Electronic signature- India Scenario

Ramachandran

Framework for Electronic Signature

- 1.4 billion residents , 640,000 villages
- The Information Technology Act was enacted on 9th June 2000 and subsequently amended in 2008
- 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
- Acceptance of electronic documents as evidence in a court of law.
- Acceptance of electronic signatures at par with handwritten signatures.

Information Technology Act

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 policy, 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

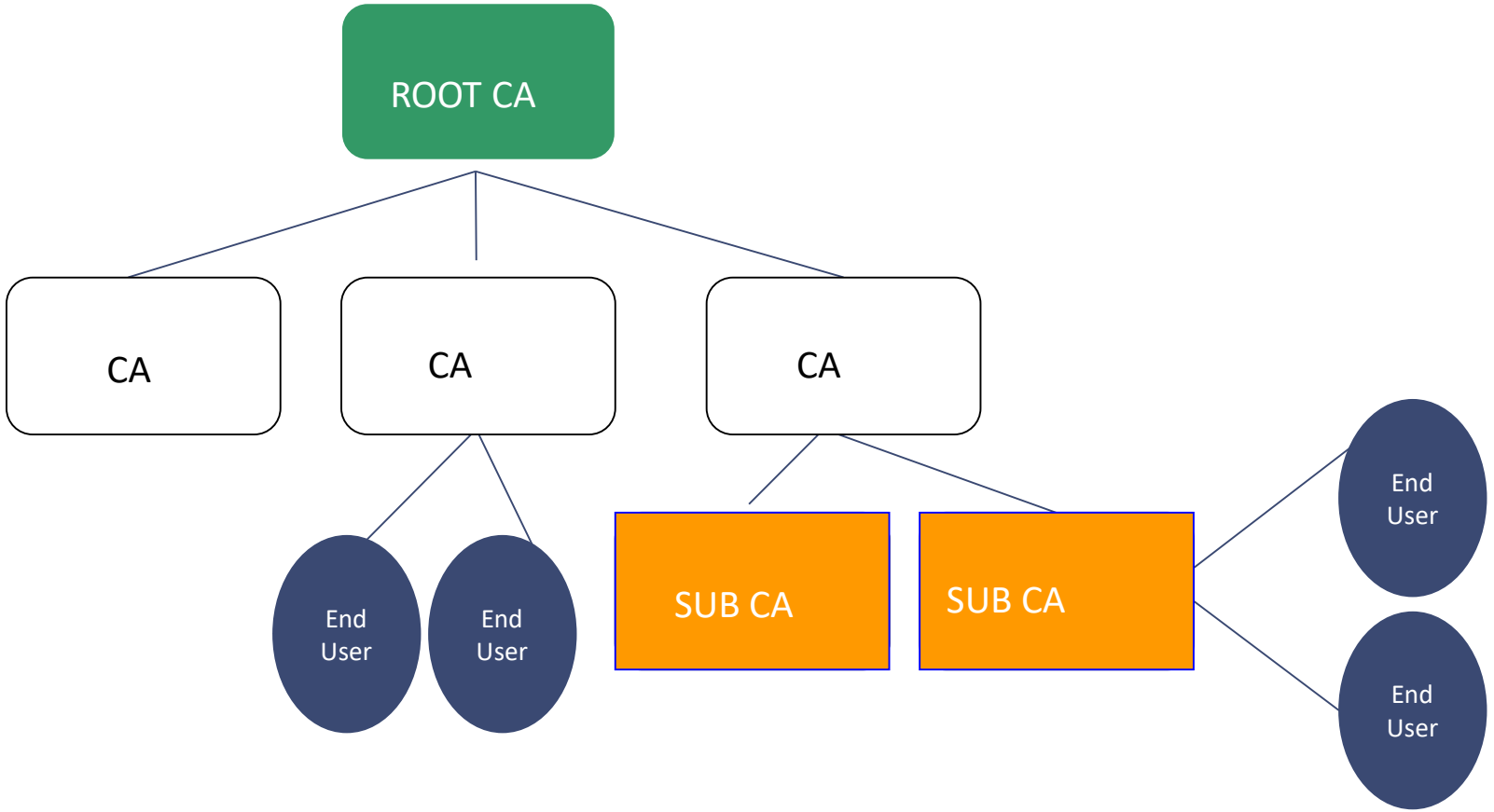
CCA & Licencing to CAs

- Controller of Certifying Authorities issue license to Certifying Authorities
- The License 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 & audit in accordance with the provisions under ACT.

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.
- At present there are 19 CAs licensed by Root CA

India PKI Model



Certifying Authorities (CAs)

- CAs can be private sector companies, Government departments, public sector companies, Non-Government Organizations (NGOs) or a Foreign Legal entity.
- CAs operating under same policy, standards, and verification methods, subjected to be audited by the criteria set by Root CA
- CAs are required to provide CRL, OCSP and Timestamping Services.
- CAs are also not allowed to issue certificate other than that approved by CCA.
- A Certifying Authority can create sub-CAs to meet the business branding requirement.

Electronic Signature Certificates

- 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.
- 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.

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.

There are two types of certificates issued, namely:

1. Personal certificate : For Personal certificate, after verification of Identity and address
2. Organizational person certificate : For Organizational person certificate, Organizational id, Organizational email id, mobile number, Organizational address are verified

In both the case, the verification is carried out through online video by CA

Storage Medium (FIPS Level 2 or higher)

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

- Crypto Token - Under the physical possession by applicant, valid for 2-3 years
- HSM (CA) - eSign service, one-time key generation and deletion immediately after signature creation, certificate is valid for maximum of 30 minutes

Types of Certificates

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

- End User Certificate (issued for personal use) Affixing individuals electronic Signature
- End User Certificate (issued for organization use) Affixing individuals electronic Signature
- System Certificate Machine to machine authentication
- Time Stamping Authority Certificate Generating Timestamp Token
- Code Signing Certificate Signing of software code
- OCSP Responder Certificate OCSP response Signature
- Encryption Certificate Key Encryption
- Document Signer Certificate Organizational application signature
- SSL Certificate Secure Communication

Assurance Level & Applicability

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 & Applicability

- Class 1(software medium) - Relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance.
- Class 2(Hardware medium) -Relevant to environments where risks and consequences of data compromise are moderate.
- Class 3(Hardware medium) - primarily intended for e-commerce applications,
- eKYC-Single Factor(Hardware medium)- Relevant to environments where Aadhaar eKYC based Single Factor authentication to eKYC service is acceptable
- eKYC- Multi Factor(Hardware medium) -Relevant to environments where Multi Factor authentication to eKYC service is required

Electronic Signatures

For an electronic signature to be legally accepted reliable it shall possesses the following requirements:

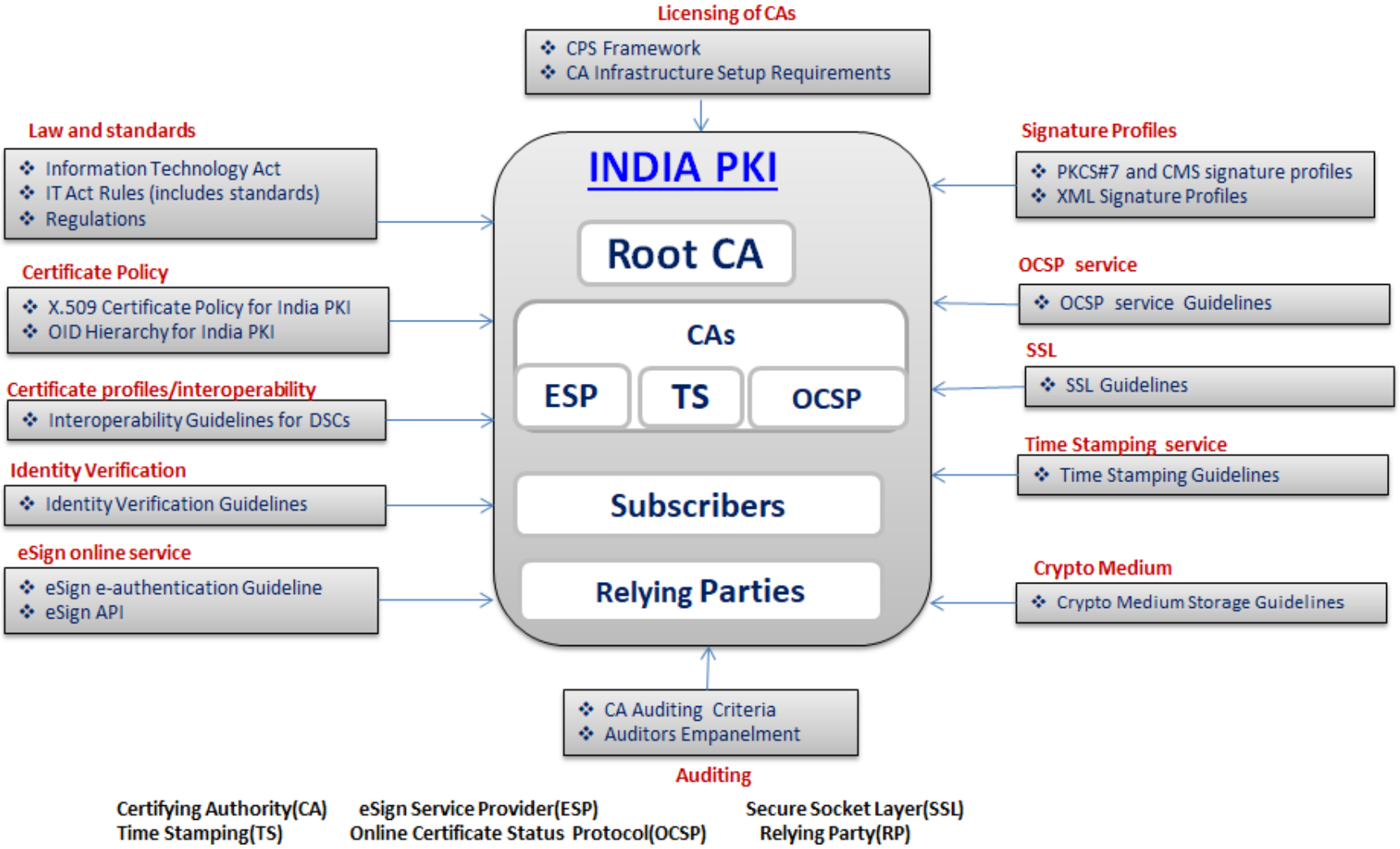
1. The signature creation data or the authentication data are, within the context in which they are used, linked to signatory or, as the case may be, the authenticator and no other person
2. The signature creation data or the authentication data were, at the time of signing, under the control of signatory 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

Standards

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- 2 or higher - Security Requirement of Cryptographic Modules

Electronic Signatures Policy Framework



Certifying Authority(CA) eSign Service Provider(ESP) Secure Socket Layer(SSL)
Time Stamping(TS) Online Certificate Status Protocol(OCSP) Relying Party(RP)

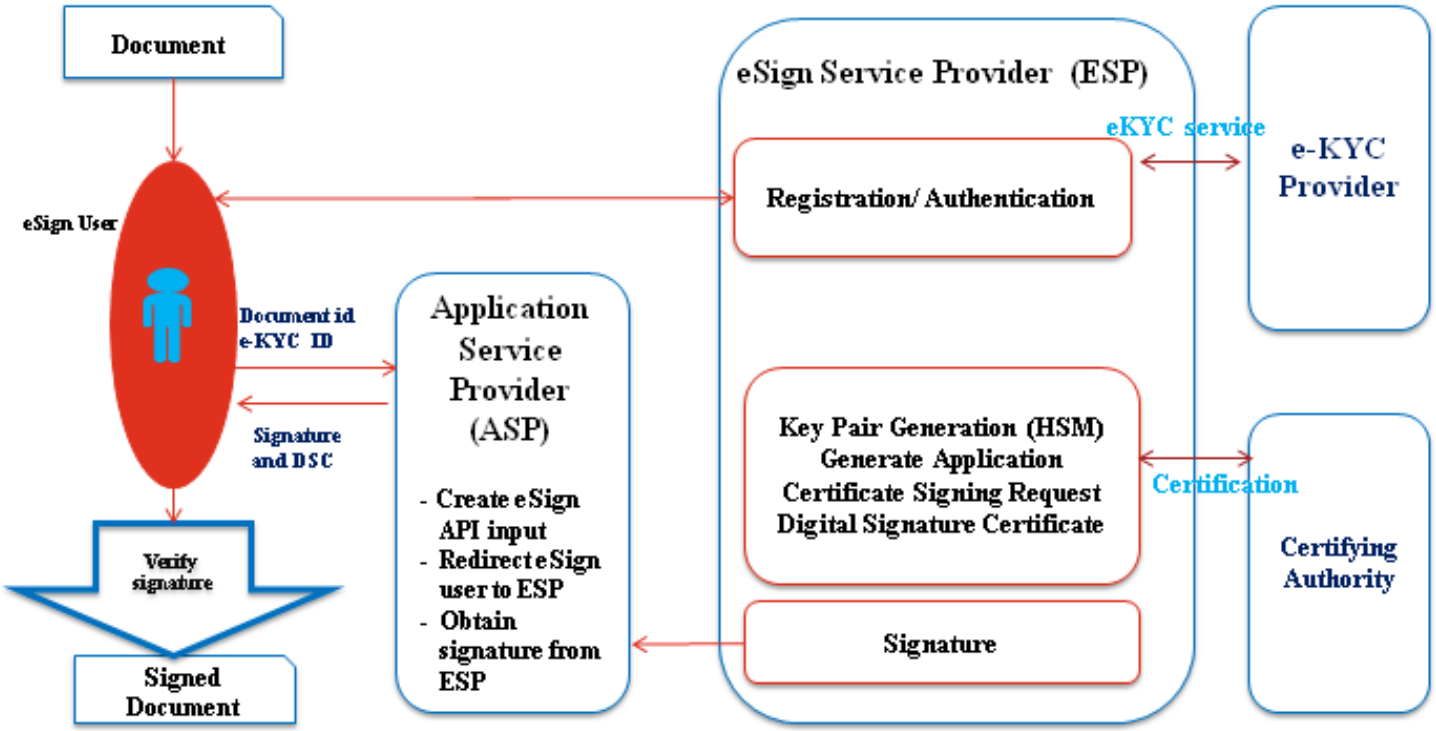
Time stamping

- 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

eSign



HSM – Hardware Security Module

OTP – One Time Password

ASP – Application Service Provider

e-KYC – electronic Know Your Customer

DSC – Digital Signature Certificate

ESP – eSign Service Provider

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.

The eSign is carried out based on the

1. Aadhaar Authentication
2. CA eKYC account authentication

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.

- Applicants are required to submit the information to CA and CA carryout a verification to establish the information submitted by the applicant is genuine.

- 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

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]

Recognition of CA operating under a Regulatory Authority

- Recognition of Foreign Certifying Authorities is based on Principle of reliability & reciprocity.
- For recognition, it is required that foreign CA should have been established under the laws of that country
- Recognition requires an equivalent level of reliability
- 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

Recognition of CA operating under a Regulatory Authority .. Cont

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;

The 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

Thank you