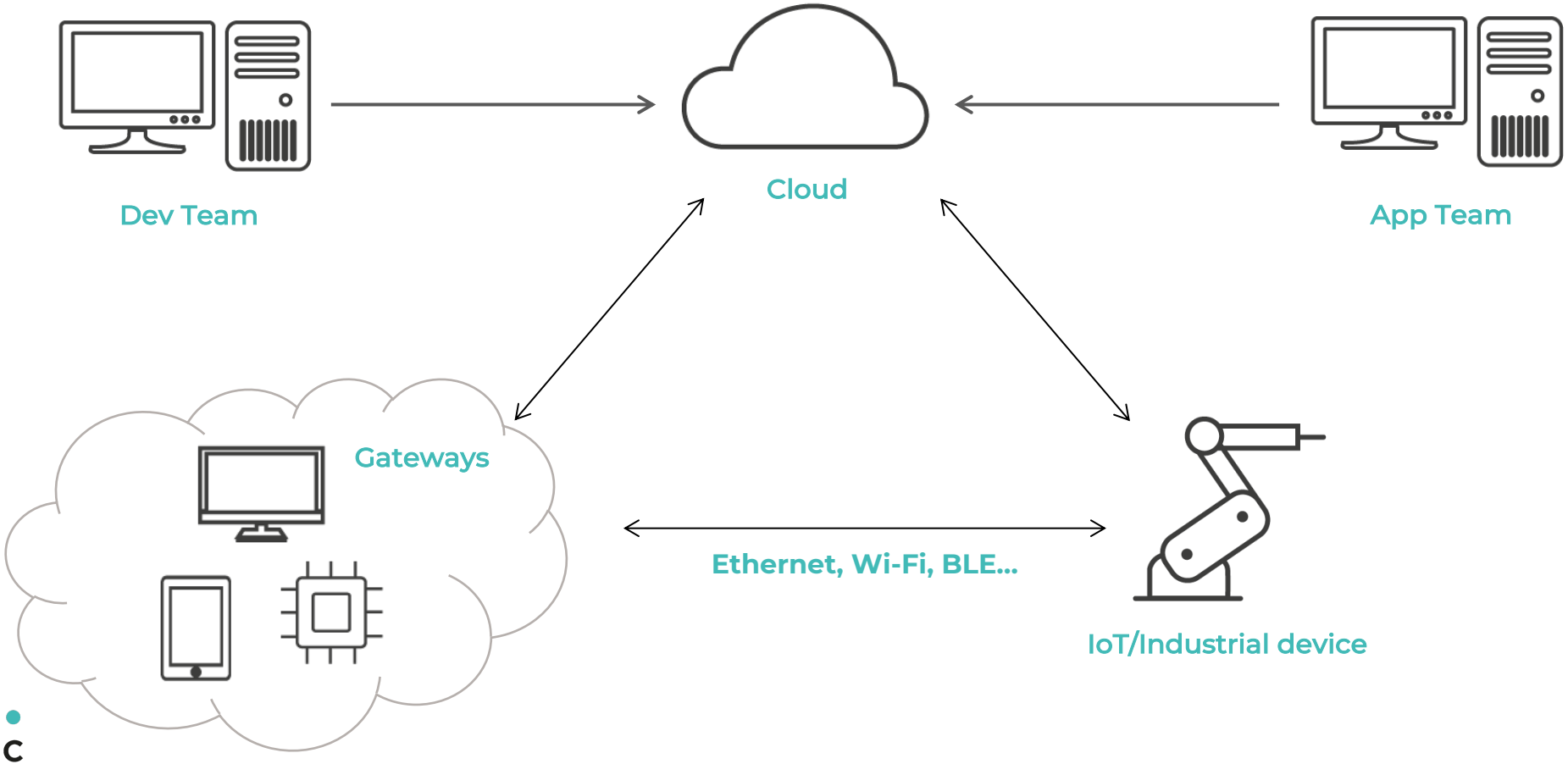
A case study

IoT system overview



Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

Security objectives

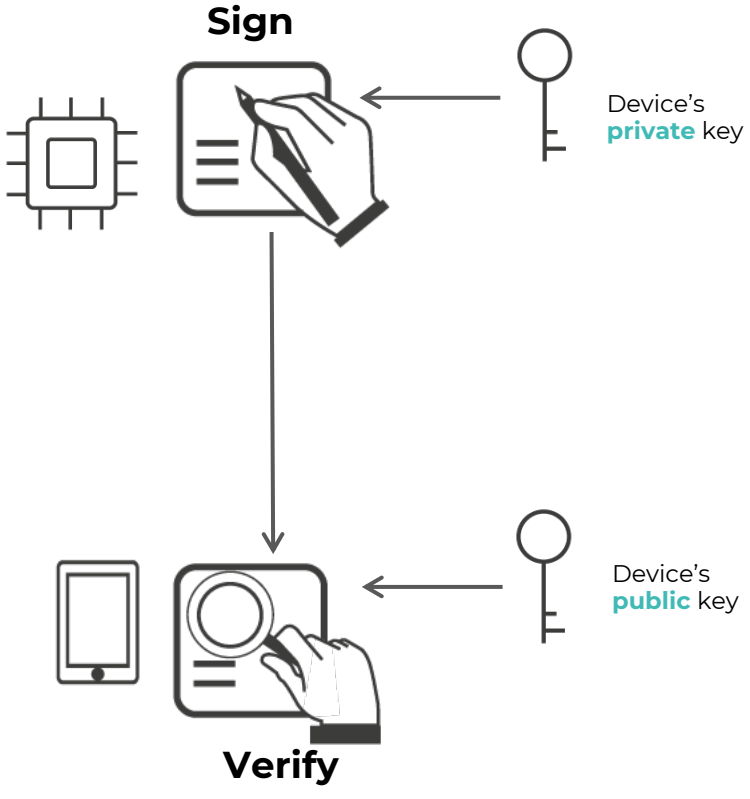
- Identify users and devices
  - Who is who
- Provide secure services
  - Data streams
  - Manage device firmware
- Rely on standard components as much as possible
  - Public key cryptography, certificates and PKI

Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

Public Key Infrastructure

Public Key Cryptography

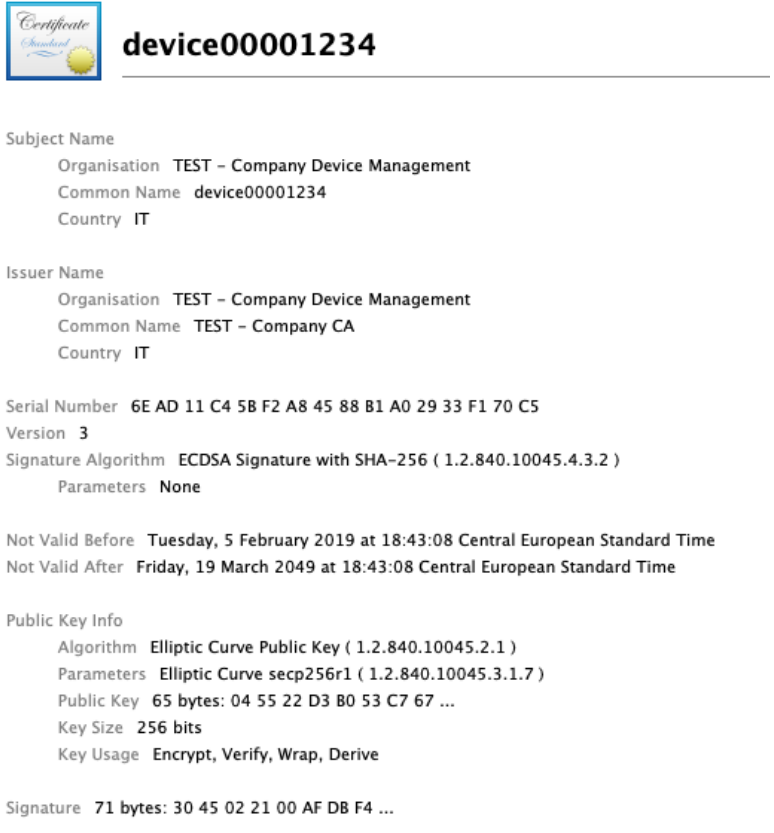
- Each entity has a key pair
  - Private key
    - The owner must keep it secret
  - Public key
    - Distributed to other parties
    - Secure association key and owner
- Main applications
  - Digital signature
  - Authentication
  - Key exchange



Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

Certificates

- Electronic document used to au
  - Subject (identity of key's owner)
  - Public Key
  - Issuer's signature (trusted entity that ha contents)
  - Constraints on the key duration and usa
- Standard format is X.509v3



Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

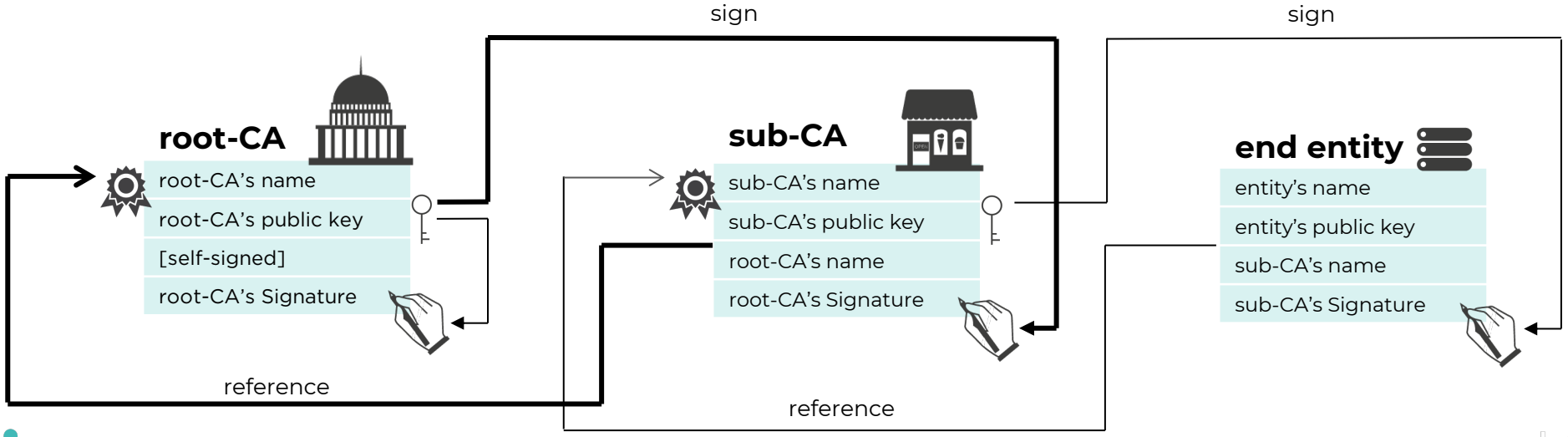
Certification Authority

- The primary role of the CA is to digitally sign certificates
  - Signature is again a digital signature
- CA's Private Key is the most sensitive data of the whole ecosystem
  - If compromised, the whole system is compromised
  - Need to be securely stored (e.g. dedicated HW)

Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

Certificate Chains

- Hierarchy of root-CA with sub-CAs
  - root-CA delegates some tasks to sub-CAs
  - Compromising a sub-CA does not affect the other CAs



Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

Key ceremony

- Procedure to generate the CA's key pair
  - Using a dedicated machine with no connections
    - An ad-hoc virtual machine can be used
  - Keys are generated and securely saved (e.g. into a dedicated HSM – Hardware Security Module)
    - A non-digital backup of the keys is made (e.g. on paper)
  - The machine is securely cleaned from sensitive data
    - Or even destroyed
  - Cost/security trade-off

Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

Generation of credentials

- Each entity must have its own credential
  - In particular each end device must have it
  - Each user with specific role (Dev/App team)
- Device’s credential is composed of
  - Private keys stored on the device
  - Public certificate bound to the device and trusted by all other entities
    - Released by a trusted CA

Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

IoT Secure Suite
Key ingredients

SECPAT

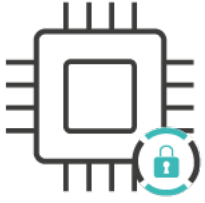
IoT® SECURE SUITE

The key ingredients

IOT SECURE SUITE®

PKI with dedicated CA

Smart Key provisioning process



Secure Key storage architecture

Secure FOTA

SEC PAT

Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

#1: PKI with dedicated CA

- State-of-the-art **PKI** with X.509-v3 standard certificates
- Ad-hoc **key ceremony**
- CA's private keys securely stored
- Secured procedure for device certificates generation

- Definition of PKI structure and its configuration
- Safe and reliable set up of PKI through key ceremony
- CA's sensitive data securely stored on HW Secure Token/HSM

Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

#2: Smart key-provisioning process

- Each device is provisioned with a unique set of keys
  - For secure device authentication
  - For secure firmware upgrade
  - Application-specific keys
- The key-provisioning process is secured

- Fine-grained device identification
- Device strong authentication
- Secure data exchange between devices and cloud

Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

#3: Secure key storage architecture

- Hardware protection of sensitive data
  - Platform-specific security mechanisms
  - Secure Element (SE)
- SE safely stores secrets and private data
- SE enables secure exchange with other system elements

- Non-clonable device
- IP protection

Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

#4: Secure FOTA

- The firmware is encrypted and signed
- The devices can determine whether the firmware is genuine or not

- Firmware over-the-air accessible only to genuine devices
- Only genuine firmware can be installed on devices

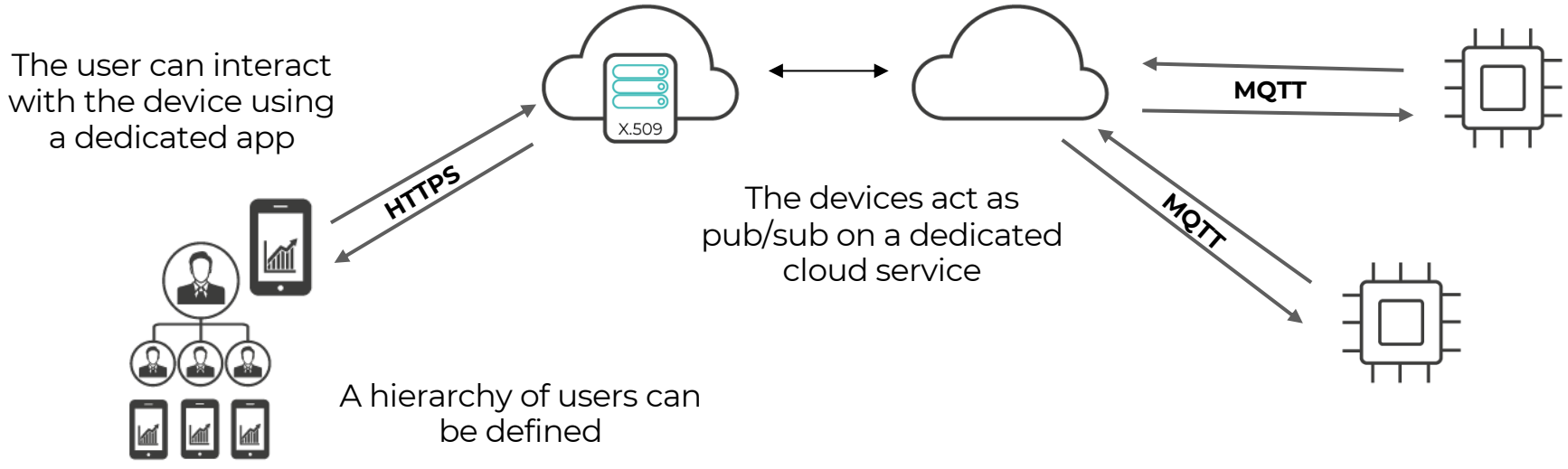
Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

A case study

SECPAT

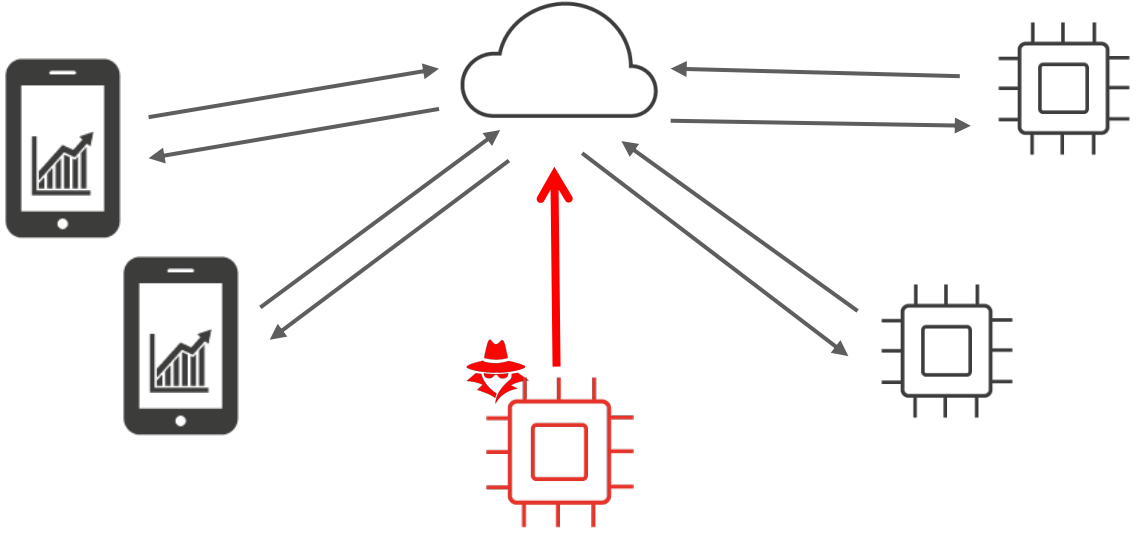
IOT SECURE SUITE

Interactions



Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

Security requirements

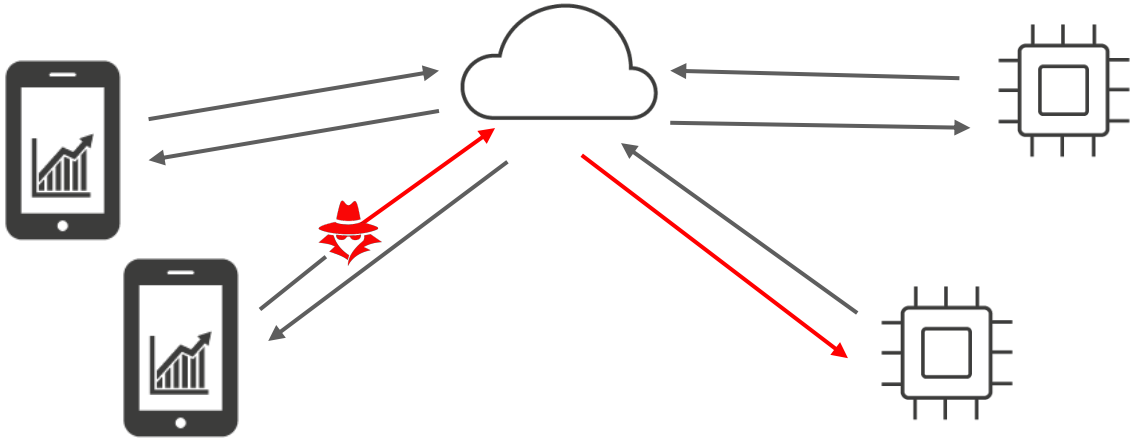


Security requirement #1:

Prevent the use of infrastructure by unauthorized devices and/or users

Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

Security requirements



Security requirement #2:

Ensure that remote commands cannot be manipulated from third parties

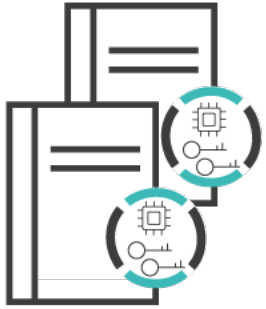
Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

Securing the architecture

#1: PKI with dedicated CA

Safe and reliable setup of PKI with a dedicated CA

Embedding of CA certificates on mobile clients



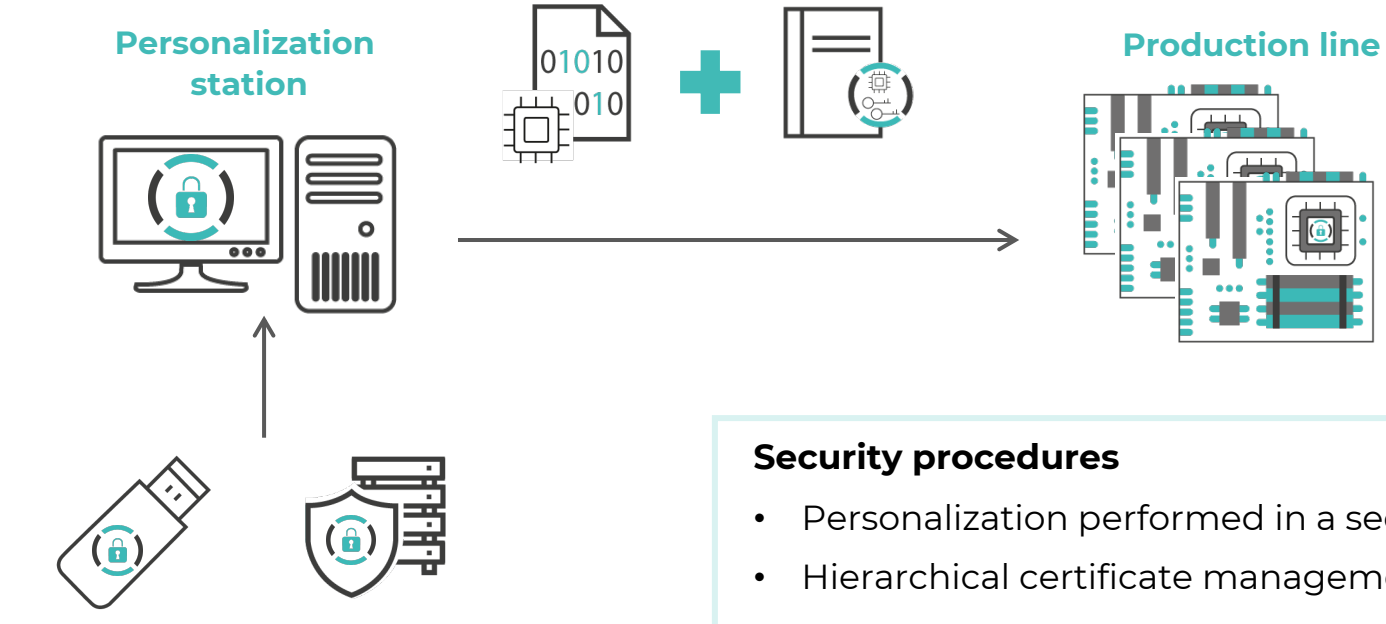
Definition of a secure procedure for device certificates generation

Security procedures

- CA's private keys are securely stored on a Secure Token/HSM
- CA is hosted on a dedicated machine with no connection
- CA can generate device's certificates either on-the-fly or in batches

Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

#2nd: Smart-key provisioning process

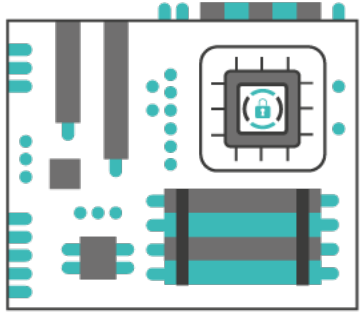


Security procedures

- Personalization performed in a secured line
- Hierarchical certificate management
- Personalization software with native interface for Secure Token/HSM

Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

#3: Secure key storage architecture



Each genuine device hosts a SE that safeguards device's private information.

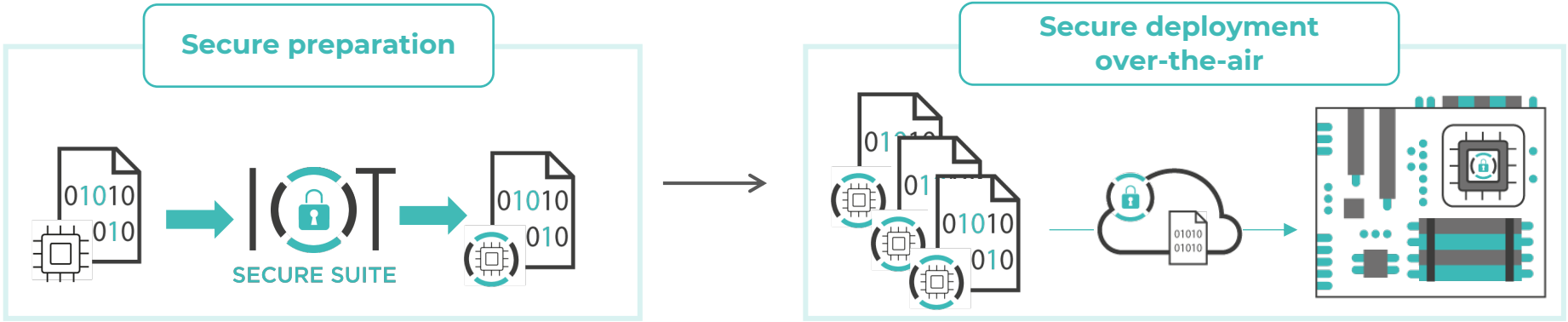
Security procedures

The Secure Element stores:

- Key material for firmware decryption
- Device's private keys for authentication
- Device's certificate

Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

#4: Secure FOTA



Security procedures

- Firmware update is **encrypted**
- Firmware update is **signed** with the Development Team's private key

Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

The results: IoT Secure Suite®

SECURE SUITE®

We take into account all the components of the system

Client protection

Channel protection

Data protection

Cloud protection

Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

Security: requirements vs achievements

REQUIREMENTS	ACHIEVEMENTS
Prevent the use of infrastructure by unauthorized devices and/or users	✓ Prevented the use of infrastructure by unauthorized devices and/or users
Ensure that remote commands cannot be manipulated from third parties	✓ Ensured that remote commands cannot be manipulated from third parties
	**+ Prevented the spread of unauthorized firmware upgrades**
	+ Prevented the theft of PII and IP
	+ Secured communication in the entire infrastructure

Private & Confidential | Copyright © 2021 Security Pattern s.r.l.

Thank You!

hello@securitypattern.com