Challenges of a Public Key Infrastructure(PKI) for industrial systems

Jean-Michel Brun - Schneider Electric

Cyber Security, Distinguished Technical Expert

Life Is On | Schneider Electric

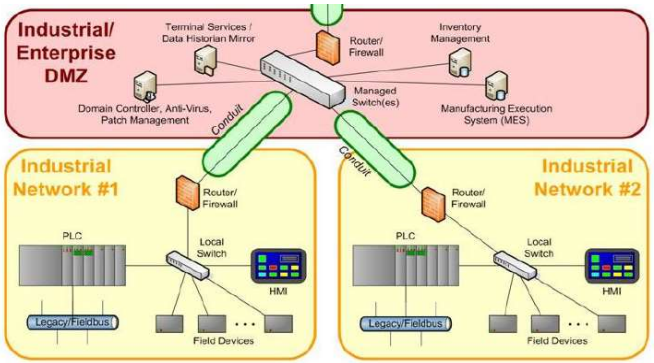
PKI/Certificate as security enabler in IIoT

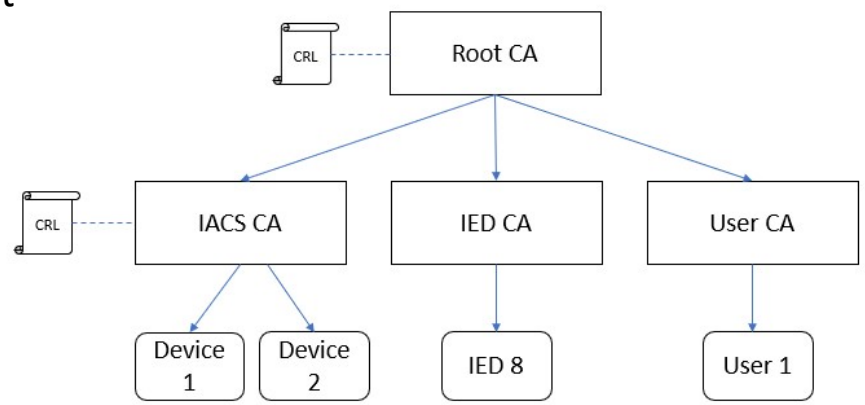
- “Executable” integrity through Digital Signature
  - Firmware signing, software signing
- Device authenticity
- Secure communications (confidentiality, integrity, non-repudiation) between entities
  - Software 2 Software, Software 2 Machine or Machine 2 Machine.
- User authentication (User digital certificate)
- Authorization / Role-Based-Access-Control (in client entity’s certificate)

- handle industrial security standard requirements:
  - IEC 62443-4-2 : Industrial Automation Control Systems
  - IEC 62351 (Part 8 & Part 9) : Power System

PKI /Certificate interest in IIoT environment

- Bring trust to entity's(*) digital certificates (X509)
  - Certificate Authority (CA)
- Remove trust by revocation of entity's digital certificate
  - Certificate Revocation List (CRL)
- Lifetime of entity within the IIoT system
  - Rely on Timestamping
- Centralized management of devices and users
  - Ease device commissioning/decommissioning, device replacement
- PKI Trust Model
  - e.g Hierarchical Trust Model fits industrial system structure
  - Can take into account regular evolution of the industrial system

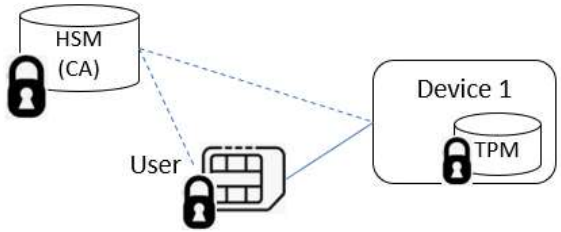




- *(*) Entity = device, user,…*

PKI /Certificate challenge in IIoT (1)

- Store securely private key (confidentiality) and pub. key/certificate (integrity)
  - Hardware Security Module : CA management
  - Secure element / TPM at device level,…
  - Secure storage for User : Smart card, …



- Require very strong process to manage/operate the PKI in a secure way
  - Security policies definition, CA/certificate creation & revocation , CRL creation, …
  - Strong competencies
- Need several PKI (*operational responsibility*)
  - Manufacturer PKI : e.g Firmware signing
  - *System Integrator PKI (potential): for system design and installation*
  - End-User PKI : final commissioning on end-user infrastructure

PKI /Certificate challenge in IIoT(2)

- Lifetime of Industrial system and product
  - Need accurate definition of the lifetime of CA , entity certificate,…
  - Be able to manage Post-Quantum shift ?
- Has to fit Industrial operation constraints (device installation & replacement) with secure commissioning
  - Allow offline device enrollment to CA
    - Through Certificate Signing Request (PKCS#10) generated in Device
    - Need secure manual operation to send back certificate in device
  - Allow online device enrollment to CA
    - Use of enrollment protocol SCEP, EST (*e.g listed in IEC 62351*)
    - Manage certificate renewal
  - Deploy certificate of new device to other connected devices (M2M)
- Need to have/set
  - connection to End-User CA/system owner, generally on Premise
  - connection to a CRL distribution point or to an OCSP responder

PKI /Certificate challenge in IIoT

Q&A