



CASE STUDY

Deploying PKI at Scale for Internet of Things

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 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. 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 and manage the lifecycle of certificates used in thousands or even millions of devices connected in an IoT ecosystem. emCA is flexible and can be customized to fit the needs of digital certificates 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 for 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's 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 makes sure that the device has received data from a trusted source.

About eMudhra:

Much like the name, which is an embodiment of the seal of authenticity in the electronic or digital world, eMudhra is a cyber security solutions company and a trust service provider that is focused on accelerating the world's transition to a secure integrated digital society. With presence in 5 continents and a global delivery center in Bengaluru, India, eMudhra is empowering secure digital transformation of over 45 global banks, several Fortune 100 customers and thousands of SMEs.



USA | India | Singapore | UAE