Dynamic Legal Regime of PKI: A Case Study of India

Vakul Sharma

Establishing PKI

Circa 2000

- Internet is an open system of communication, which has its own set of problems.
- These problems relate to integrity, confidentiality and authentication of communication channels and processes. Since the computerized environment is more process based than personalized, it is hence necessary to have an *identification strategy* to ascertain the integrity, confidentiality and authentication of communication channels and processes and at the same time building a system of non-repudiation. *(India was 12th country to legislate on digital signatures*)

- A system of identity authentication is thus required.

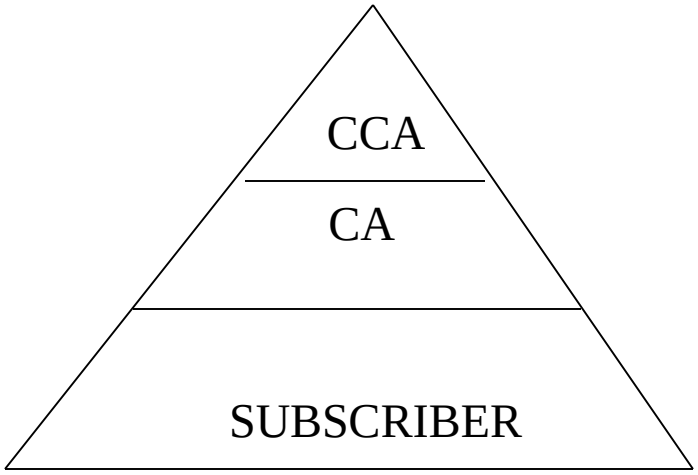
Who shall perform this identity authentication function?

Who shall authenticate that a digital signature belongs to a specific signer?

Who shall be the dispenser of the public keys?

After all, it is a matter of Governance.

Public Key Infrastructure



Levels of Hierarchy

Creating a trusted third party

Good Governance = Trust

Licensor – Licensee Relationship

- The trusted third party will not only authenticate that a digital signature/e-sign belongs to a specific signer but also dispense the public keys. Such a trusted third party is referred to as a “certification authority”.

- Its function is to verify and authenticate the identity of a subscriber (a person in whose name the Digital Signature Certificate is issued).

- A certifying authority has to receive a licence from the ‘root’ certifying authority or controller of certifying authorities, before it starts issuing digital signature/e-sign certificates to the subscribers.

- The issuing certification authority’s digital signature on the digital signature certificate can also be verified by using the public key of the certification authority listed in the repository of ‘root’ or controller of certifying authorities.

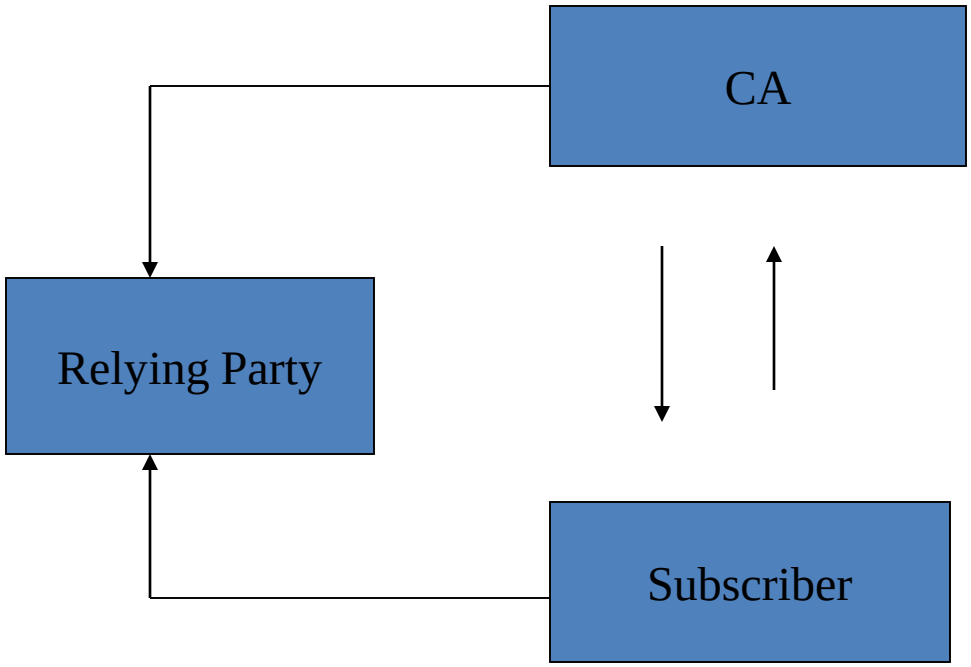
- A PKI system is much more than the ‘subordinate-superior’ relationship existing between the certifying authorities and the controller.
- It is a set of policies, processes, server platforms, software and workstations used for the purpose of administering Digital Signature/E-sign Certificates and public-private key pairs, including the ability to generate, issue, maintain, and revoke public key certificates.
- PKI represents a system of creating and authenticating digital ‘binding’ relationships based on trust.

Creating Binding Linkages

In order to create ‘binding linkage’ between the subscriber and the CA one needs ‘binding policies’.

These policies in turn define the level of trust a relying party shall put forth in the Certifying Authority’s overall certificate issuance and management process.

Binding Linkages

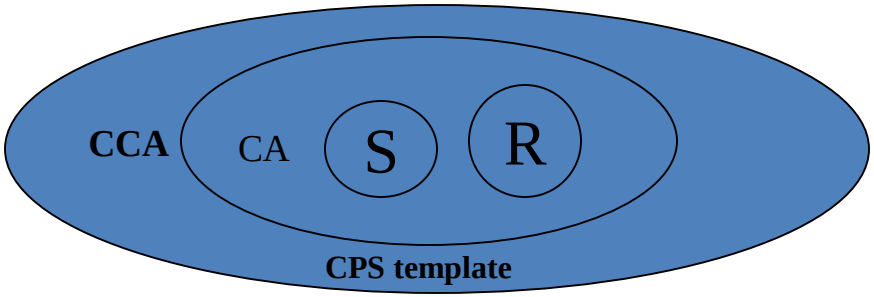


It is the Controller, who provides a template for such binding linkages in the form of Certification Policy Statement* (CPS)

It was felt that CPS must define the obligations and liabilities of the parties involved in issuing, managing, and processing certificates.

*The IETF Framework [Internet Engineering Task Force] defines the Certification Practice Statement (CPS) as the “statement of practices which a certification authority employs in issuing certificates”.

PKI:Bond of Trust



S = subscribers

R= relying party

It is better for a city to be governed by a good man than even by good laws.

Aristotle

Surveyed laws related to PKI of more than 45 countries and found that the basic law on PKI remains static – whether it is across Asia-Pacific, U.S (including its various States)-Canada or Europe.

PKI harmonization across the world, but the question is where are the benefits of this *technology platform harmonization*

- commercial exploitation (?)

One of the basic reasons is lack of *cross-certification* among CAs across the countries.

In fact, more and more subscribers (across the world) want *cross certification, for the purpose of cross border trade (*e-commerce), which has been the objective of Model Law of E-commerce, 1997.

- Central Government has notified the Information Technology (Recognition of foreign Certifying Authorities operating under a Regulatory Authority) Regulations, 2013

And

- Information Technology (Recognition of Foreign Certifying Authorities not operating under any Regulatory Authority) Regulations, 2013 on April 6, 2013.

Yes, from the *liability perspective* – CAs obligations towards the subscribers and the relying parties (in the event of cross-certification) will increase. But one cannot ignore the tangible benefits to CA's business model.

It is strange that at one level we talk about PKI harmonization across the world and at the other we are reluctant in granting global acceptability to locally issued signature certificates by the licensed CAs.

PKI: A paradigm shift

PKI 2.0

- A model for other services
  - Digital locker facilities
  - Integration with *Aadhaar* based e-Sign
  - Banking
  - Insurance
  - Taxation
  - Land reforms (Land registries)
  - Judicial infrastructure/court case management
  - Authenticated repositories
  - GSTN (?)

- PKI has been a precursor to e-Governance /digital India ecosystem

  - Electronic Service Delivery (most of the States in India have enacted their ESD Rules)

  - Social welfare initiatives

Electronic Service Delivery Rules

Initiatives taken by the State Governments to frame Rules under section 90 of the IT Act

[*State of Chhattisgarh, Karnataka, Andhra Pradesh*, *Manipur, Meghalaya, Maharashtra etc.]*

Guaranteed Delivery of Public Services Act

Initiatives taken by the State Governments to enact legislations guaranteeing delivery of public services in a stipulated time period

[*Assam, National Capital Territory of Delhi*, *State of Maharashtra*, Madhya Pradesh, Himachal Pradesh, Rajasthan, Bihar, J & K, Jharjhand, Karnataka, Uttrakhand etc*.]

Future of PKI

PKI 3.0

Governance based on trust

- PKI in the last 17 years has been able to create trust in digital medium
- Trust based on integrity, authentication and non-repudiation
- Trust based on uniformity of applications
- Trust based on delivery of electronic services

- M2M/IoT (authenticating machines)
- Smart city (authenticating users/resources)
  - Infrastructure management
  - Social welfare management

- Section 10. Power to make rules by Central Government in respect of electronic signature.

- The Central Government may, for the purposes of this Act, by rules, prescribe—

(a) the type of electronic signature;

(b) the manner and format in which the electronic signature shall be affixed;

(c) the manner or procedure, which facilitates identification of the person affixing the electronic signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to electronic signatures.

In fact, it would be interesting to see the new *electronic signatures* regime unfolding taking cognizance of: (a) type of electronic signature; (b) manner and format of electronic signature fixation; (c) manner or procedure facilitating identification of signer; (d) integrity, security and confidentiality of electronic records or payments; and (e) any other legal issue pertaining to electronic signature.

“ It's not enough to be *up to date*; you have to be ***up to tomorrow***.”

-David Ben-Gurion

Thanks

vakul@vakulcorp.com