India PKI Forum

Sponsored by Controller of Certifying Authorities, Ministry of InformationTechnology, Govt. of India

CASE STUDY

Deplyoing PKI at Scale for Internet of Things

info@indiapki.org

www.indiapki.org

Deplyoing PKI at Scale for Internet of Things

Providing state-of-the-art PKI framework that help enterprises deploy a foolproof IoT ecosystem

Industry
IT and Infrastructure

Business Matters
According to Eclipse IoT Working Group's 2017 IoT developer survey, security is the top concern for IoT developers. These billions of physically connected devices have become an attractive ground for hackers and cybercriminals largely because of the nature of deployment. Thus a solution is required that could ensure data confidentiality, information integrity, authentication, and data access control.

Business Need
As new technologies emerge, there is always an element of risk that comes in. The connected devices must provide trustworthy information, sometimes directly to the user and sometimes to the platform. There is a requirement for high integrity messaging, secure communications and powerful authentication at scale.

Approach
Primarily, IoT has two security requirements: trust and control, and the same have to be achieved on a large scale for IoT. PKI technologies have already been proven in large-scale systems like the global payment system. However, securing IoT brings in new challenges that force the society to rethink traditional assumptions about key management and the impending security threats.

Background

IoT is a network of physical objects that can interact with other devices or platforms over the internet. The internet enabled systems and devices share sensitive information and perform actions based on manual user input or through automation.

IoT is expected to offer advanced connectivity of devices, systems, and services that go beyond server to server communications and covers a variety of protocols, standards, and applications and as the number of networked devices continues to grow, the requirement of better security is the need of the hour.

IoT solutions and implementations must account for the fundamental need of secure systems and data, including three core goals of information security i.e. confidentiality, non-repudiation, and integrity. This can be achieved through Public Key Infrastructure (PKI).

Digital Signature and Encryption Technology

- The Digital Signature Technology works on the Public Key Infrastructure framework which uses a Cryptographic Key Pair – Private and Public Key for secure access and transmission of Information.
- Efficient and unbreakable encryption algorithms that can handle voluminous data and mitigate the risk of unauthorized access to sensitive data

Benefits

- PKI is an open standard, free to adopt, implement and customize solution
- Even with low computational power and memory, cryptographic algorithms can often still be computed
- It has the capability to address the security needs of data at-rest and in-transit
- User/Device identity is established using Digital Signature Certificates
- Ensures the integrity of data-in-transit or at-rest
- Ensures only authorized personnel have access to sensitive data

Solution

PKI has been the backbone of internet security since its inception through the use of Digital Certificates. These Digital Certificates are issued across industries using varied signature algorithms, public key sizes, standards and cryptographic properties that meet specific needs.

Digital Certificate Management Lifecycle is designed to assist and manage the lifecycle of certificates used in thousands or even millions of devices connected in an IoT ecosystem. It can be customized to fit the needs of digital certificates in IoT security requirements. The solution is equipped to handle mass digital certificate issuance, reissuance, suspension or revocation that is critical to ensure continuous integrity of devices. There is no IoT deployment too large or small. Digital certificate requests can be automated through globally renowned standards and protocols such as REST, SOAP, SCEP, SAML etc.

The Digital Certificates issued address key information security principles; which are:
- Confidentiality
- Authenticity
- Non-repudiation
- Integrity

Encryption and Authentication in IoT ecosystem, bring in Trust and control to devices connected in IoT. Authentication solutions help in securely establishing identity and authenticating one device to another with the help of Digital Certificates embedded in the devices; thus ensuring that only trusted devices are allowed to connect to a nearby server and also enabling trusted communication between devices.

In short, it enables large-scale authorization and reliable encryption for ultimate trust and control and makes it the right choice for securing connected devices.

It ensures the integrity of data through the following:

Encryption: Disguising of data in transit and at rest.

Authentication: Identifying trust amongst users/devices in network information exchange.

Signing: It helps in verification of untampered data and also makes sure that the device has received data from a trusted source.