Associazione Italiana Strumentisti

ISA Italy Section

«LE DIMENSIONI DELLA SICUREZZA INDUSTRIALE»
I percorsi della sicurezza industriale dagli standard ISA/IEC 62443 ai temi della cybersecurity

**Milano, 30 Maggio 2018**

**Auditorio TECNIMONT**

# Cyber Security basata su chiavi asimmetriche per l'ambiente power system (SCADA).

InfoCert

Fabrizio Leoni

# INTERNET OF THINGS

## THREATS AND CONCERNS 1/2

Insecure web interface

Week authentication

Insecure network services

Lack of encryption

Privacy concerns

Insecure cloud interface

Insecure mobile interface

Insufficient security configurability

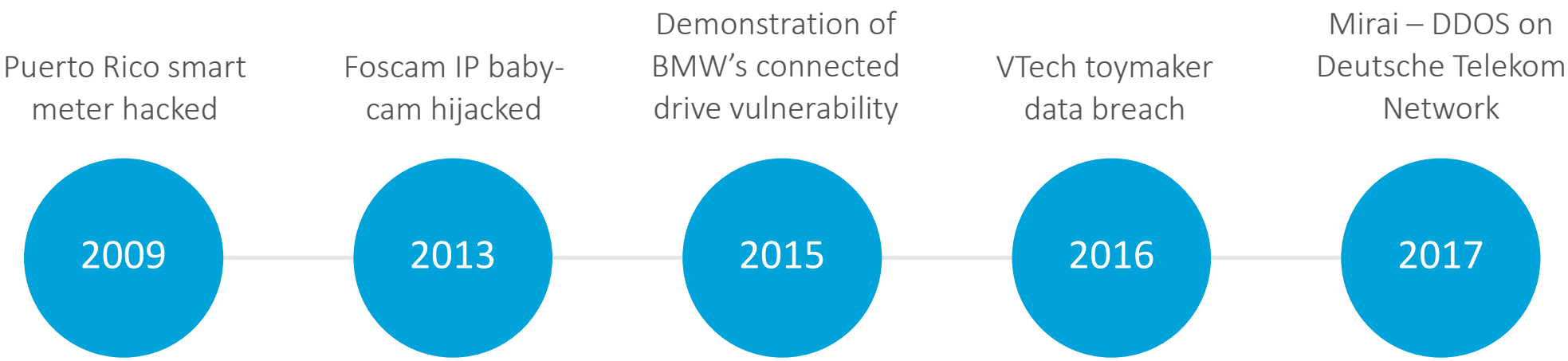
Insecure software

Poor physical security

InfoCert

# INTERNET OF THINGS

## THREATS AND CONCERNS 2/2



# INDUSTRIAL INTERNET OF THINGS

## CONVERGENCE OF IT AND OT TRUSTWORTHINESS

Information technology (IT)

IoT

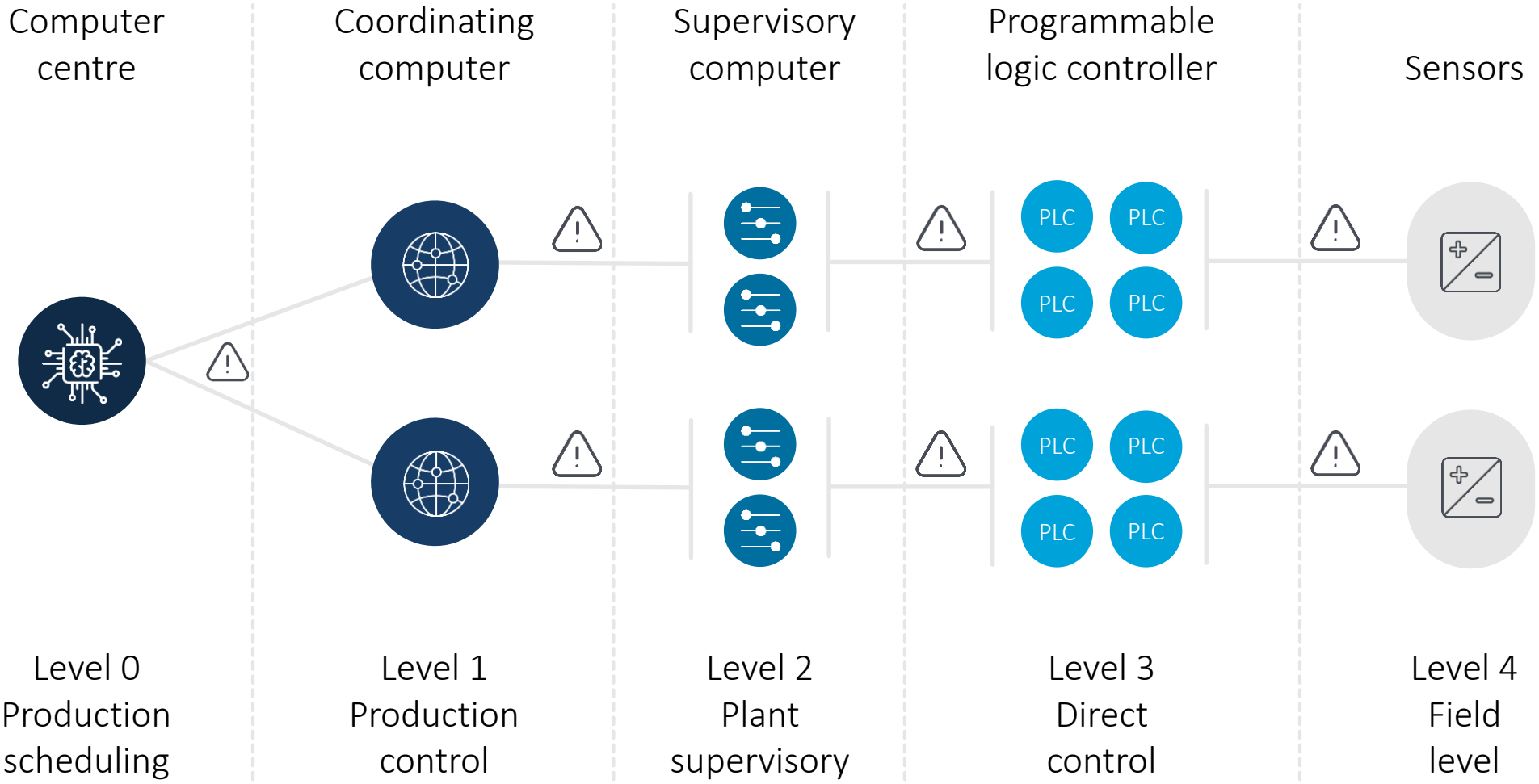
Operation technology (OT)

Safety  Privacy  Security  Reliability  Resilience

IIoT

# SCADA

## COMMUNICATION CHANNELS

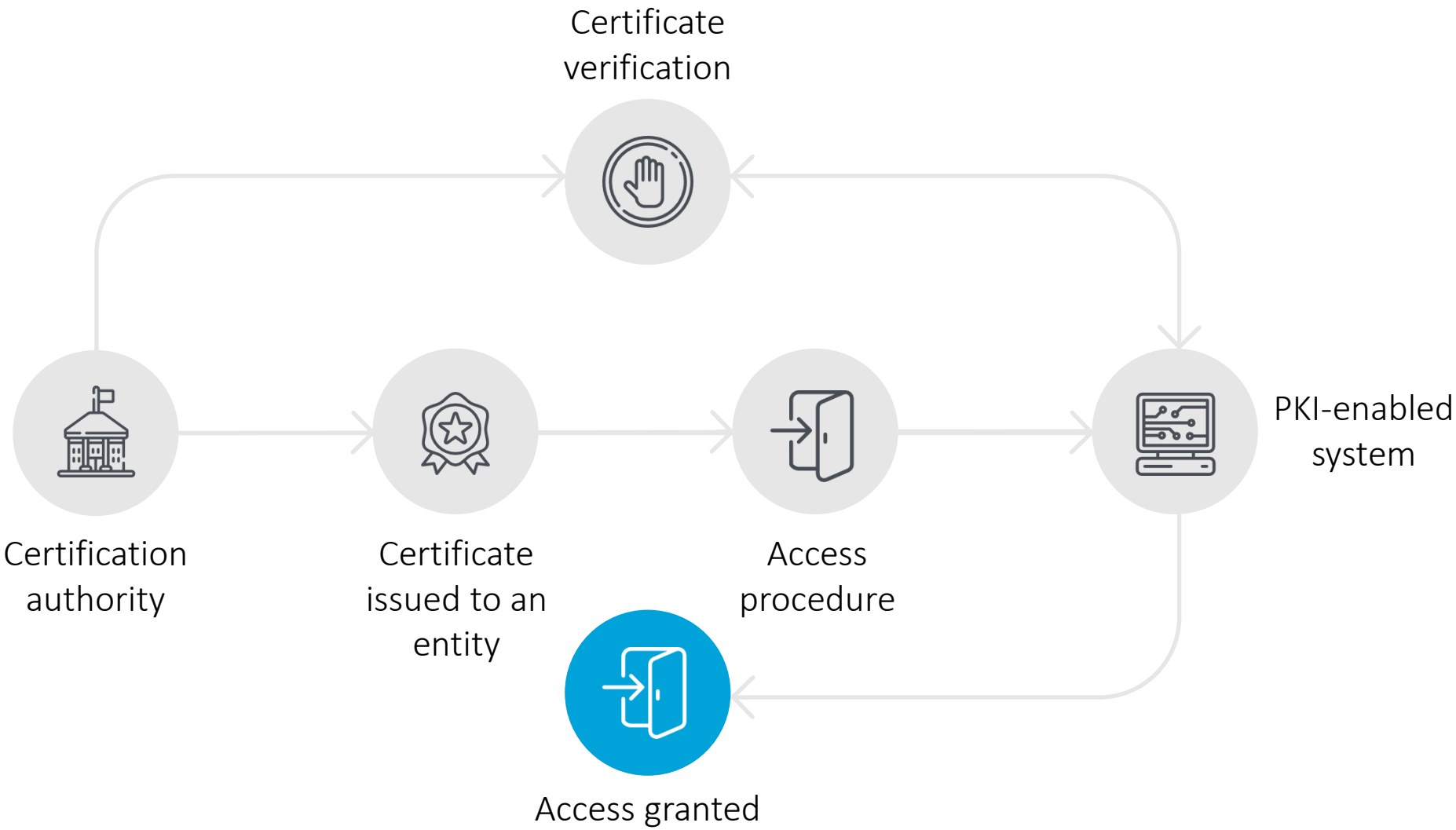


# PKI INFRASTRUCTURE

## MAIN COMPONENTS

# PKI INFRASTRUCTURE

## ENROLLMENT AND ACCESS PROCESS

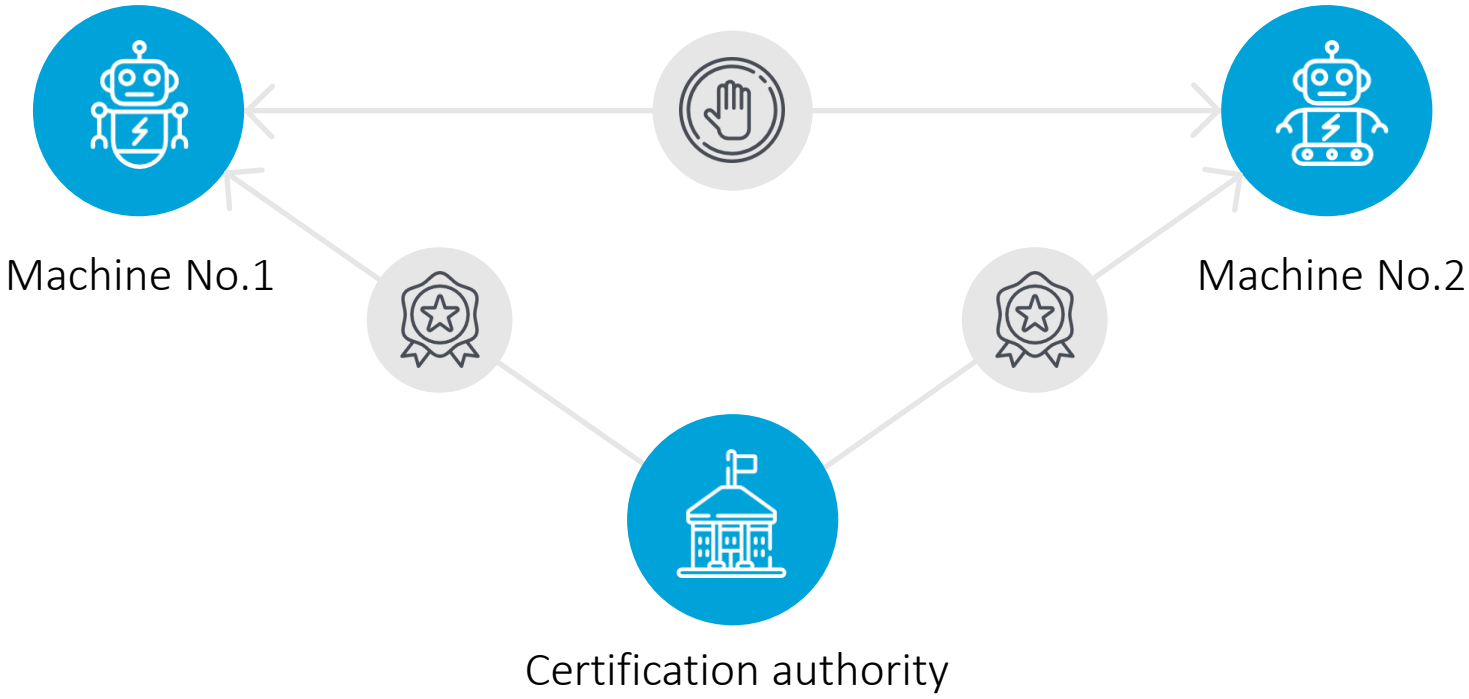


# IEC 62351

## GUAARANTING INTEROPERABILITY

IEC 62351 specifies cryptographic key management, namely how to generate, distribute, revoke, and handle public-key certificates and cryptographic keys to protect digital data and its communication.

The purpose of part No 9 of IEC 62351 is to guarantee interoperability among different vendors by specifying or limiting key management options to be used.



# IEC 62351 – PART 8

## ROLE BASED ACCESS CONTROL

Attribute certificates provide an effective way to separate the management of identity from the management of authorizations associated with an identity. Attribute certificates can be used to extend the information in a public key certificate. They allow for instance for temporary enhancement of the permissions of the public key certificate holder by specific role-based access information.

| Predefined Roles | | | |
|---|---|---|---|
| Attribute name | Value | Comments | M/O |
| Viewer | <0> | | M |
| Operator | <1> | | M |
| Engenieer | <2> | | M |
| Installer | <3> | | M |
| Secadm | <4> | | M |
| Secaud | <5> | | M |
| Rbacmnt | <6> | | M |

# INFOCERT CASE HISTORY

## HYDROPOWER GENERATION PLANT

# ENROLLMENT

## TO NATURAL PERSON OR SCEP THINGS

Natural person:

- The Registration Authority Officer perform the natural person identification;
- The authentication certificate request form is signed by the subscriber;
- The certificate is issued by the Certification Authority;
- The subscriber installs the certificate into the browser;
- The certificate can be sent by mail or downloaded through the RAO's system.

SCEP things:

- The ChallengPassword is created by the Registration Authority Officer and sent by this latter to the secure devices producer;
- The producer decrypts the file and installs the encryption keys in the secure devices;
- Each secure device has its own unique key;
- When the device is installed in the functioning environment the SCEP automatic enrollment process starts.

# ATTRIBUTE CERTIFICATE

## AREA OF RESPONSABILITY

1

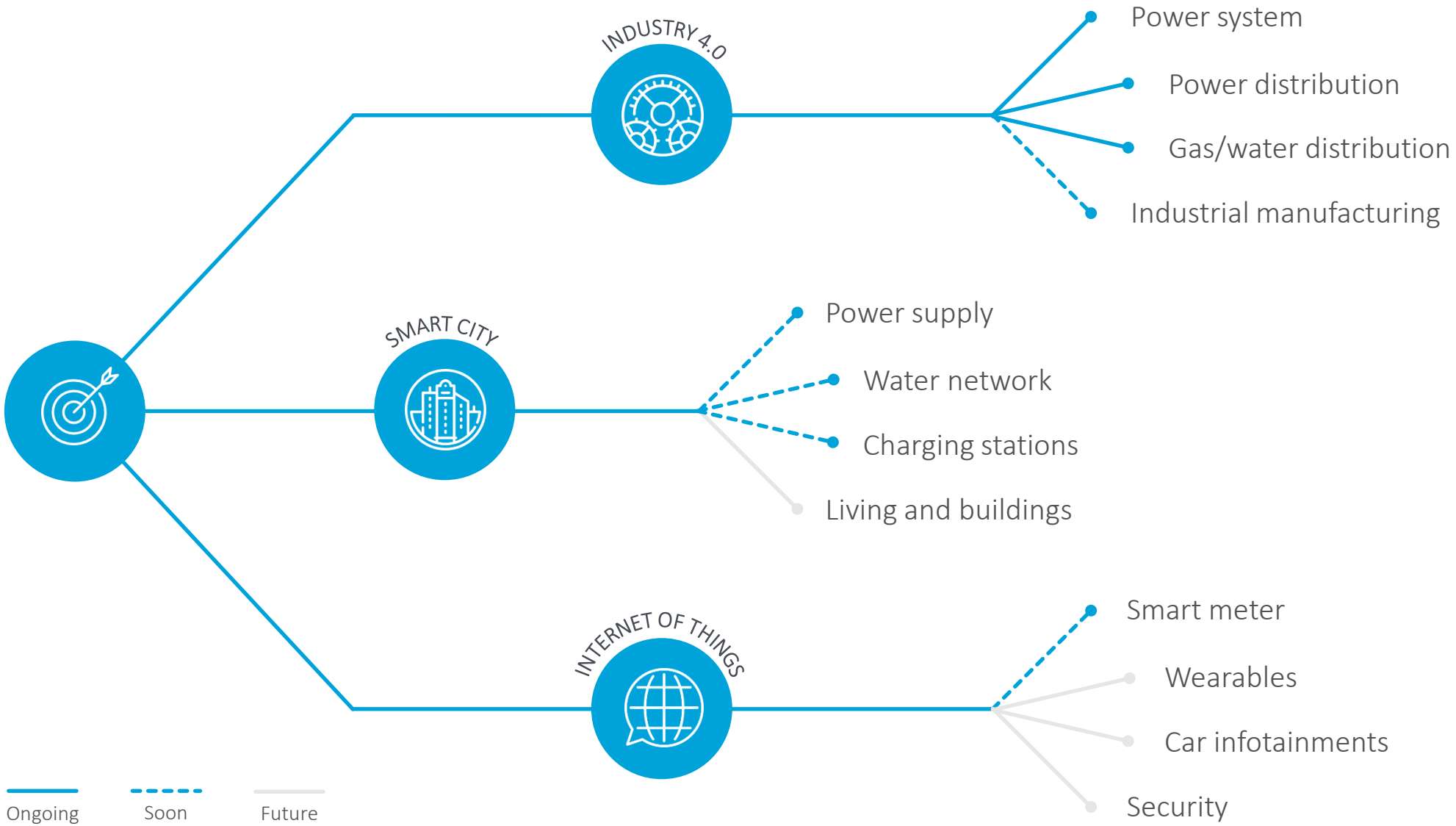
- Possibility to define specific Area Of responsibility (AOR) according to internal company policies.

2

- Possibility to define one or more roles according to IEC 62351-8:
  - Standard role nomenclature;
  - Definition of specific roles for the company.

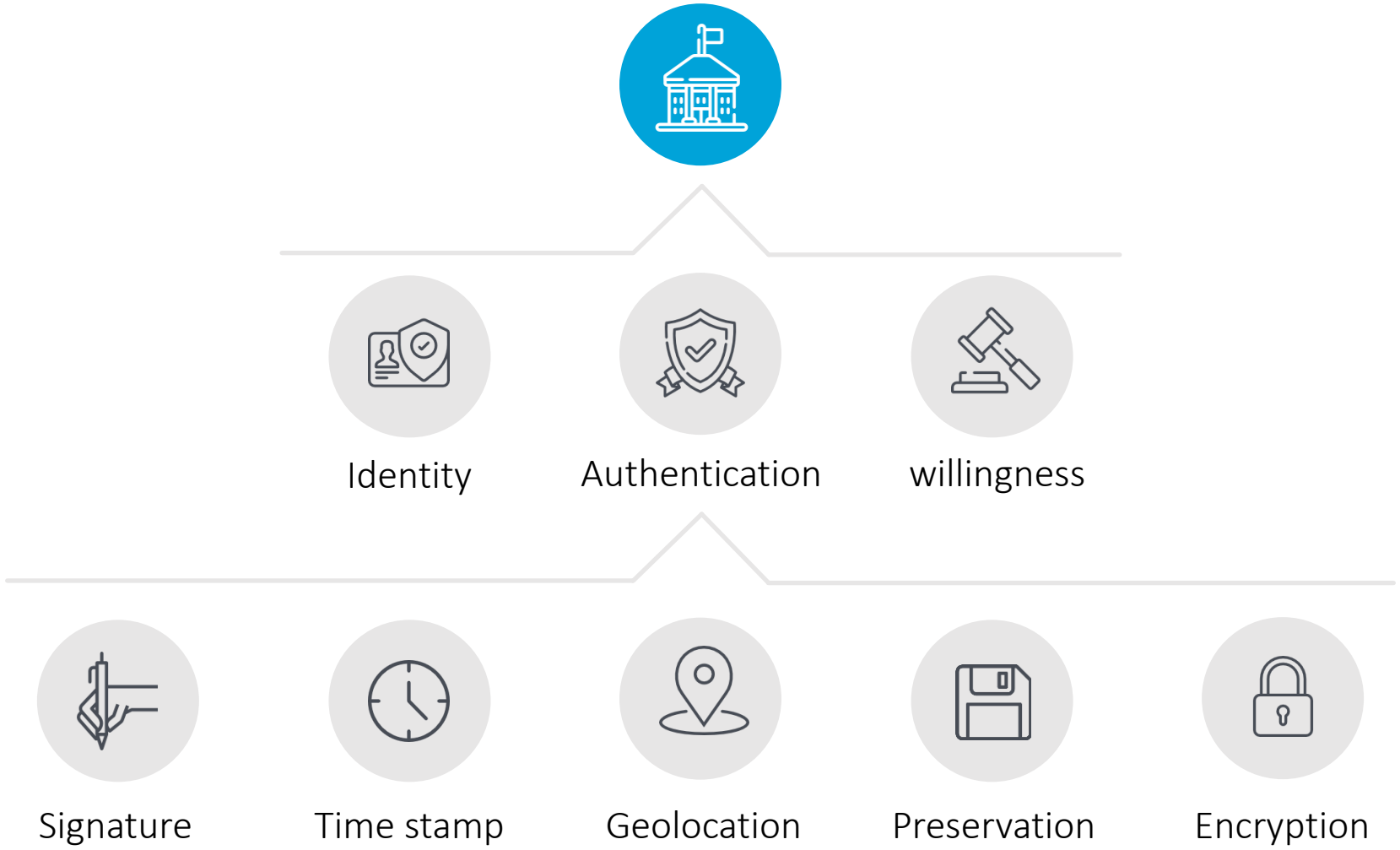
# POTENTIAL USE CASES

## FOCUS ON INDUSTRY 4.0, SMART CITY AND IOT INITIATIVES



# TRUSTED THIRD PARTY

## THE ROLE




InfoCert