ASIA PKI FORUM

Protecting a
fundamental right

The right to be you.

Trends Observed for PKI Adoption

1

Mobile PKI adoption enhances security through strong authentication, ensures regulatory compliance, and streamlines certificate management across mobile devices and platforms.

2

Advanced Metering Infrastructure providers are increasingly adopting PKI to fortify their security posture, recognizing their critical role in national infrastructure and the need to protect against cyber threats to the power grid.

3

Smart City leverages its PKI investment to secure critical infrastructure, protect citizens' data, authenticate visitors, and safeguard enterprise operations, creating a comprehensive digital trust framework that underpins all smart city initiatives.

Thailand Ministry of Finance

Challenges

- Security challenges issues faced
  - Sharing of tokens
- High Cost of replacing lost tokens
  - 20% replacement annually
- Administration overhead for management
  - User provisioning
  - Issuance of tokens

Solution

- Hardware tokens are replaced with Mobile PKI - ~30,000 users
- Self-service based provisioning of Identities
- Centralised portal for authenticating different applications

Customer's ROI

- Cost savings
- Reduction of ops overhead – Self Service by users
- Expanded from Mobile PKI to Workplace Use Case to max their investments
  - mobile digital signing
  - physical access
  - Workplace security

Users authenticate themselves via Mobile VSCs on Nexus Smart ID Mobile App.
Thailand Ministry for Finance provides full life-cycle management with self-service and automated processes for common identity use cases such as to issue, renew, and lock mobile identities for 100,000+ users.

https://www.nexusgroup.com/thailand-ministry-of-finance-embraces-next-gen-identity-management-platform/

IoT – Energy

الشركة السعودية للكهرباء

Saudi Electricity Company

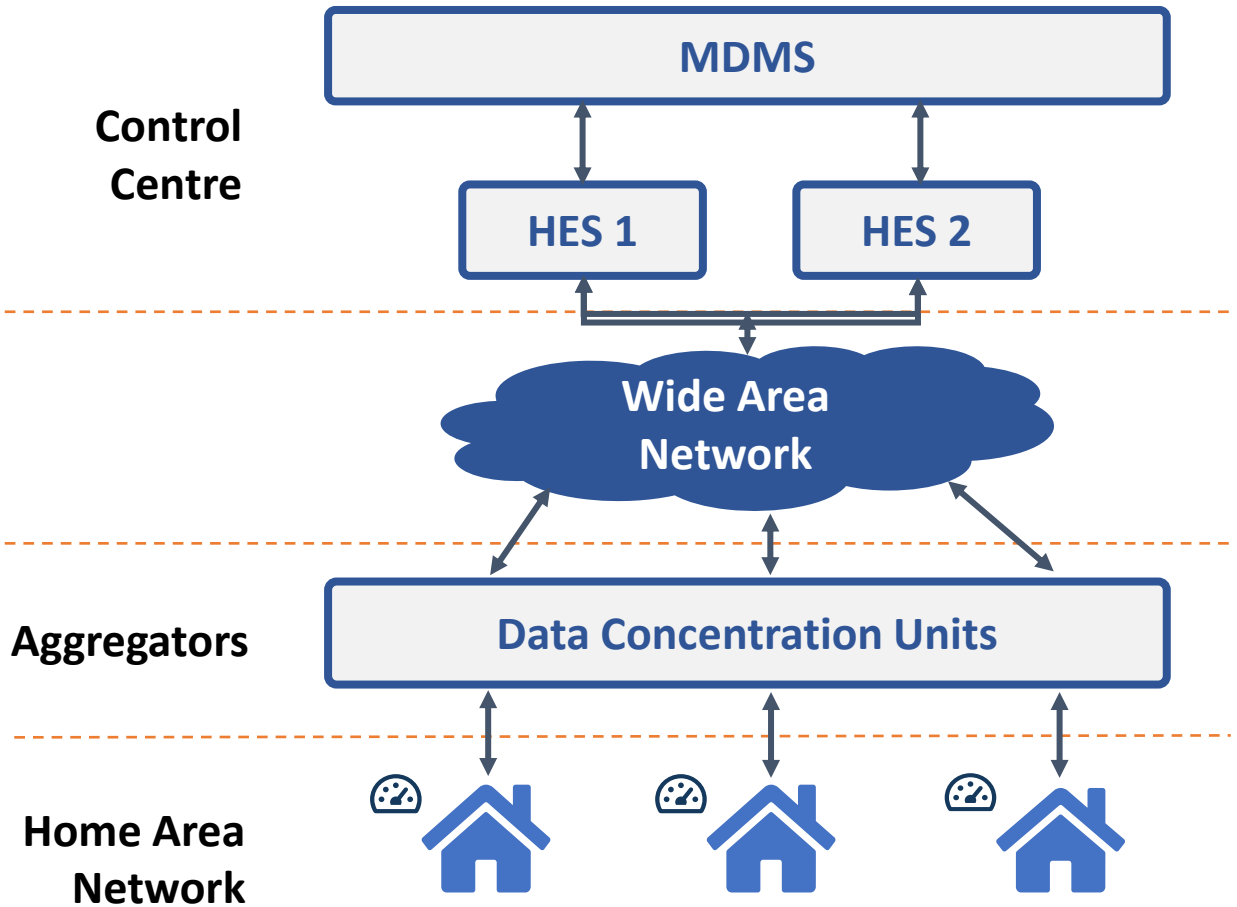
Customer: Saudi Electricity Company (SEC)

SEC selected Nexus via partner Emircom to secure their smart metering system including ~10 million smart meters from multiple vendors. Solution includes trusted identities for authentication and asymmetric as well as symmetric encryption for data confidentiality.

Solution: Smart ID IoT PKI + Utimaco HSM for symmetric key management

Not a public reference

Threats for AMI



AMI Network

- There could be many different intentions with an AMI cybersecurity attack, for instance:
  - Cheating the system to get cheaper or free electricity
  - Blackmailing power utility for money, e.g. “ransomware”
  - State critical infrastructure terrorism (Stuxnet, etc)
- Independent of purpose, there are multiple possible attack approaches, for instance:
  - Firmware manipulation
  - **Supply Chain Attack**
  - Authentication bypass in metering protocols
  - Remote disconnect commands
  - Theft of customer information
  - (Distributed) Denial of Service, (D)DoS attack
  - Buffer overflow through the AMI meters’ firmware
  - And more…

New Smart City in Middle East

A few of the use cases

Multi-Tenant Trust Centers with Private and Public CA's.

- Mobile PKI for Visual ID for each Citizen.
- Mobile PKI Authentication to Citizens/Workforce to eGov Services/Applications/ Intranet.
- Mobile PKI Digital Signing of Documents.
- PKI for email security (Signing and Encryption).
- PKI for millions of Workplace/IoT Devices.
- PKI for API Security.
- PKI for Digital Degree in Education.
- PKI for 5G/6G Security in Telecom.
- PKI for Autonomous EV Charging stations.
- PKI for Autonomous Connected Vehicles (V2X).
- PKI for Smart Meters (Advance Metering Infrastructure).
- IDP using Digital Access with Mobile PKI.

Smart ID Building Blocks for the Smart City