EVIDEN

Automated and secure deployment of your IoT devices

Arnaud Duchamp
19/09/2023

an atos business

EVIDEN

1 Context

Context

Industries developing IoT usage

Smart Grid Utilities

Predictive maintenance
Smart metering
Threat detection on generator
Overvoltage detection

Smart Building

Building Management
Lift monitoring
Temperature monitoring
Smoke detection
Air quality monitoring

Health

Hospital devices
Building Management
Pacemaker and defibrillator
Real time remote medical monitoring
Insulin pump

Transportation

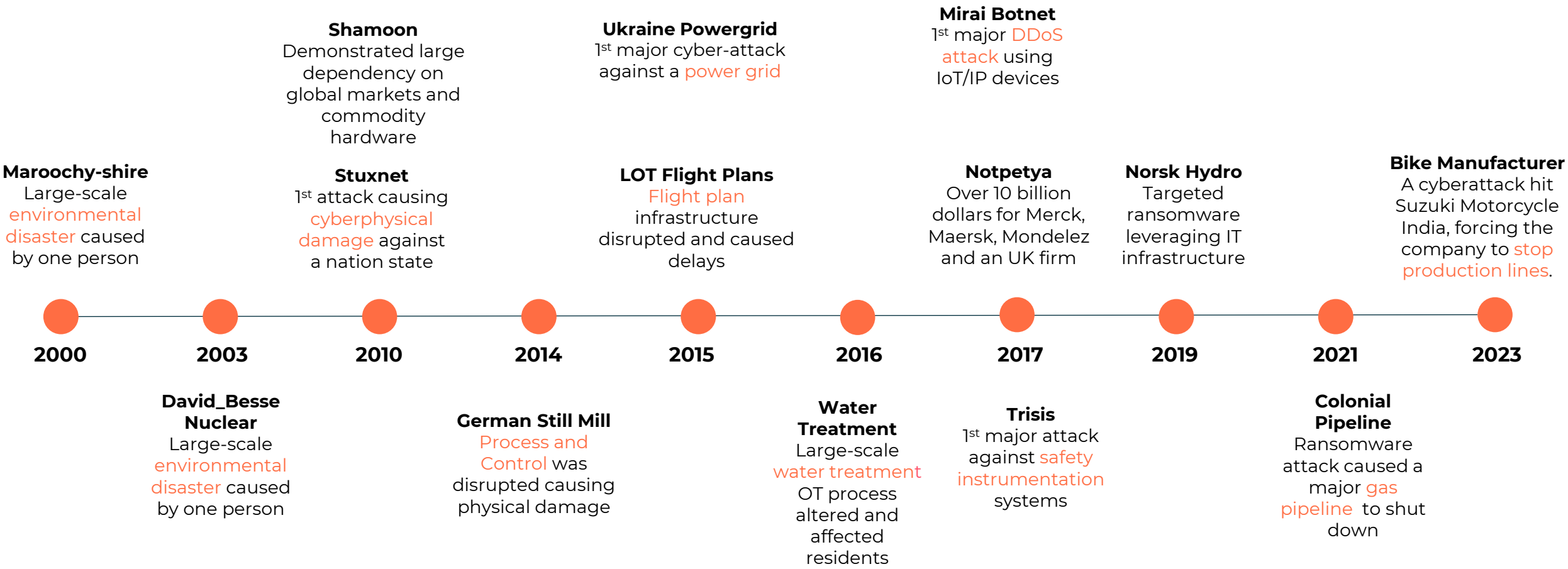
V2X security for C-ITS
Vehicle to grid
Heath, pressure, vibration sensors monitoring on railway infrastructures
SW upgrade integrity

Industry 4.0

Predictive maintenance
Remote maintenance and remote operation
Devices consumption monitoring

Context

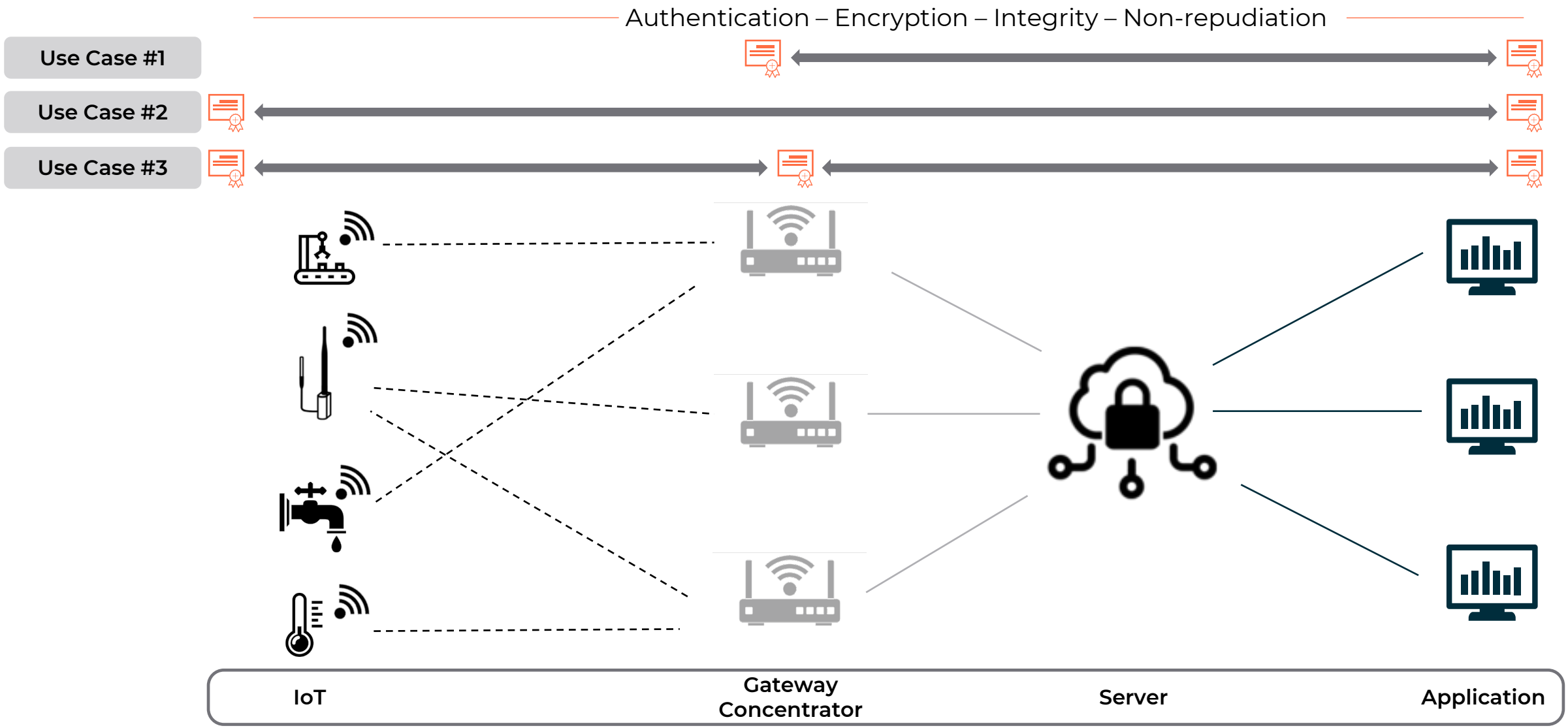
Samples Attack



EVIDEN

2 Objective

Achieve End to End Security



EVIDEN

3 Solution

How to achieve End to End Security?

Solution

Deliver a digital identity to every device

- X.509 certificate based identity issued by local PKI
- Proven technology
- Ensure authentication, encryption, integrity and non-repudiation functions
- Can be integrated with local authorization system

Note: Pay attention to the protection of the cryptographic keys

Protection level goes from:

- Rich OS, unsecure software zone located in the ”Normal World”
- Trusted Execution Environment, secured chipset zone not physically isolated from the rest of the chip
- Secure Element, separate chip including a secure processor for sensitive operations, tamper-proof storage for keys and runtime memory

Drawback

Delivering identities when integrating the device requires tedious operations:

- Manual check of shipment
- Local Asset registration
- Creation of record in commissioning tool
- Manual local registration and profiling
- Manual key pair generation (usually using openssl)
- Manual enrolment at PKI
- …

How to achieve End to End Security?

And how to avoid this cumbersome integration phase?

Solution

Deliver a digital identity to every device at the factory stage.

Device gets its immutable identity in Manufacturing site and throughout the whole life of the device.

It allows to:

- Integrate security capabilities into devices
- Protect intellectual property rights and fight against counterfeit products

Examples:

- Alstom provides digital identities to devices integrated within their train during manufacturing
- Siemens includes digital identities into his devices like PLC for smart factory

Drawback

This manufacturer identity is then issued by a manufacturer PKI.

Customers don't necessary need to trust all certificates issued by a manufacturer PKI.

Customers would prefer to take advantage of their own PKI and rely on their trusted Root CA.

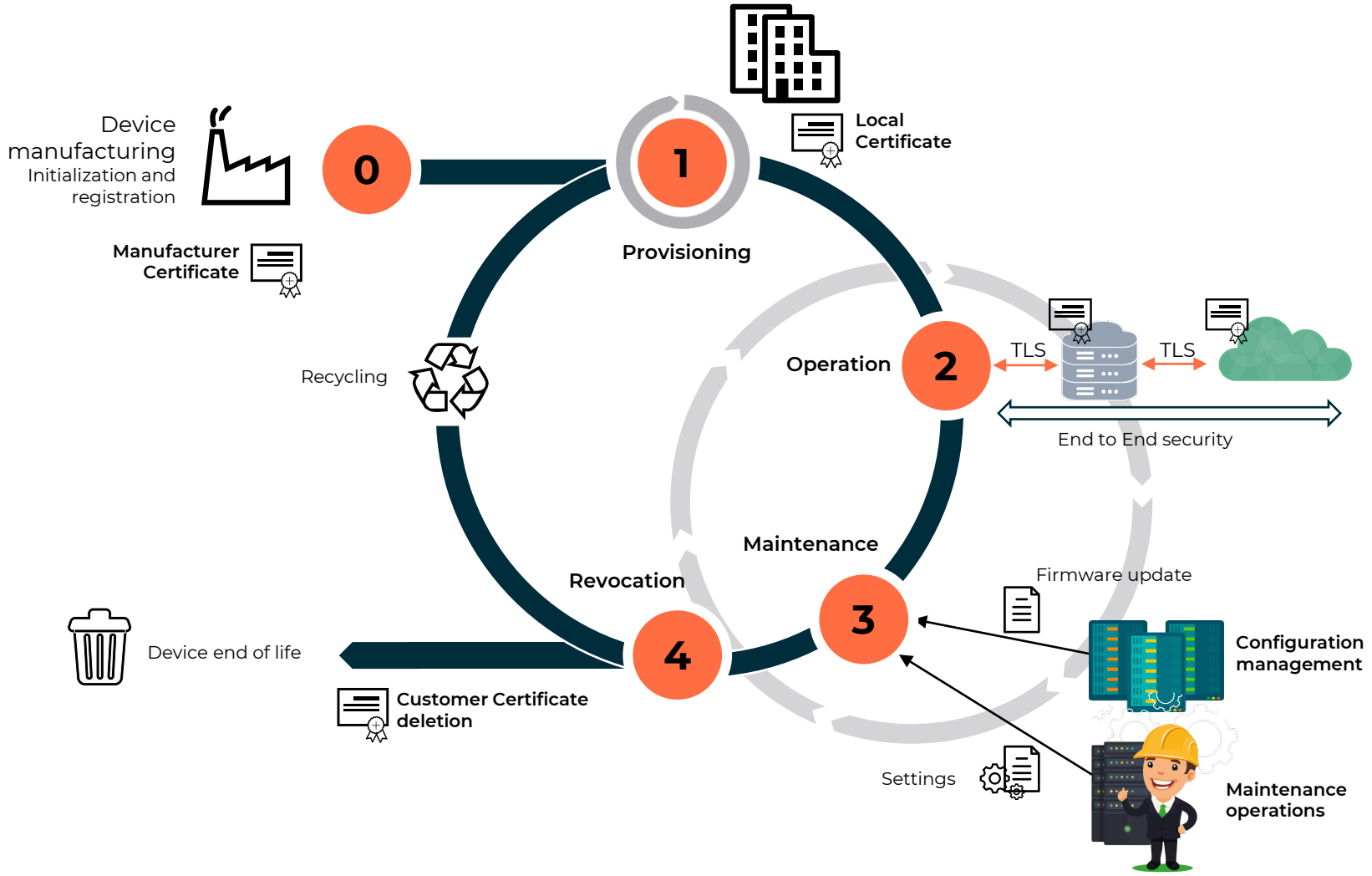
Customers would like to be able to renew the device identity to strength security (larger keys, crypto-agility)

Alstom solved this issue by delivering a "PKI in a box" together with their train.

They're transferring the PKI operation when delivering a project to a customer

How to achieve End to End Security?

Ideal solution, take advantage of Manufacturer and Local Certificate



Certificate based authentication

Communication encryption

Permission management

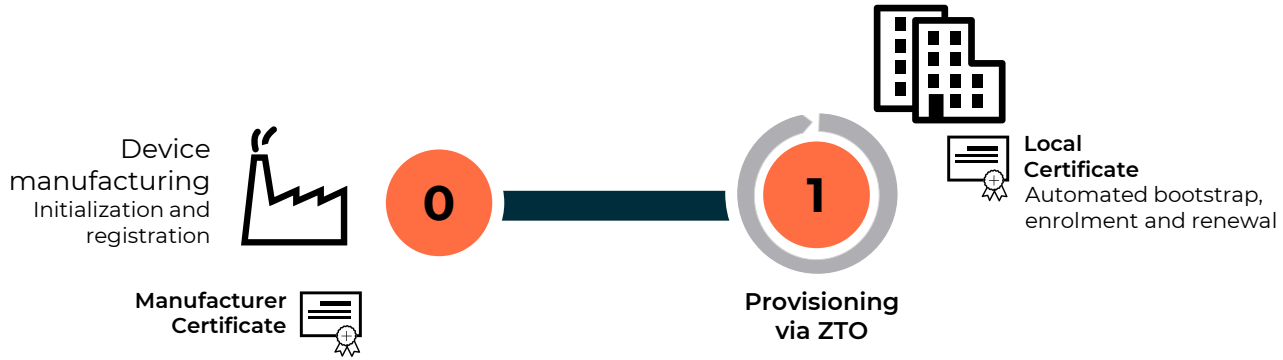
File Integrity

Source Authentication

Permission for maintenance

How to achieve End to End Security?

Ideal solution, take advantage of Manufacturer and Local Certificate



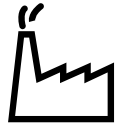
EVIDEN

4 Zero Touch Onboarding

Provisioning via Zero Touch Onboarding

Manufacturer

Device manufacturing
Initialization and registration



Manufacturer Certificate

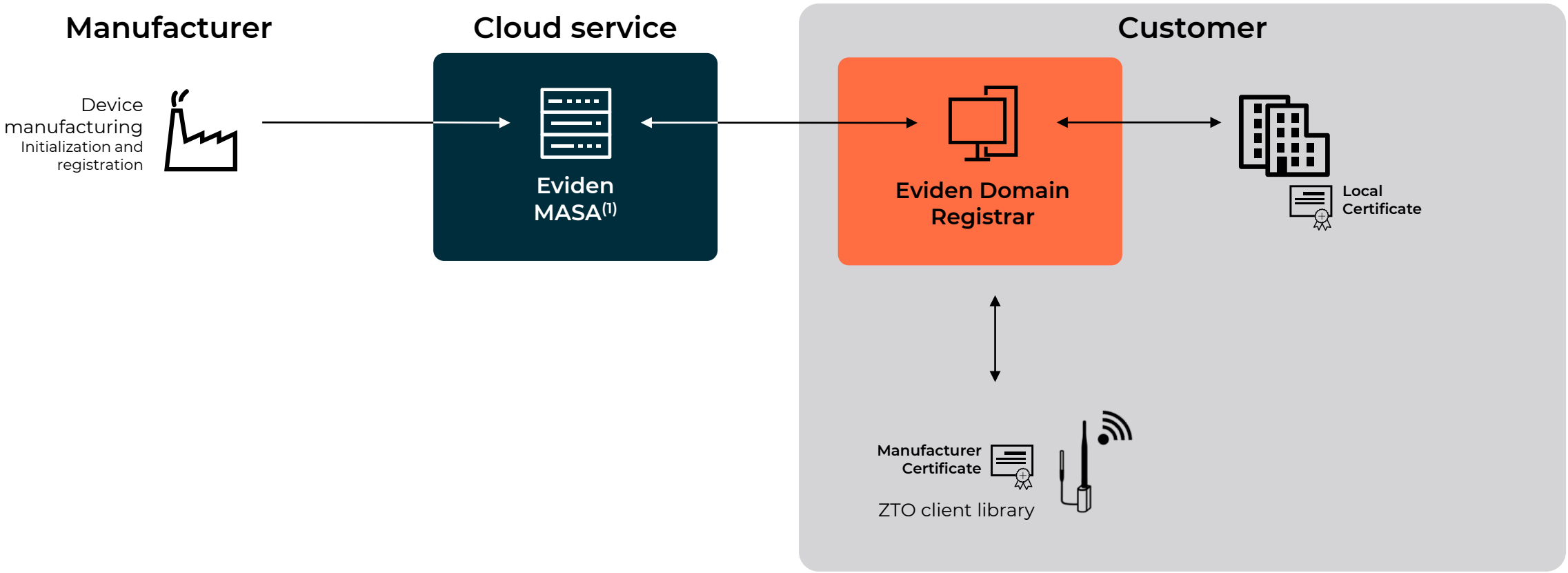
Customer

Local Certificate

Provisioning via Zero Touch Onboarding

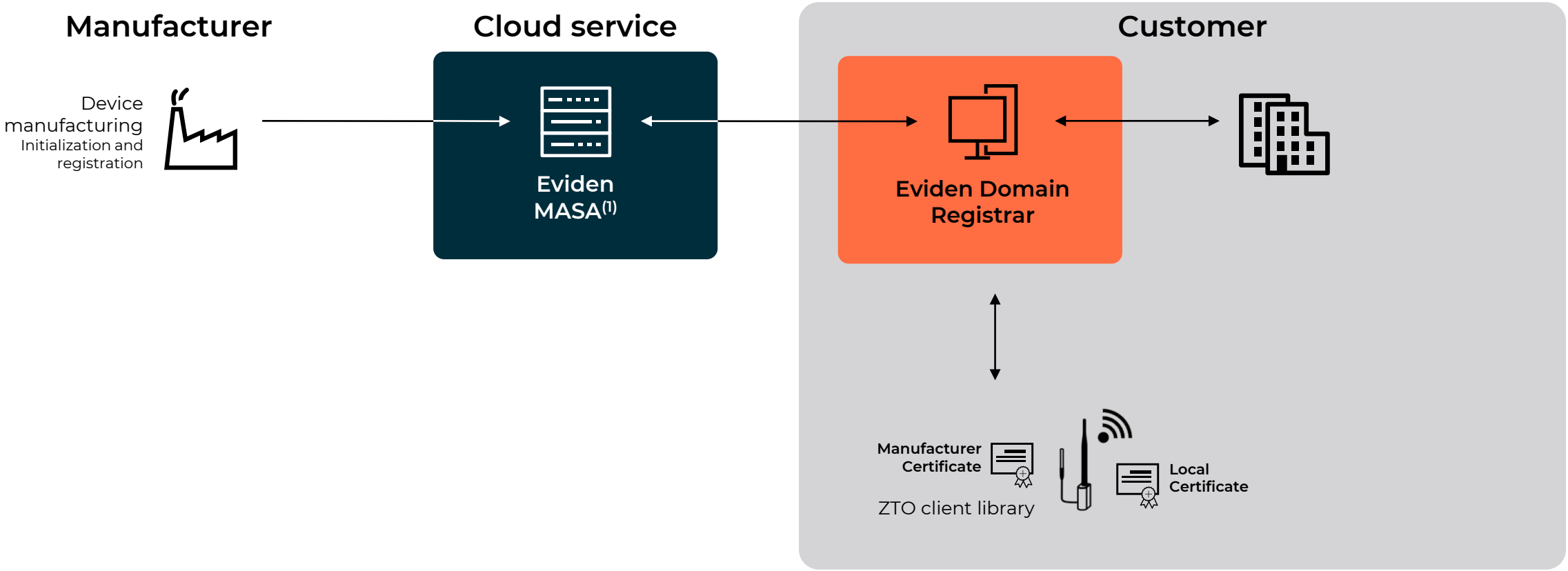
(1) MASA: Manufacturer Authorized Signing Authority

Provisioning via Zero Touch Onboarding



(1) MASA: Manufacturer Authorized Signing Authority

Provisioning via Zero Touch Onboarding



(1) MASA: Manufacturer Authorized Signing Authority

Key Benefits of Zero Touch Onboarding

Take-away

Increased cybersecurity

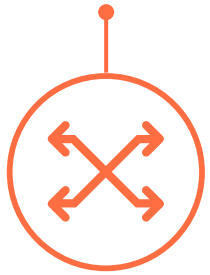
Protection against current threats and attacks by infected unprotected/non patchable IoT devices

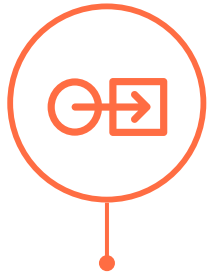
Easy, fast & secure deployment and operation

Automated & worry-free solution without effort

Modularity

Structured as modular system



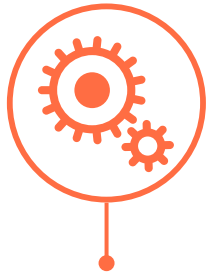


No expertise needed by the installer

Installer has no access to passwords and credentials

Compliance

Meeting legal requirements, compliance, guidelines industry standards and security policies, ensuring data security



Safety increase

Safety of machines managed throughout their lifecycle (during onboarding process and operation)

EVIDEN

Questions?

EVIDEN

Thank you!