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

Proposal for Mutual Recognition Framework of Public Key Infrastructures (PKI) and Digital Signatures

Enhancing Trust and Security in Cross-Border Communication

Proposal by
Controller of Certifying Authorities
Government of India

13-June-2023 | Global DPI Summit, Pune

भारत 2023 INDIA

वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE

Introduction

The mutual recognition Framework (MRF) for Public Key Infrastructures (PKI) and Digital Signatures is a proposed concept along with the agreement that outlines the terms and conditions under which two or more countries will recognize and trust each other's digital certificates. It involves the establishment of mutual recognition agreements between participating countries, the development of technical and policy requirements that enable interoperability between different PKI systems, and the implementation of accreditation and supervision processes to ensure compliance with these requirements.

Components of the Framework

The PKI Mutual Recognition framework consists of several components that work together to enable secure and interoperable communication between different PKI systems. Here are the main components of the framework:

- **Mutual Recognition Agreement**: The framework includes a mutual recognition agreement between participating organizations or countries. This agreement specifies the terms and conditions under which digital certificates issued by one CA will be recognized and accepted by another CA.
- **Operational Requirements:** The framework includes the components to operationalize the proposal considering the stake holders including Government and Private participates consisting of Regulator as well as Certifying Authorities. This also covers the Technical and Policy requirements for functioning of the framework.

Mutual Recognition Agreement

In this direction, India proposes a draft MRF Agreement that includes provisions such as:

- The types of digital certificates that will be recognized.
- The assurance levels of the digital certificates that will be recognized
- The Identity Verification Requirements of the individuals / organizations
- The processes for validating digital certificates and revoking them if necessary
- The types of certificate authorities (CAs) that are eligible to participate in the MRF
- The technical requirements for interoperability between the different PKI systems (e.g. use of specific encryption algorithms or key lengths)

- The duration of the agreement and the process for renewing or terminating it
- dispute resolution mechanisms

It's important to note that the above list is just a common example, actual content of the draft may vary depending on the specific use case and the specific regulations or laws in the countries involved.

The mutual recognition shall rely on the basic parameters of:

1. National PKI Framework, in the form of laws, rules, regulations, etc.
2. Legal framework to recognize digital signatures made under National PKI Framework
3. Supervision methodology to ensure compliance to national PKI framework
4. Adoption of Technical best practices in terms of standards, algorithms, etc
5. Identification and representation of Trust under National PKI Framework

Recognized audit schemes make an important aspect on trusting outside the country. Hence, this mutual recognition relies on specific Audit Assessment schemes including WebTrust for CAs and ETSI for Trust Service providers.

Before it is signed by the parties involved, a draft Mutual Recognition Agreement is reviewed, negotiated and possibly modified to ensure that the requirements of all parties are met. It shall also be reviewed by legal teams, to ensure it follows the laws of the countries involved, and it's in compliance with the industry regulations and standards.

Operational Requirements

The framework includes the components to operationalize the proposal considering the stake holders including Government and Private participates consisting of Regulator as well as Certifying Authorities. This also further includes the Technical and Policy requirements towards setup and functioning of the framework.

- **Technical Requirements**: The framework specifies technical requirements for certificate issuance and management, including key length, algorithm, and certificate revocation. These technical requirements ensure that digital certificates are issued and managed in a secure and standardized manner.

- **Policy Requirements**: The framework also specifies policy requirements for certificate issuance and management, including identity verification and certificate renewal. These policy requirements ensure that digital certificates are issued and managed in accordance with best practices and standards.
- **Regulator / Supervision Body**: The framework involves the National Regulator or an equivalent body from the government who is consider as the Supervision Body towards establishing and functioning of PKI in the country.
- **Certificate Authorities / Trust Service Providers**: The framework involves multiple Certificate Authorities (CAs) that issue and manage digital certificates. These CAs are responsible for verifying the identity of certificate holders and issuing digital certificates that are trusted and recognized by other CAs. These CAs play a critical role in ensuring the security and integrity of the PKI system.

The operational requirements may vary from country to country depending on the structure established in each country. However, these shall agree to meet a uniform functioning to meet the interoperability requirements between the nations.

Next steps

India invites countries from G20 nations as well as countries willing to participate in this direction towards working further on this framework and strengthening it for operationalization.

The subsequent discussions (bilateral / multi-lateral) shall be convened towards:

1. Inputs towards finalizing the template for Mutual Recognition Agreement
2. Scoping of operational requirements in the lines described above

Enclosures:

- Detailed background note
- Draft Mutual Recognition Agreement