance of recognition within 4 weeks
Recognized Foreign Certifying Authority shall not issue certificates in India

****