सत्यमेव जयते

Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

Indian Secure Trust Ecosystem & Moving towards Mutual Recognition

Mr. Aashish Banati
Deputy Controller, Office of CCA
Government of India

PKIA 2023

Public Key Infrastructure and its Applications (PKIA 2023)

4th International Conference
September 8-9th, 2023
Bangalore, Karnataka, India

भारत 2023 INDIA
वसुधैव कुटुम्बकम्
ONE EARTH • ONE FAMILY • ONE FUTURE

Indian Secure Trust: The PKI Landscape

1. India has a strong trust backbone built on the basis of Public Key Infrastructure (PKI)
2. The PKI in India is governed by the Indian Information Technology Act, 2000 and the Controller of Certifying Authorities (CCA) under the Ministry of Electronics and Information Technology (MeitY) is the regulatory body for PKI in India.
3. PKI / Trust Services are operated by 20+ Service Providers under National PKI Framework
4. India has one of the largest userbase for e-Signed transactions.
   - 10 million+ active long lived certificates enabling billions of transactions every day
   - 400 million+ short lived certificate transactions using eSign initiative under Digital India Programme.
5. India has legal validity to these signatures, with admissibility in the court of law.
6. India conforms to global practices on Public Key Infrastructure making it at par for reliance in other major countries / economies

Adoption across the Industry

1. India has a vast implementation of e-signature ecosystem, on which the country's **Digital Public Infrastructure** relies up on.
2. E-signature establishes the 'Remote Trust', enabling the organizations trust a digital transaction with zero human intervention.
3. The transactions between the entities are digitally signed (with a verified identity of the signer) making such transactions to be executed instantaneously without any moderation or back end manual processing requirements.
4. Such 'Remote Trust' has enabled complete digitalization of several use cases like Tax Filings, e-Procurement, banking among various other use cases.
5. **The new age use cases like Unified Payment Interface (UPI), Aadhaar Authentications, and other Digital Public Infrastructure initiatives are able to perform the transaction within a few seconds due to the remote trust established by a trusted digital signature at each stage of the transaction.**

Recognition of e-signatures within India

1. The uniform recognition and acceptance of e-signatures is made via National PKI Framework established by the regulator.
2. This has been achieved by the way of setting up uniform regulations, standards, policies and procedures.
3. The system is standardized and operated in an effective and trustable model, which has become a large use case of intra-country recognition & adoption of PKI / Digital Certificates.
4. With transparent ecosystem, there is proactive adoption of PKI based digital certificates by the businesses and applications across the country, with least intervention by the government / regulator.
5. The legal admissibility of these signatures makes it more reliable for public and private applications to voluntarily adopt the PKI Framework, and use it for their e-authentication and e-signature requirements.

Foreign CA Regulations in India

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 Foreign Certifying Authorities

CA operating under a Regulatory Authority

1. Foreign Certifying Authorities operating under a PKI Regulatory Authority comparable to that in India
2. Recognition of Foreign Certifying Authorities is based on Principle of reliability & reciprocity.
3. For recognition, it is required that foreign CA should have been established under the laws of that country
4. Recognition requires an equivalent level of reliability
5. The foreign regulatory authority accords similar recognition to the Controller and to certifying authorities licensed under the Act.
6. Controller of Certifying Authority (CCA – India) to enter into a Memorandum of Understanding (MoU) with each recognized Regulatory Authority

Recognition of Foreign Certifying Authorities

CA NOT operating under a Regulatory Authority

Any Foreign CA may apply to Controller for recognition, it may require to submit following details:-

1. A Certificate Practice Statement (CPS)
2. A statement for the purpose & scope of anticipated DSC technology, management, or operations to be outsourced
3. Certified copies of the business registration & license of foreign certifying authority that intends to be recognized
4. Audit report of infrastructure
5. Maintenance of local office
6. Fee of USD 25,000
7. Performance Bond USD 10 Million
8. Issuance of recognition within 4 weeks

Moving towards Mutual Recognition

1. India is keen to progress on Mutual Recognition with other countries.
2. As part of this objective, India has proposed creation of a Mutual Recognition Framework with G20 members countries as well as invited countries. A presentation was also made in G7 side event.
3. India proposed to create such a framework with reciprocal in nature, which will give way for:
    1. Mutual Recognition of e-signed documents (signed under National PKI framework). This gives way for usage of personal documents (ID, Driver's license, educational certificates, etc), financial documents, etc outside the home country, when they are electronically signed by the "issuer" organization.
    2. Mutual Recognition of Business Contracts (signed under National PKI framework). This will give way for more ease of doing business when parties are involved across different nations, and solves the major concern of legal admissibility of such contracts when parties are from different jurisdictions.
    3. Mutual Recognition of Import / Export documents, when signed under National PKI Framework. This will help in easier establishment of trade between the countries with complete online process.

Proposed Mutual Recognition Framework

1. PKI Mutual Recognition framework is essential for enabling secure and interoperable communication in today's globalized world.
2. By promoting trust and security, reducing complexity and costs, and increasing interoperability, the framework provides a standardized and trusted approach that can benefit organizations and governments around the world.
3. India has proposed a detailed framework proposal and overview, along with a draft agreement.
4. This envisages an idea of establishing trust based on the fundamentals of PKI, with equivalent level of reliability & also established under the laws of a country.
   1. The countries shall publish their root trust anchor or a trusted CA trust list.
   2. The countries shall ensure that they have an active and compliant National PKI Framework.
   3. The countries shall demonstrate their compliance via globally accepted practices (eg: Webtrust/ETSI)
   4. Technical & operational framework for recognition shall also be established by the countries.

Conclusion

1. Cross border recognition of Digital Transactions will make easy way in globalization of Digital Public Infrastructure Initiatives.
2. With proven model of ‘secure remote trust’, Public Key Infrastructure plays a crucial foundational layer to move towards Global Mutual Recognition.
3. We will be happy to work with the countries to progress towards the proposed Mutual Recognition Framework.
4. We also invite countries to take part in this initiative, so that we can work towards a safe and secure information exchange and build a Secure Digital “World”.

सत्यमेव जयते

Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

भारत 2023 INDIA

वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE

Thank You