InfoCert

TECNOINVESTIMENTI GROUP

MIDPKI

MACHINE IDENTITY
PUBLIC KEY INFRASTRUCTURE

InfoCert solution for a
secure IoT system

Highlights

1 Introduction to IoT

2 InfoCert MID PKI for trusted IoT

3 Innovations and benefits

Introducing IoT

> *“Since many of the benefits from the Internet of Things will occur on the basis of widespread adoption, sharing data across the value chain and novel services and developing global standards are pivotal to ensure effectiveness, interoperability and economies of scale. Coordination on Standardization is crucial for the Internet of Things, where market up-take is hampered by the fact that many devices do not speak the same language and cannot exchange data* (in a secure way) *across different gateways and smart hubs.”*

Internet of Things Standardisation and Architectures Workshop Report

The alignment with (vertical) business stakeholders

Semantic interoperability to ensure the modularity and scalability of the solutions

Built-in security and privacy features

Definition of relevant success metrics: technical and pre-commercial

European Commission and AIOTI are driving the convergence of IoT standards

MDI PKI executive summary

Internet of Things (IoT) continues to connect objects and relay information to people, so that new possibilities for business and personal life arise.

In light of the reams of sensitive data that the IoT generates, the **need for security** has never been greater

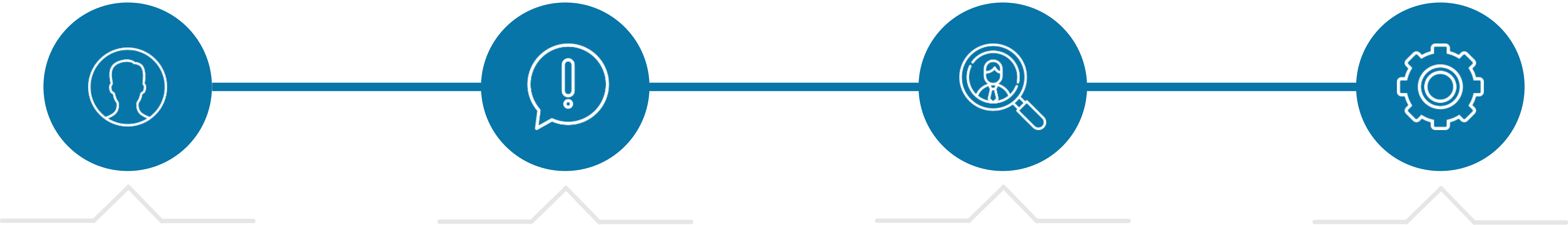
Trust in IoT is much more critical than in traditional digital transactions

Trust between objects is fundamental for ensuring:

- Identity Proof
- Privacy
- A clear Liability Framework

The need of trust

Considering the high level of automation and the **huge amount of data** coming from the most varied smart devices, IoT, Industry 4.0 or Smart City; environments need to be secured with a Trust Layer able to compensate the **lack of trust** that, nowadays, makes consumers, business, public authorities and citizens hesitate to carry out transaction electronically and to adopt new smart services



IDENTIFICATION

The smart device is identified by a trusted third party

IDENTITY CLAIM

The smart device tries to access the system

VERIFICATION

The identity of the device is verified prior the access to the system

ACTIONS

The device can operate on/in the system

TRUST THROUGHT IDENTITY

The operativity of a smart device on/in IoT, Industry 4.0 and Smart City environments should be allowed only after the verification in a **trusted** way of its **identity**. The **identity verification** should be performed by a **trusted third party** able to guarantee that the device pretending to have a specific identity is actually the device which owns such identity and that, based on this, it's enabled to have specific behaviors or to perform specific actions

InfoCert MID PKI for trusted IoT

InfoCert is the leading Qualified Trust Service Provider (QTSP) in Europe and the most qualified actor to manage all the risks connected to the current automated environments in which huge amount of data are generated and exchanged

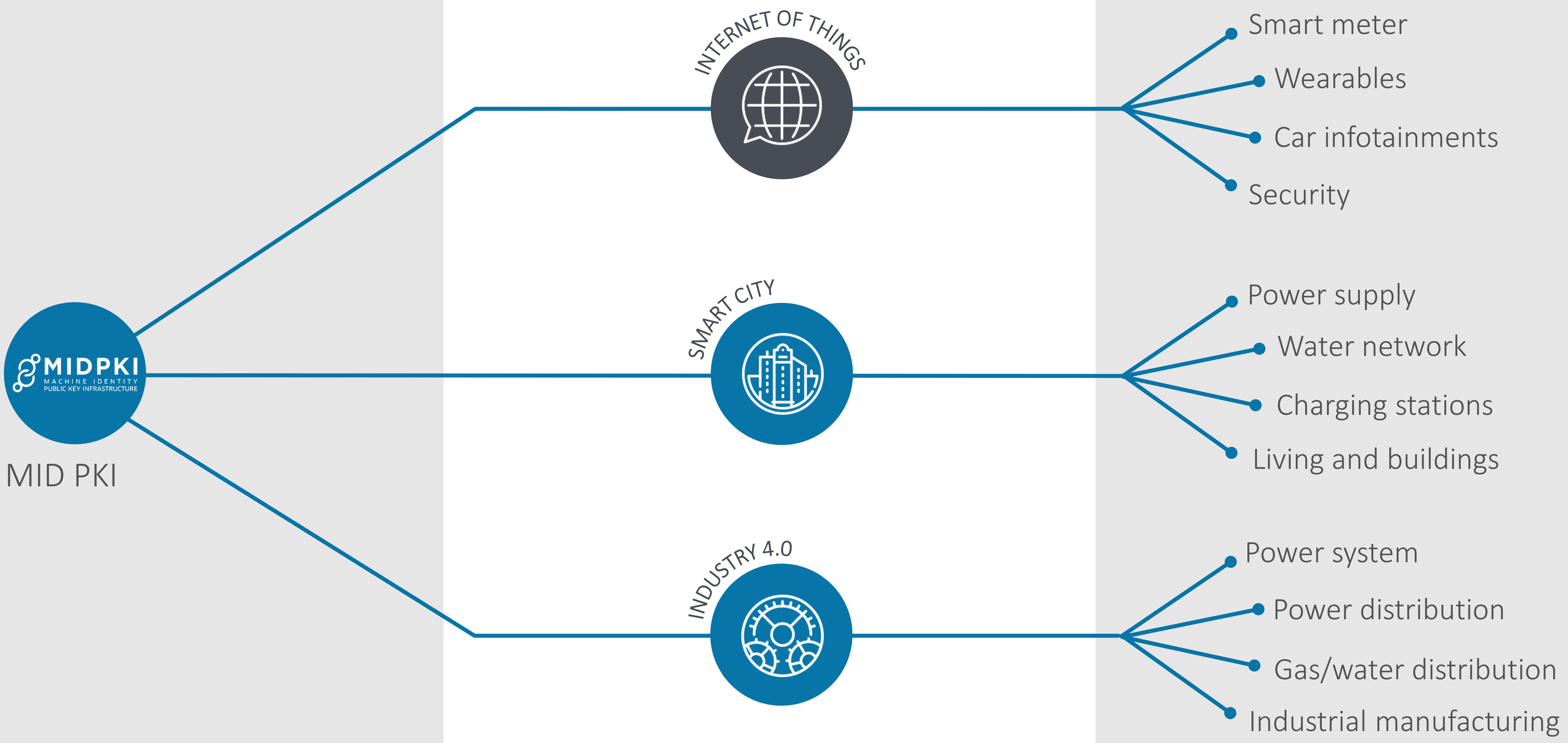
InfoCert has recently developed a “Cyber security key management Trust Layer” according to **IEC 62351-9** standard that will dramatically increase the security in IoT communication among power system equipment

Such Trust Layer could be deployed across the **entire IoT world** and could be easily enhanced to be deployed in many sectors

Such trusted IoT system enables real time control of all the logistics and predictive maintenance to promptly intercept and resolve potential malfunctions. This technology is named “Machine Identity PKI” (**MID PKI**).

The potentials of InfoCert MID PKI

SOLUTION | APPLICATION ENVIRONMENT | USE CASES



MIDPKI MACHINE IDENTITY PUBLIC KEY INFRASTRUCTURE

MID PKI

INTERNET OF THINGS
- Smart meter
- Wearables
- Car infotainments
- Security

SMART CITY
- Power supply
- Water network
- Charging stations
- Living and buildings

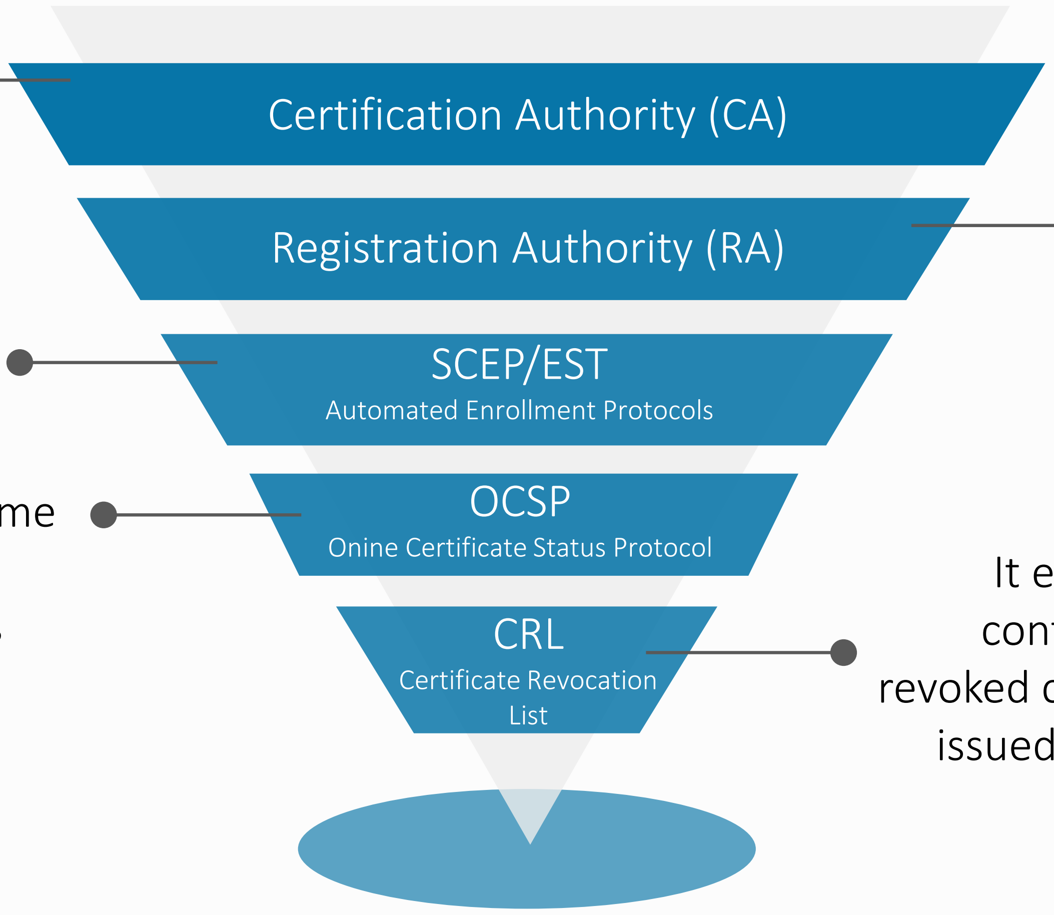
INDUSTRY 4.0
- Power system
- Power distribution
- Gas/water distribution
- Industrial manufacturing

The architecture of MID PKI solution

InfoCert MID PKI for trusted IoT environments could be ON PREMISES and CLOUD BASED

Certificates are issued for both machines/devices and for the personnel who interact with them

It issues different kinds of electronic certificates based on different trust levels



Certification Authority (CA)

Registration Authority (RA)

SCEP/EST

Automated Enrollment Protocols

OCSP

Onine Certificate Status Protocol

CRL

Certificate Revocation List

It records and verifies information used by the CA

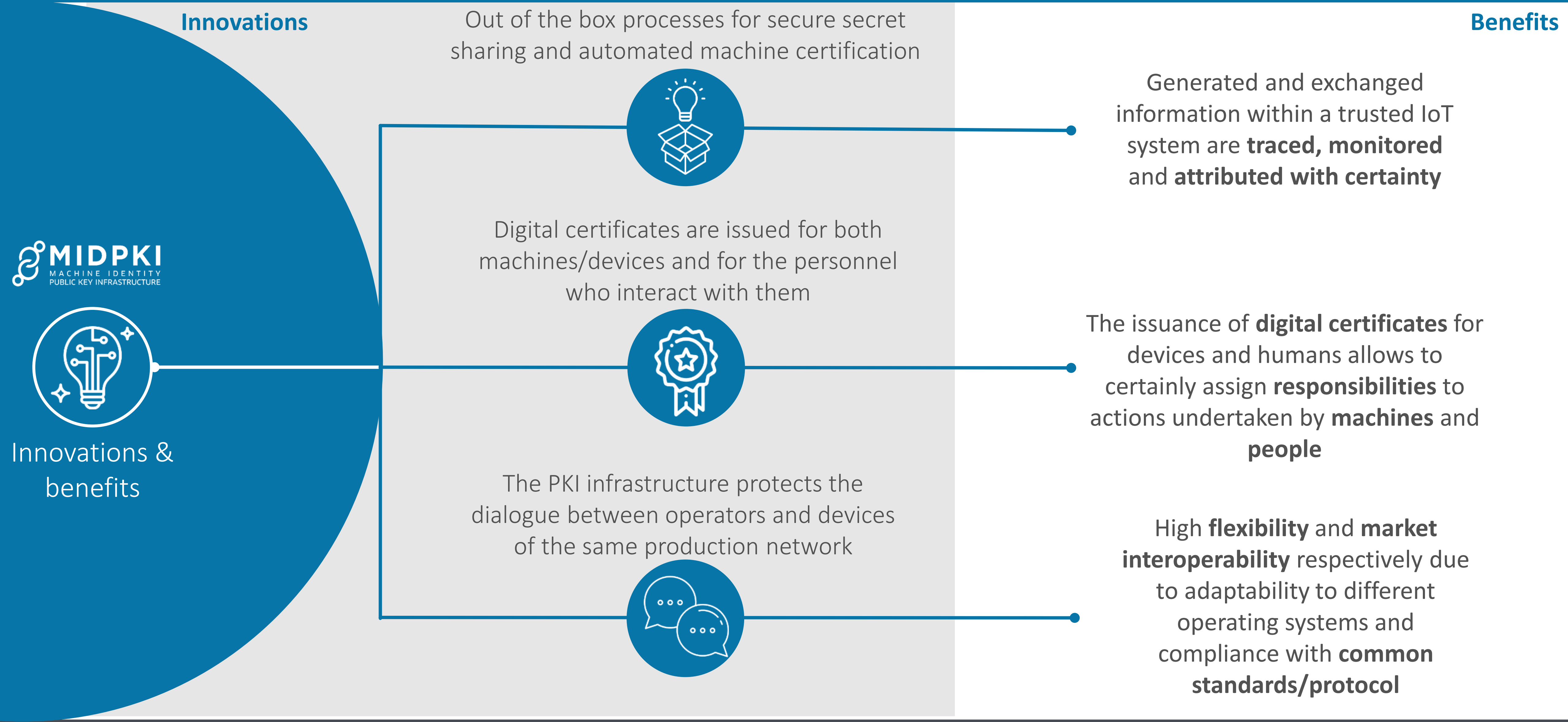
Enables automatic machine identity self-enrollment

It ensures real time checking of certificate status

It ensures full control on the revoked certificates issued by the CA

Technological and organizational structure

Main innovations & benefits



Innovations & benefits

Innovations

Out of the box processes for secure secret sharing and automated machine certification

Digital certificates are issued for both machines/devices and for the personnel who interact with them

The PKI infrastructure protects the dialogue between operators and devices of the same production network

Benefits

Generated and exchanged information within a trusted IoT system are **traced, monitored** and **attributed with certainty**

The issuance of **digital certificates** for devices and humans allows to certainly assign **responsibilities** to actions undertaken by **machines** and **people**

High **flexibility** and **market interoperability** respectively due to adaptability to different operating systems and compliance with **common standards/protocol**

InfoCert

TECNOINVESTIMENTI GROUP

Grazie.

www.infocert.it