Cross Border Recognition of Certifying Authorities

PKI Interoperability

Trusting among disparte PKI Domain

Trusting Digital Transactions across the Globe

Cross Jurisdictional on line Trade

Cross-border Paperless Trade

About Me….

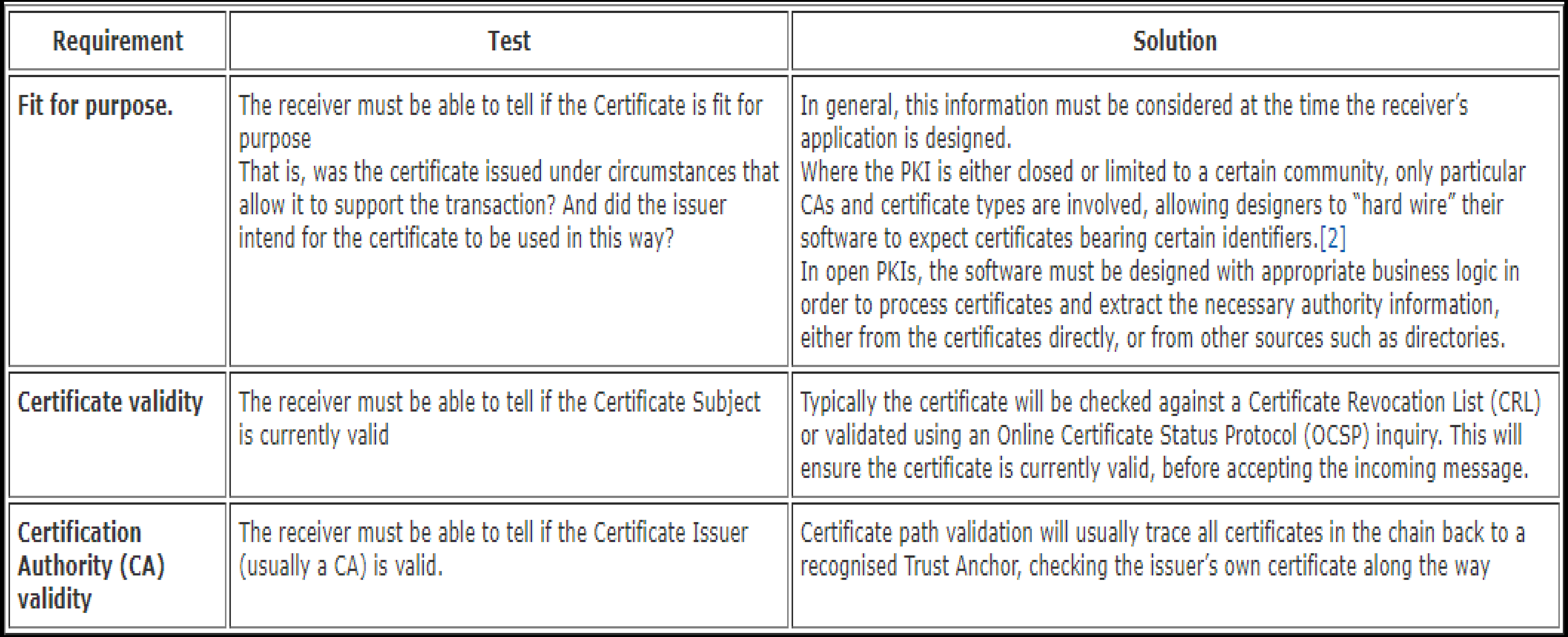
- Manoj Kumar Kulshreshth, Senior Technical Director, NIC, MeitY, Govt. of India
- Post Graduation in Physics, PG Diploma in Comp. Sc, PG Diploma in Cyber Law
- Ethical hacker Certification
- 32 Years Experience in IT Field: Software Design, Development, Infrastructure Management, Worked in various positions in Certifying Authority as Registration Authority Officer, CA officer and Chief Operation Manager
- Worked as Manager of Cyber Security Operation Center
- Presently heading e-sign unit, providing e-sign service and Aadhaar Data Vault Service, State Technical officer in PKD-ICAO (electronic passport)
- Areas of Interest- PKI, Data Protection, Quantum Cryptography and Cyber Law

Outline…

- Setting the stage-Issues
- Options-PKI Interoperable Models
- Inter-Domain Interoperability Initiatives
- Indian Legal Framework for Recognizing Foreign Certifying Authority
- A Use Case –Electronic Passport in India

Cross Border Recognition of certifying Authorities

- Setting the Stage– What all we should Know to believe a Electronic Transaction



Requirement	Test	Solution
Fit for purpose.	The receiver must be able to tell if the Certificate is fit for purpose That is, was the certificate issued under circumstances that allow it to support the transaction? And did the issuer intend for the certificate to be used in this way?	In general, this information must be considered at the time the receiver's application is designed. Where the PKI is either closed or limited to a certain community, only particular CAs and certificate types are involved, allowing designers to "hard wire" their software to expect certificates bearing certain identifiers.[2] In open PKIs, the software must be designed with appropriate business logic in order to process certificates and extract the necessary authority information, either from the certificates directly, or from other sources such as directories.
Certificate validity	The receiver must be able to tell if the Certificate Subject is currently valid	Typically the certificate will be checked against a Certificate Revocation List (CRL) or validated using an Online Certificate Status Protocol (OCSP) inquiry. This will ensure the certificate is currently valid, before accepting the incoming message.
Certification Authority (CA) validity	The receiver must be able to tell if the Certificate Issuer (usually a CA) is valid.	Certificate path validation will usually trace all certificates in the chain back to a recognised Trust Anchor, checking the issuer's own certificate along the way

Technical Ingredients

Cross Border Recognition of certifying Authorities

Issues to be considered for inter-domain interoperability-

1. Technical -Protocol, Data Structure, sharing Certificates, Certificate Revocation Information, Information Security ISO27001

2. Non-Technical - details necessary to establish the relationship between two PKI domains e.g. how certificates issued in foreign PKI domain, CP, Policy, Procedures etc.

3. Legal -The acceptance of digital signatures in multi-domain jurisdictional environment e.g. recently passed e-sign regulation, legal notice

Putting policies, laws and technologies together in an interoperable manner

Cross Border Recognition of certifying Authorities

- Option - Cross Certification

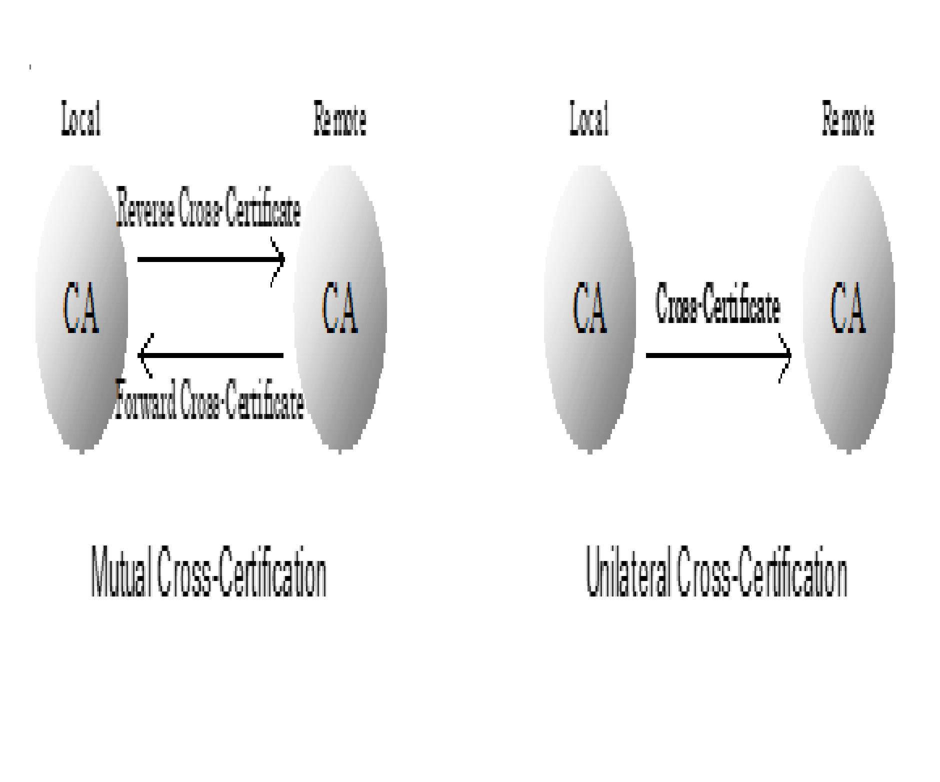

Local
Remote
Reverse Cross-Certificate
CA
CA
Forward Cross-Certificate
Mutual Cross-Certification
Local
Remote
CA
Cross-Certificate
CA
Unilateral Cross-Certification

Fig. 1 Cross Certification (Mutual CC, Unilateral CC)

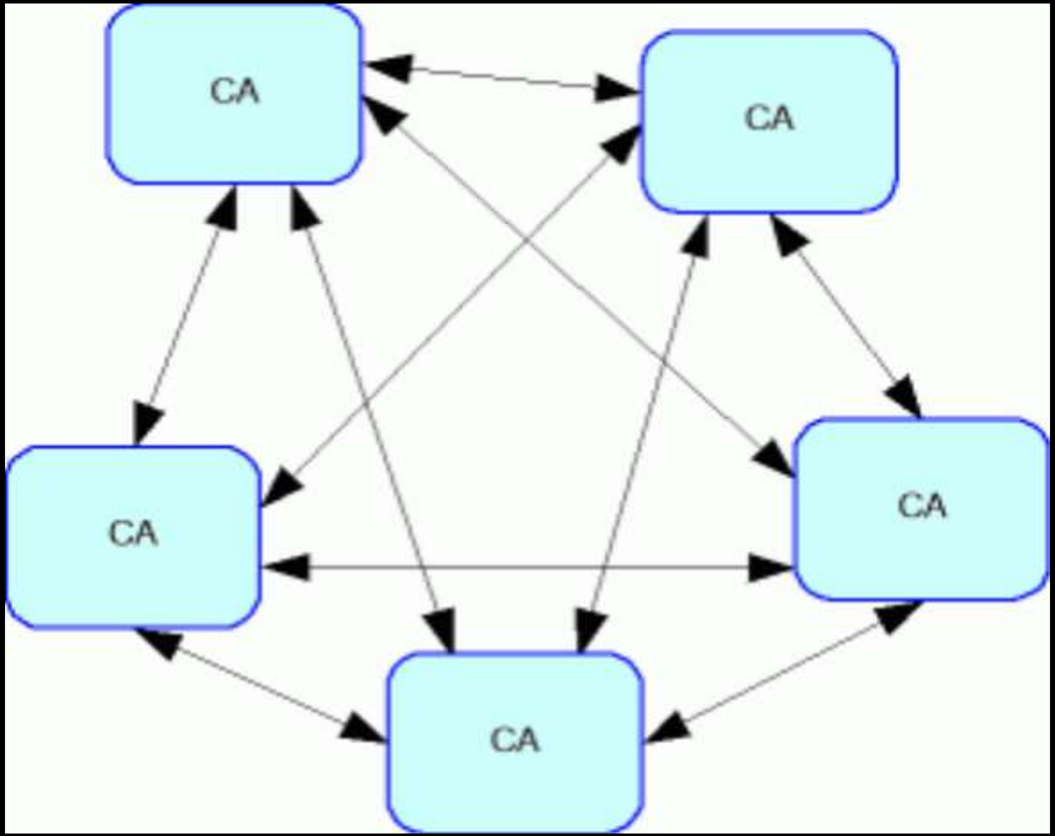
The act of one CA issuing certificate to another CA

The fundamental purpose of cross-certification is to establish an interoperability path between two distinct PKI domains or between two CAs within same PKI Domain

Trust is achieved by cross-certification

One primary advantage is that each PKI domain retains its autonomy, external trust relationships can come and go without affecting the internal trust relationship between the relying parties and their trust anchor within a given PKI domain.

Peer to Peer Cross-Certification Model-Mesh

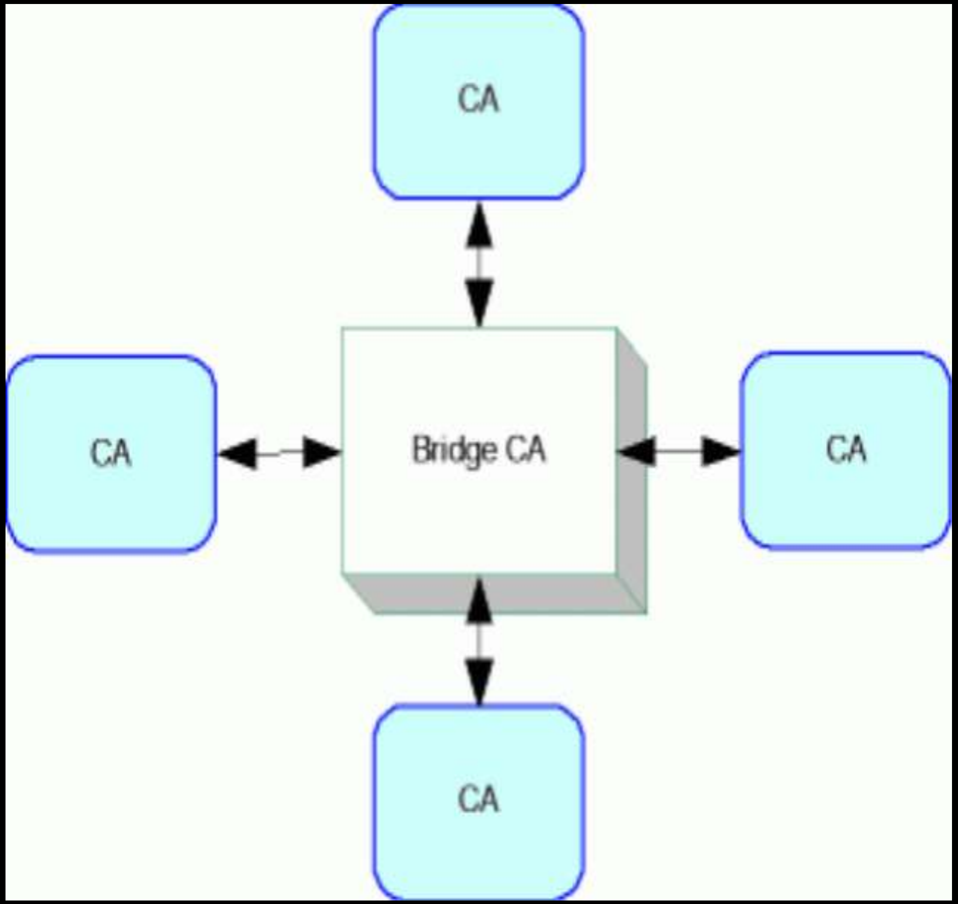


CAs issue cross-certificates to each other. Relying party can trace back to its trust anchor from the repository or by including a chain of signatures on the certificate itself.

As number of CAs grows, the number of cross-certifications grows even faster : If every pair of CAs cross certifies, the number of cross-certifications required is n sqr.

Achieving interoperability through mesh certification model is technically and logistically challenging due to overhead

Bridge CA (hub and spoke Model)



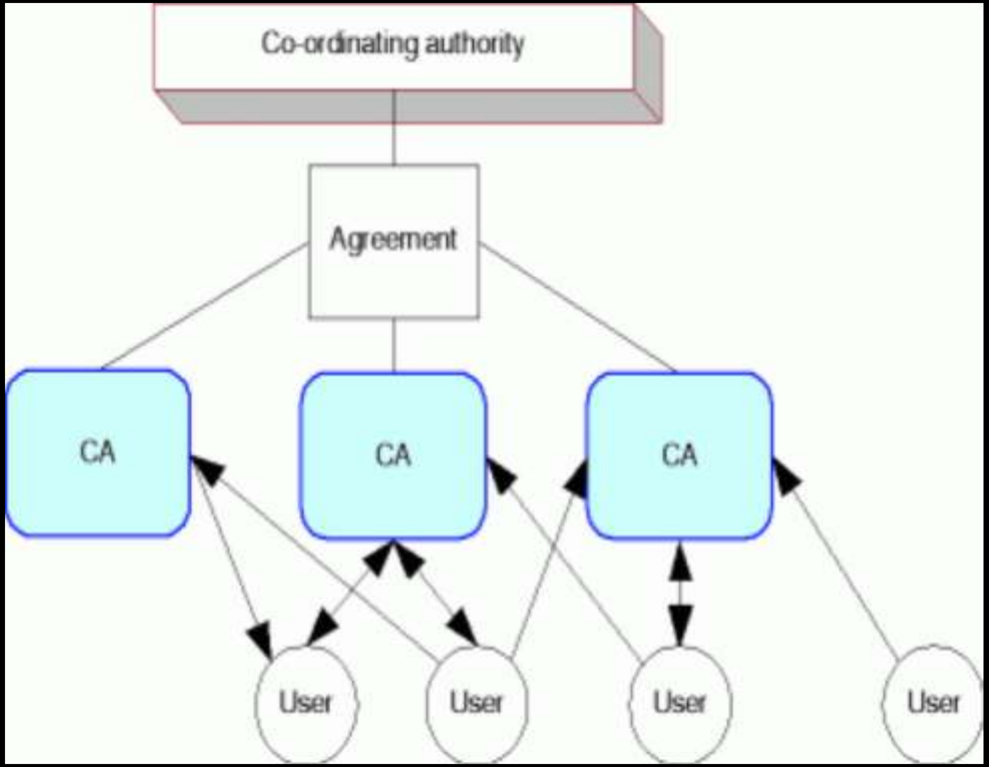
The Bridge CA essentially acts a facilitator or introducer of one organization or enterprise to another.

Each organization can enter into a cross-certification arrangement with the bridge CA under one or more certificate policies.

The organizations now have a `trusted path' to each other via Bridge CA

Bridge CA reduces overhead involved in mesh model, especially when the number of orgnizations that fall under the umbrella of the same policy is significant

Cross-Recognition Trust Model- A Concept (WebTrust)



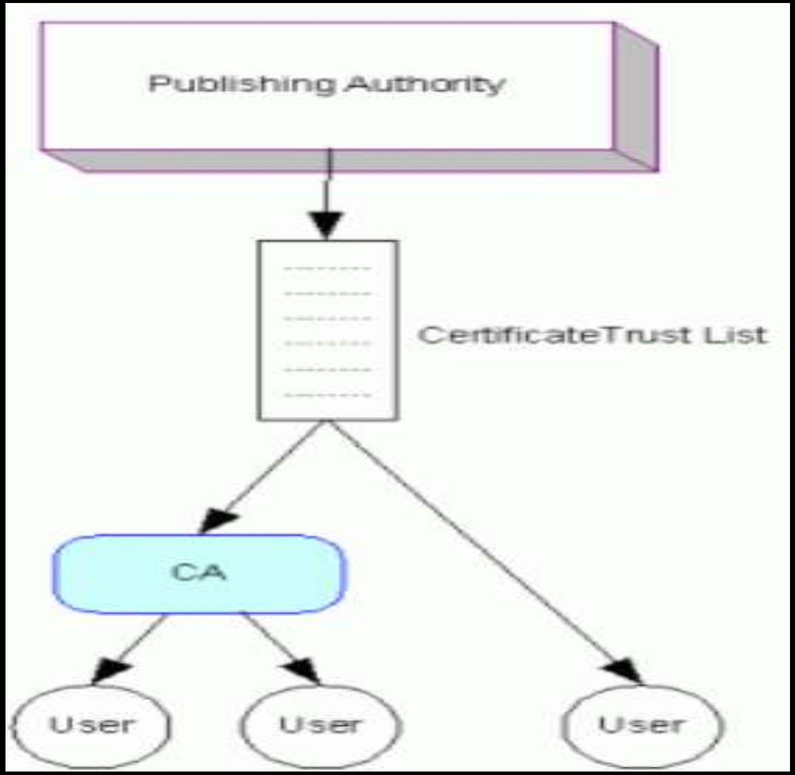
The foreign CA is regarded as trustworthy if it has been licensed/accredited by a formal licensing/accreditation body or has been audited by a trusted independent party

An Interoperability arrangement in which a relying party in one PKI domain can use authority Information in another PKI domain to authenticate a subject in other PKI Domain and vice-versa

It’s a based on notion that independent CAs would somehow be licensed or audited by a mutually recognized trusted authority i.e. an accreditation authority or an independent auditor

Relying part is expected to make trust decisions rather than CAs, the necessary information for the same shall be conveyed to the relying party through certificate extensions.

Certificate Trust List (CTL) Model



Web Browsers employs CTL

A CTL is a signed PKCS#7 data structure that contains a list of trusted CAs. A “trusted CA” is identified within the CTL by a hash of the public key certificate of the subject CA. It also contains policy identifiers and support the use of extensions

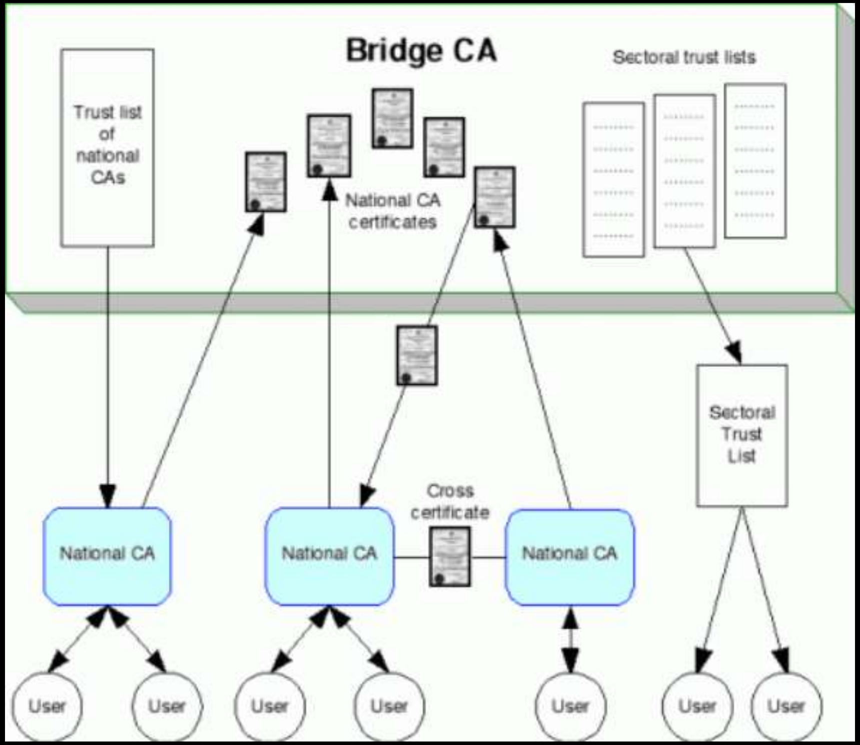
It replaces the need for complex process of cross-certification

The Key is that relying party trust the issuer of CTL, which then allows relying parties to trust CAs conveyed within CTL. The Distribution of CTL could be out-of-band mechanism

Acceptable practices, controls and procedures are required to achieve viable inter domain interoperability

Cross Border Recognition of certifying Authorities

Gateway/Bridge CA-



The EU is providing PKI Interoperability between PKIs of EU government. This Gateway will bridge together each of these National CAs

A centralised administrative structure of a bridge, that servers trust using both cross-certifications and CTLs

It publishes CTL of National CAs. Those national CAs can retrieve CTL and are free to add and subtract CAs and republish it to their Government users according to their national preference

It may also publish CTLs of CAs in particular sectors e.g. List of CAs accredited to provide health certificates

CAs can perform their own cross certification and this gateway will work as intermediary

It maintains directory service listing each CA and maintains CRLs

It provides OCSP and route requests to appropriate CA to determine if foreign Certificate has been revoked

Inter-Domain Interoperability Initiatives

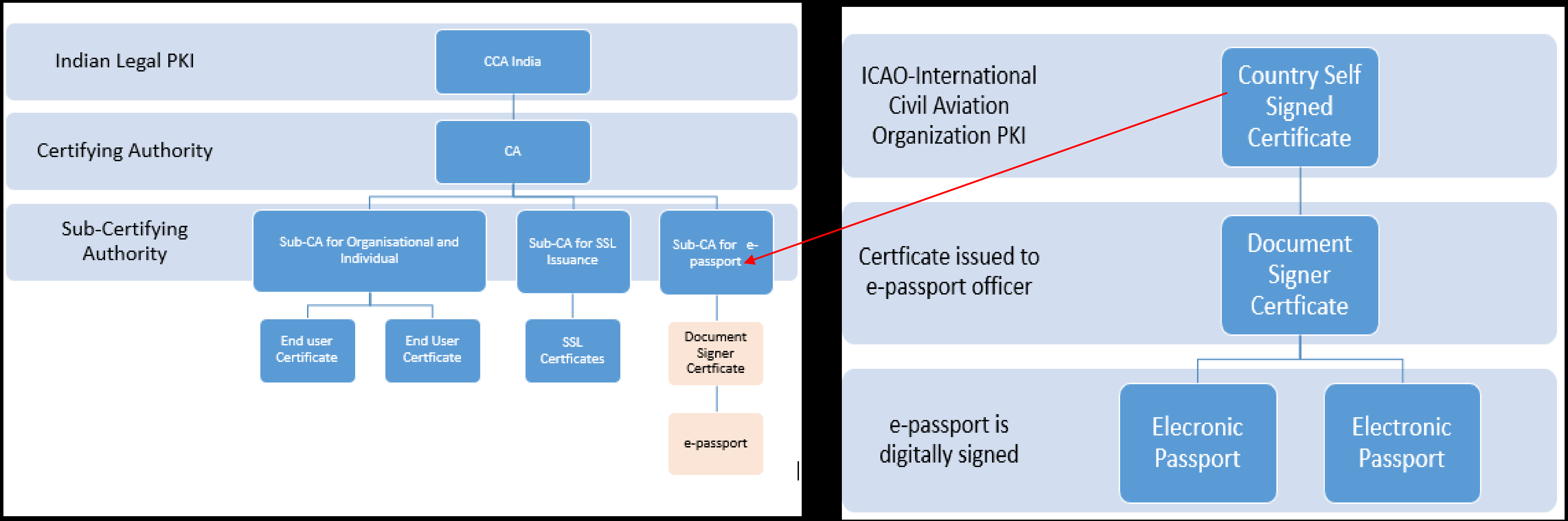
Sr No.	Country/Forum Name	Details	Model	
1	European Commission	Interoperable Delivery of PAN-European eGovernment Service to Public Administrations, Businesses and Citizens	Bridge/Gateway CA	
2	The Asia PKI Forum	To promote cooperation and interoperability among PKI across Korea, China, Japan, Taiwan, Singapore and Hong Kong	Cross-certification, cross-recognition, Bridge-CA, CTL	
3	Asia-pacific Economic Cooperation-APEC	Developed Guidelines for schemes to issue certificates capable of being used in cross border jurisdiction ecommerce	Cross-recognition, cross-certification	
4	Australia –Gatekeeper Project	Interoperability within the Australian Government Certificates Infrastructure is obtained via Gatekeeper Accreditation Certificate	Accreditation Certificate is indeed a central point of trust	

Indian Legal Framework for Foreign Certifying Authority

- As per Section 19 (1) and Section 89 of the Information Technology Act, the Controller may recognize any foreign Certifying Authority by official Gazette Notification

- The Notification contains two sets of Regulations
- One for recognized Foreign Certifying Authorities operating under a PKI Regulatory Authority comparable to that in India.
- Other set of Regulations for those Foreign Certifying Authorities which are not operating under a PKI Regulatory Authority.

A Use Case –Electronic Passport in India-Cross Certification between Indian and ICAO PKI Domain


Indian Legal PKI
CCA India
Certifying Authority
CA
Sub-Certifying Authority
Sub-CA for Organisational and Individual
Sub-CA for SSL Issuance
Sub-CA for e-passport
End user Certificate
End User Certficate
SSL Certficates
Document Signer Certficate
e-passport
ICAO-International Civil Aviation Organization PKI
Country Self Signed Certificate
Certficate issued to e-passport officer
Document Signer Certficate
e-passport is digitally signed
Elecronic Passport
Electronic Passport

Electronic passport digitally signed in ICAO PKI Domain is also valid in Indian PKI domain and hence can be produced Indian Legal System if need arises

Cross Border Recognition of Certifying Authorities

- Thanks
- mkk@nic.in
- 9818203131