Deploying PKI in IoT Security at Scale

eMudhra provides state-of-the-art PKI framework that could help corporations to deploy a fool proof IoT ecosystem.

Industry
IT and Infrastructure

Business Matters
As IoT (Internet of Things) continues to connect networked devices of different nature and relay useful information to people. Due to the emergence of IoT, new business avenues are getting created and existing businesses are flourishing. This is all happening due to voluminous data that is getting generated in the IoT ecosystem.

Business Need
As new technologies emerge, there is always an element of risks that brings in. The connected devices must provide trust worthy 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
Regarding security, the IoT has two requirements: trust and control. And the same has to be achieved on the large scale of IoT. PKI technologies have already been proven in large scale system like the global payment systems. However, securing IoT brings new challenges that forces society to rethink traditional assumptions about key management and the impending security threats.

Background
The IoT is transforming the world the way live in. In IoT, network of physical objects such as networked devices than can interact with other device or platform over 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 goes beyond server to server communications and covers variety of protocols, standards and applications.

Connected devices ranges from smart heart monitoring devices, lighting system, built-in sensors for automobiles, home security systems, smart appliances etc. The connection between these embedded devices will usher in automation for nearly all fields while also enabling advanced applications such as smart cities, smart grid, Intelligent Transport, water management etc. Gartner in its press release forecasts that 8.4 billion networked devices will be in use worldwide in 2017, up 31% from 2016 and will reach 20.4 billion by 2020. Total spending on endpoints and services will reach almost $2 trillion in 2017.

As the number of networked devices continues to grow, requirement of better security is the need of the hour.

Business Requirement
As the number of networked devices is increasing at a rapid pace, the smart devices in the IoT also present a new and more widespread threat to users and personal data. It is expected attackers will continue to explore loopholes in technology and accelerate ways potential threats can be realistically exploited.

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

Address:
eMudhra Limited. Sai Arcade, 3rd Floor, No.56,
Outer Ring Road, Devarabeesanahalli, Bangalore - 560103

Contact:
Email: info@emudhra.com
Call: 080 6740 1400

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 be adopted, implemented, customized etc.
- Even with low computational power and memory, cryptographic algorithms can often still be computed
- Has the capability to address the security needs of at-rest and in-transit data
- User/Device identity is established using digital signature certificates
- Ensures only authorized personnel has access to sensitive data
- Strengthens and unifies data protection
- Ensures the integrity of data in-transit or at-rest.

Solution

PKI has been the backbone of internet security since its inception through the use of digital certificates.

eMudhra has the experience of working with various industries to issue digital certificates using varied signature algorithms, public key sizes, standards and cryptographic properties to meet specific needs. eMudhra specializes in IoT security solutions.

Digital Certificate Management Lifecycle

eMudhra's emCA product is designed to assist manage lifecycle of certificates used in thousands or even millions of devices connected in IoT ecosystem. emCA is flexible and customisable to fit the needs of digital certificate in IoT security requirements.

emCA can scale to accommodate changes for thousand to millions of certificates. 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 to fit the emCA. Digital certificate requests can be automated through globally renowned standards and protocols such as REST, SOAP, SCEP, SAML etc.

The digital certificates issued through emCA addresses key information security principles i.e.

- Confidentiality
- Authenticity
- Non-repudiation
- Integrity

Encryption and Authentication in IoT ecosystem

eMudhra's solutions bring in Trust and control to devices connected in IoT. eMudhra's authentication solution i.e. emAS helps 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, eMudhra solution enables large-scale authorization and reliable encryption for ultimate trust and control. The solution makes it the right choice for securing connected devices. It ensures the integrity of data through the following:

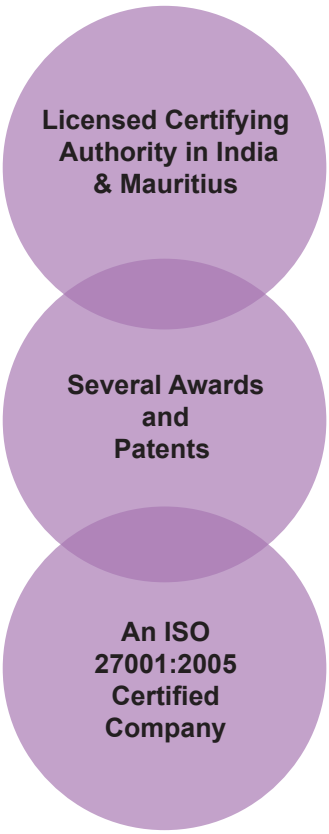
Encryption: Disguising of data in transit and at rest.

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

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

Address:
eMudhra Limited. Sai Arcade, 3rd Floor, No.56,
Outer Ring Road, Devarabeesanahalli, Bangalore - 560103

Contact:
Email:info@emudhra.com
Call: 080 6740 1400



About eMudhra

eMudhra is a technology and digital identity and transaction management company providing solutions which ease financial and statutory needs of consumers. eMudhra was established in 2008 and is a Certifying Authority in India and Mauritius to issue Digital Signature Certificates.

eMudhra's current enterprise and consumer solutions include Digital Signature Certificates, emSigner – Paperless Office Solution, emAS – secure multifactor authentication for banks, emCA for Digital Signature issuance and management and Prism – Voice of Customer Analytics using Semantics.

eMudhra is a market leader in India and has worked with large Banks, Financial Services companies and several Government agencies in India to implement Digital Signature based solutions which include secure access and paperless workflows.

eMudhra won the e-Asia award, an award given by AFACT (A United Nations body) for implementing Digital Signatures based on India's National ID – AADHAAR to bridge Digital Divide.

Address:
eMudhra Limited. Sai Arcade, 3rd Floor, No.56,
Outer Ring Road, Devarabeesanahalli, Bangalore - 560103

Contact:
Email: info@emudhra.com
Call: 080 6740 1400