ETSI IoT Week 2022

IoT Devices Identity Management

Lorenzo Gatti – InfoCert S.p.A.

14/10/2022

ETSI IoT Week 2022

Lorenzo Gatti (Male) is a Software Architect focused on the device management world and the IoT ecosystem. Since 2010 he has focused on the field of SCADA remote control in the utility world working for the major Italian electric and gas companies.
Since 2020 he works for InfoCert as IoT Innovation Manager focusing on the security of IoT devices using PKI systems and standard authentication protocols.
At the end of 2020, he joined the TC-57 Committee of the IEC group related to the IEC62351 specification dedicated to IoT electrical device communication.

Contacts:
Email: lorenzo.gatti@infocert.it
LinkedIn: www.linkedin.com/in/lorenzo-gatti-b53b1479

14/10/2022

IoT Week 2022

SUMMARY

1. IoT Identity management: a wide range of problems
    1. Technical standard & National regulations
    2. Public vs Isolated network
2. Current state of the art
    1. PKI & Certificates
    2. Enrollment protocol – EST
    3. A strange story: OCSP Stapling
3. InfoCert MIDPKI
    1. EST use case: EV Charging stations
    2. Italian use case: Observability Project
4. IoT and the future

14/10/2022

Connecting your IoT Device to an existing Platform is not simple as you can imagine.

There are a lot of problems regarding a few basic questions:

- How can my platform recognize the device as mine?
- How can the device trust the destination of its communication?

In addition, during an IoT device installation and power-up, several actors are involved in the process.

- Manufacturer plant
  - Identity is generated here?
- Production process
  - Isolated?
- Installer operator
  - 3rd parts? Trusted?
- IoT platform
  - Which vendor? Capabilities? Constraints?
- Protocols

- Mutual authentications? Encryption?

Current IoT regulations are:
- Technical specification
- Focused on device management and device data without device identity in mind

IEC 62351 is a specification target electrical devices.
Explicitly requests the usage of X,509 Certificate to identify a device.
In addition, the standard requests use the EST (RFC 7030) to distribute and manage the device identity.

DNP3 follows the same way as IEC specification.

From the National side there are some little steps in the direction of regulating device identity management and security.
Important concept - federation between subjects:
- Smart grids
- Smart cities

the Italian regulatory act (540/2021/R/EEL) requests the owner of > 1MW electrical plants to install and manage the 'CCI' - Central plant controller - that enables the observability of the network from the Italian authority - Terna. The CCI requires an X509 Certificate used by Terna to identify the device and accept the data using their IoT Platform and SCADA.

The network is the major difficulty you can face during the design of your IoT installation.
Protocols like MQTT and platforms rely on cryptographic tokens (X,509 certificates) to setup the communication.

The network which contains the devices could be:
- Public: connected to the internet (remote installations or renewables plants)
- Private: no internet connection – VPN (factories, plants)

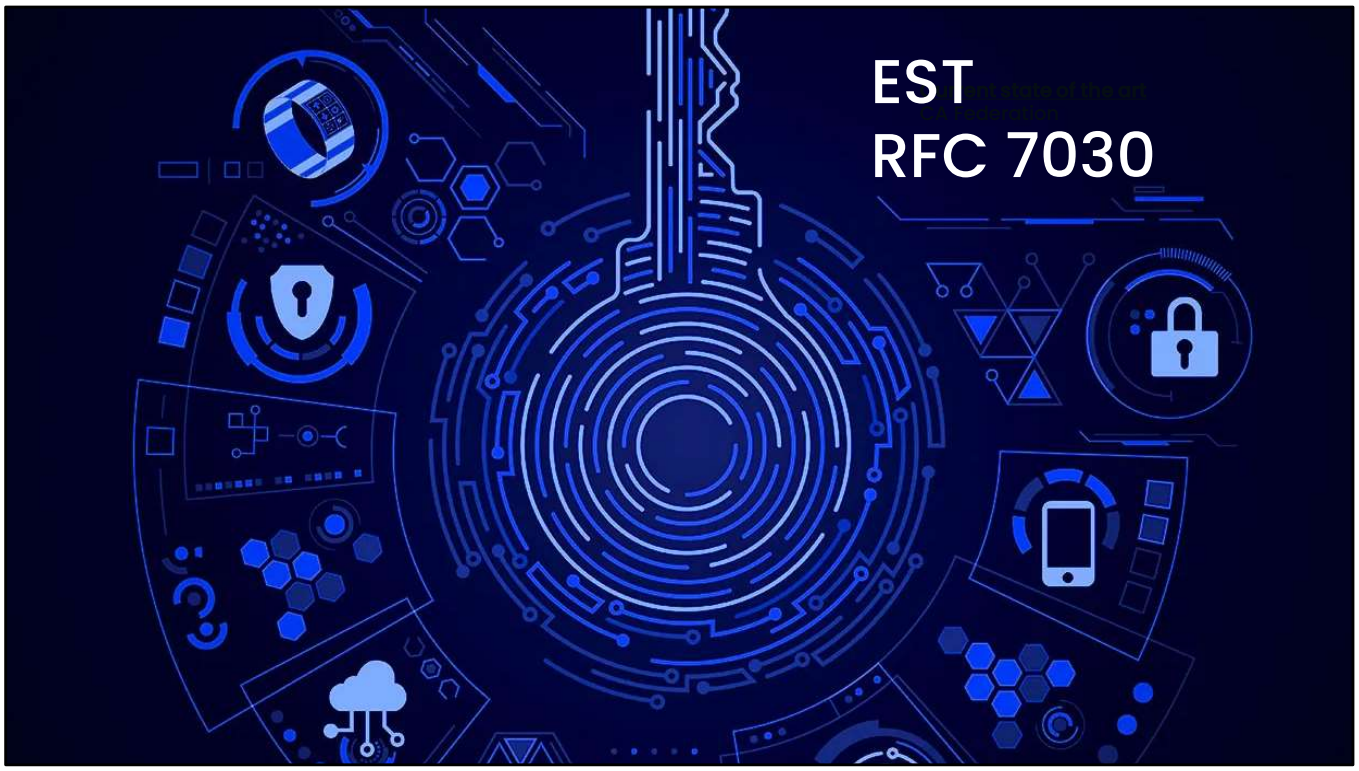
When your device is installed in a private and isolated network – a plant, a remote field, or a highly secure subnet - the question is how to publish the state change of the certificate or make a certificate request.

Integrating your device with a 3rd parts vendor is a problem and must be managed carefully.

PKI capabilities are:
- Emit certificates as device identity
- Manage certificate lifecycle: revoke, suspend, renew
- Federation with 3rd parts PKI (CA Trust Chain)

The adoption of a PKI as an Identity Management tool for the IoT is possible due to:
- The device mounts TPM – or Secure Element – from the beginning
- High Device calculation capabilities (RSA 2048, Elliptic Curves, Hash)
- Intelligent routers or network devices (dockerized local environment)

OCSP and CRL are the latest concepts that can be useful to manage IoT device identities. Revoke, suspend and reactivate certificates are mandatory in the modern world.



PKI and Certificates aren't very smart or agile objects. Usually, in the human world, releasing a certificate involves a very complex procedure to recognize the requestor and a human operator that verifies the identity. In the IoT world, this is not possible due to distance, the number of devices and other constraints.

The current standard-de-factor protocol used to release a certificate to a device is called EST (RFC. 7030), very different from the previous one SCEP.

EST is based on:
- CA federation
- TLS authentication
- Trust chain runtime distribution

EST Enrollment on a device needs at least:
- Device Private Key and Certificate emitted by the manufacturer CA
- Certificate of the EST Server endpoint

- EST Server endpoint

IMPORTANT: IF the device manufacturer owns a PKI, the device can be enrolled at start-up only federating the relative CA. No password or secrets sharing.

OCSP returns the state of a certificate – revoked or suspended. Using it in the IoT environment is mandatory to verify the TLS Tunnel authentication.

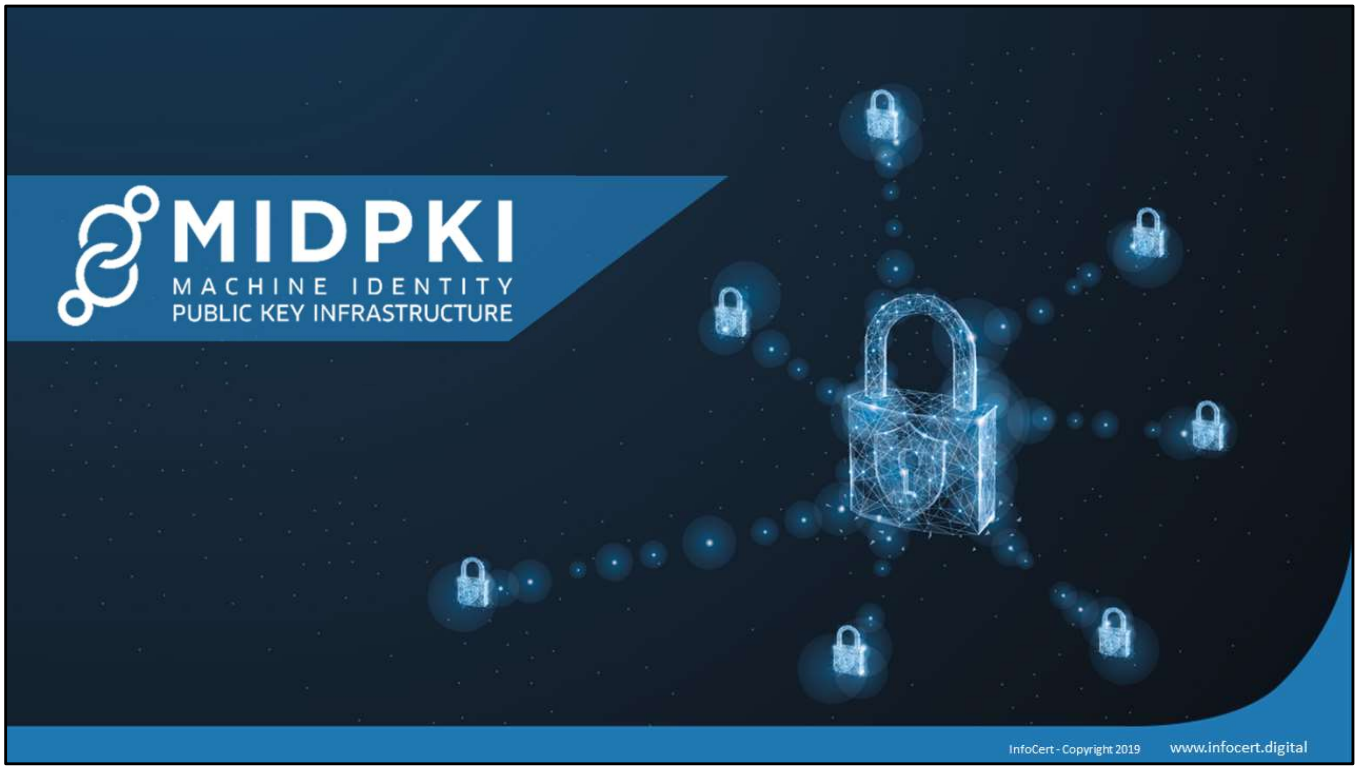
Standard OCSP is used from the server side (IoT Platform):

- The device opens the TLS channel
- Platform responds with its certificate
- The device queries the OCSP to retrieve the certificate status.

In a private network where OCSP is not reachable server response will contain the OCSP response also – OCSP Stapling.

Missing feature: OCSP from the client side. This feature is already described in TLS 1.3 but is not mandatory and no SSL library implements it (OpenSSL, mbedTLS).

Handle OCSP staples in client certificates · Issue #12921 · openssl/openssl (github.com)



InfoCert has developed a new kind of PKI. Standard PKIs are designed around the emission of certificates (this is the core of a PKI) but MIDPKI (Machine Identity PKI) is different.
MIDPKI releases identity. This identity can be:

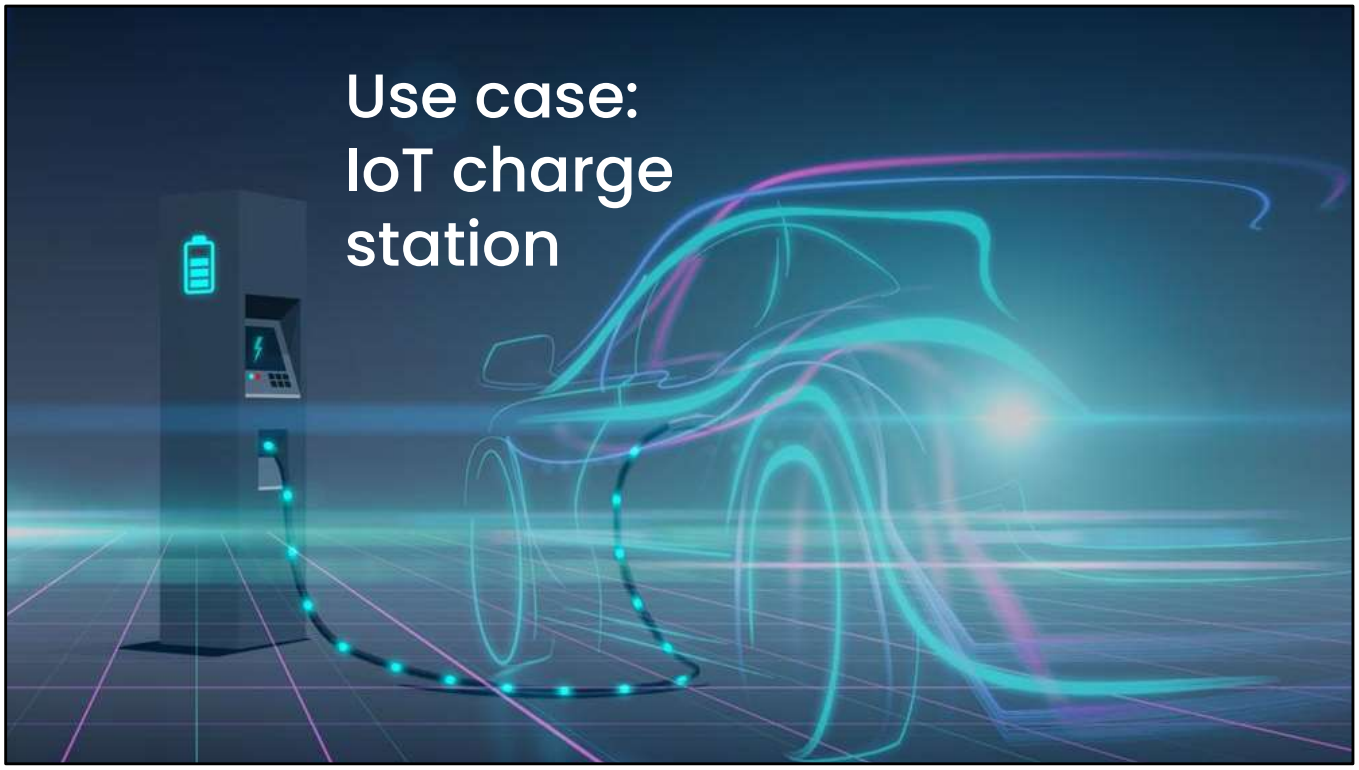
- X.509 Certificate
- OpenSSH compatible certificate (to open the door for the remote configuration)
- LoraWAN symmetric keys
- FIDO identity

Another difference from a standard PKI is the definition of an enrollment process. Usually, in a PKI you can find the support for SCEP,ACME and EST protocols with a set of user interfaces where the RAO configure the emission of certificates.
In MIDPKI we have developed a human administration interface but the most important feature is a set of enrollment business flows and automation. Our rules are:

- IoT doesn't require human intervention

- IoT needs support for huge numbers

MIDPKI is fully compatible with IEC 62351 Certificates also.



InfoCert has deployed the MIDPKI installation to support an interesting use case – EV Charge stations.

Requirements:
- Station identity managed using X.509 Certificates
- Automatic enrollment and renewal of certificates using EST protocol
- Remote management of the station using OpenSSH Certificates

Business flow developed:
- Creation, management and distribution of EST Pre-Enrollment tokens (temporary certificates)
- Integration and release OpenSSH Certificates with device identity and human roles.

MIDPKI is the identity management software in the Enel-X recharging station architecture. Connected to the Enel-X backend IoT Platform, a recharging station needs an X509 Certificate to

authenticate itself using standard protocols.

Italian Terna electricity authority resolution 540/2021 defines:

- The purpose is to real-time monitor electricity production plants with power greater than or equal to 1 MW connected or to be connected to medium voltage grids
- The usage of IEC 62351 specification
- EST usage to manage certificates
- TLS communication between actors

Major challenges:

- Different manufacturers and technologies
- Segregated and isolated networks – no internet access
- Remote installations – no remote PKI
- Multiple owners

NOTE: The Danish electricity authority is following the same path with a similar norm.

Smart Grids and Smart cities are the future and the world will become connected, based on some new technologies:

- 5G networks will open the way to TLS stable communication for all devices so certificates become very important.
- More secure and isolated Trusted Platform Modules – TPM
- Reliable batteries
- Greater computing power

PKI must follow the innovation path with:

- Support for new certificate-less protocols – LoraWAN, Sigfox, FIDO
- Approaching the field with the EdgePKI design
- National level CA federation