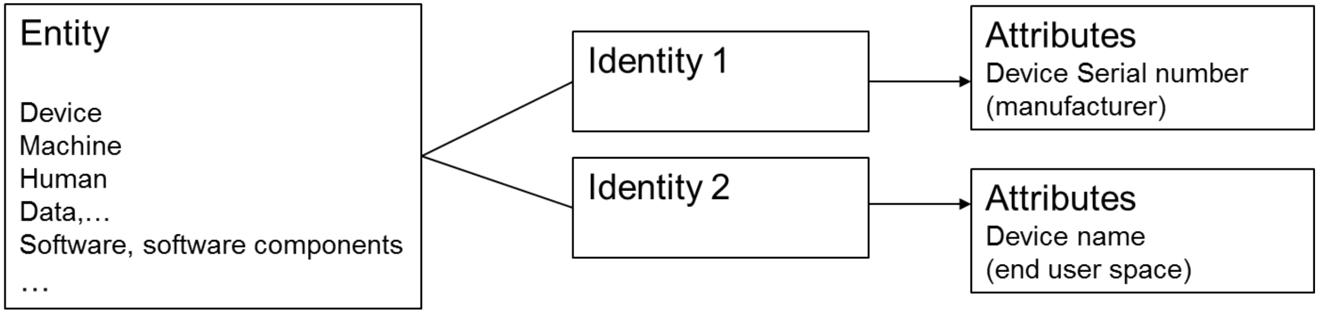
Session 3 - Secure Identities

Securing Global Industrial Value Networks– Berlin May 14th & 15th

Jean-Michel Brun - Chief Security Architect & IoT Security Leader
Schneider Electric

Identity definition and life cycle



Entity

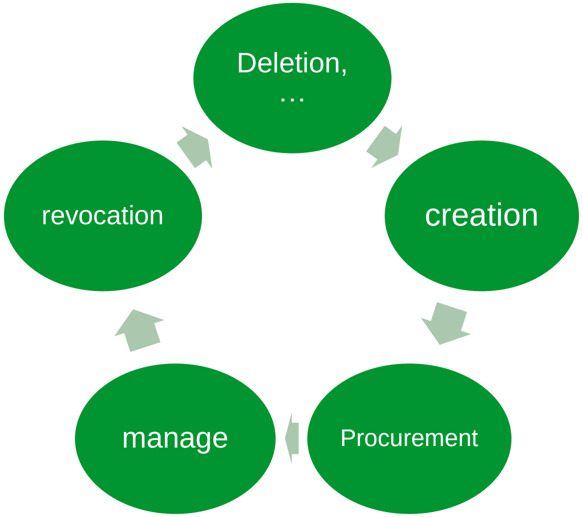
Device
Machine
Human
Data,…
Software, software components
…

Identity 1

Identity 2

Attributes
Device Serial number
(manufacturer)

Attributes
Device name
(end user space)



Deletion,
…

creation

Procurement

manage

revocation

Policies

Governance

Why ?

- Goal: enables the right entity to access the right resources at the right times and for the right reasons
- Associated security features
    - Authentication
    - Authorization
        - RBAC : Role Based Access Control
    - Audit & traceability

- We need secure identity to allow
    - (secure) Interaction & communication in the ecosystem
    - More “isolation” by fine-grain access to resources
    - Log and monitor
    - non repudiation
    - Accurate list of installed product,..

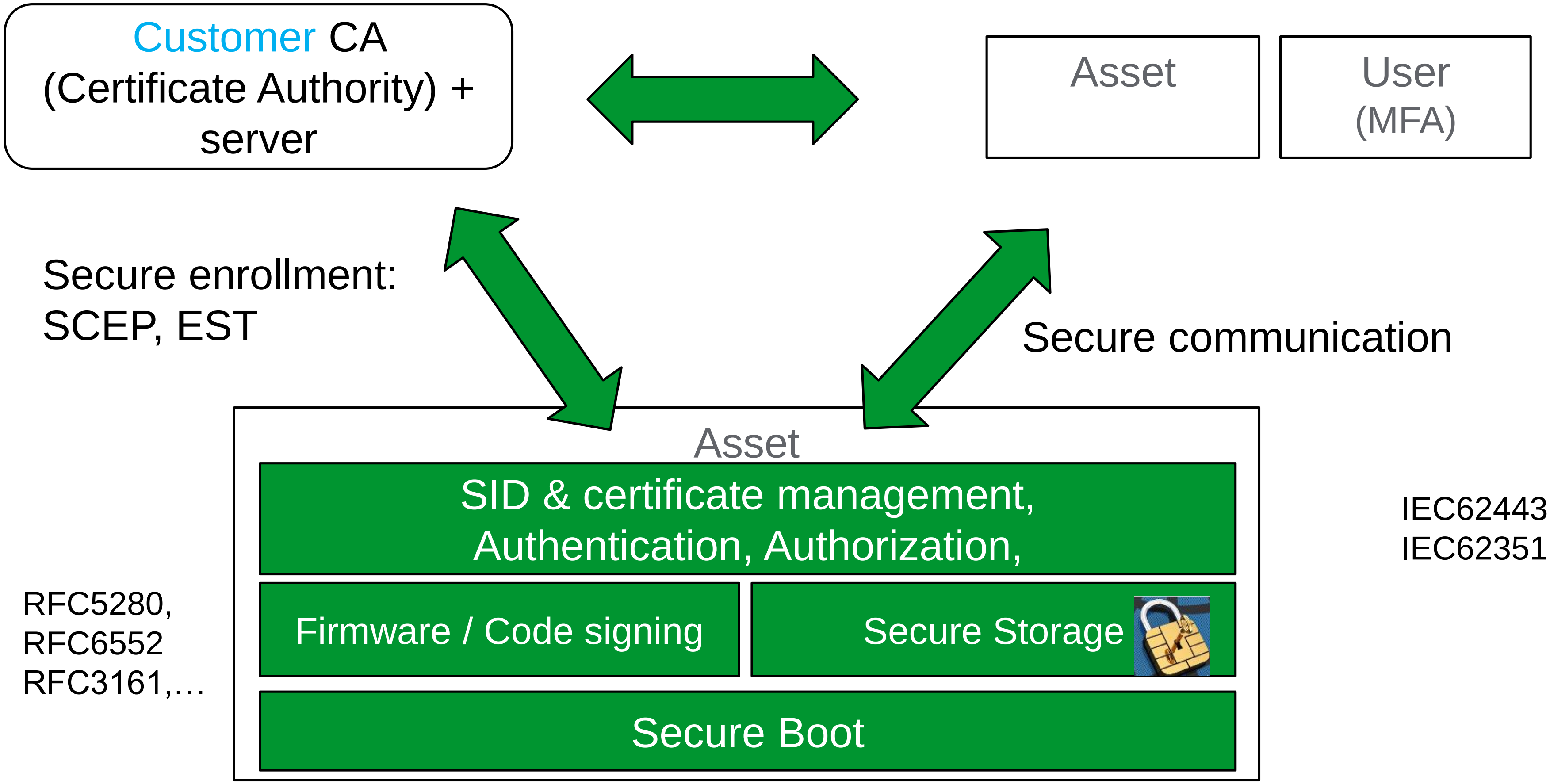
- It’s the baseline for the security chain

Secure Identity vs Threats

- Unique ID -> Secure ID
  - Avoid ambiguity
  - Protection against spoofing
  - Baseline against Information disclosure, Denial of service (context of IOT !!), repudiation,
  - Protect against counterfeiting (Device Genuineness)

- How to Secure
  - Can rely on hardware to protect the key (trust anchor)
    - Smart card → user
    - TPM → software (PC)
    - secure element -> Embedded device
  - Necessary to address high level of IEC62443 (L3 & L4)

Secure Identity at device & system level: example



Customer CA (Certificate Authority) + server

Asset

User (MFA)

Secure enrollment: SCEP, EST

Secure communication

Asset

SID & certificate management, Authentication, Authorization,

Firmware / Code signing

Secure Storage

Secure Boot

RFC5280,
RFC6552
RFC3161,…

IEC62443
IEC62351

Challenges of PKI

- Lifetime/ Expiration
- renewal of certificate / renewal in case of product replacement (IIOT)
- Revocation of certificate:
  - CRL, OCSP
- “Cross reference” between different PKI (several stakeholders)
- Trustworthiness of the CA
  - Require strong policies but very difficult to address the national requirement

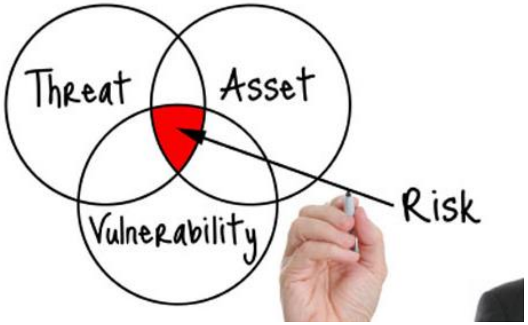
Trust Center (use case of Industry 4.0)

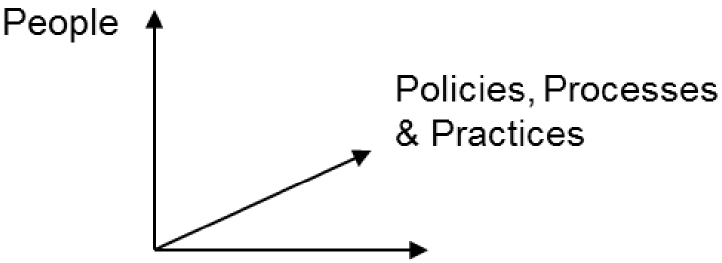
- To go further (interaction between companies)
  - Policies and governance are mandatory
  - Trustworthy organization must be in place
  - Require to keep a security boundaries (at company level)

- Some thoughts
  - The trust Center will be the 1st to be attacked
  - Require a strong SLA for the trust center operation

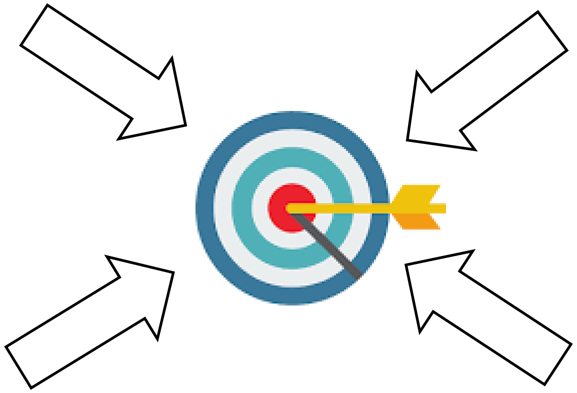
  - (PKI) Difficulties to manage the lifetime of the different certificates (incl the root)
  - What about a federation approach ?

Cyber security & Trust





Architecture, Technology
& Infrastructure



Conformance & Certification

- National Assessment
- Third Party Assessment
- Self-Assessment

Standards & regulations

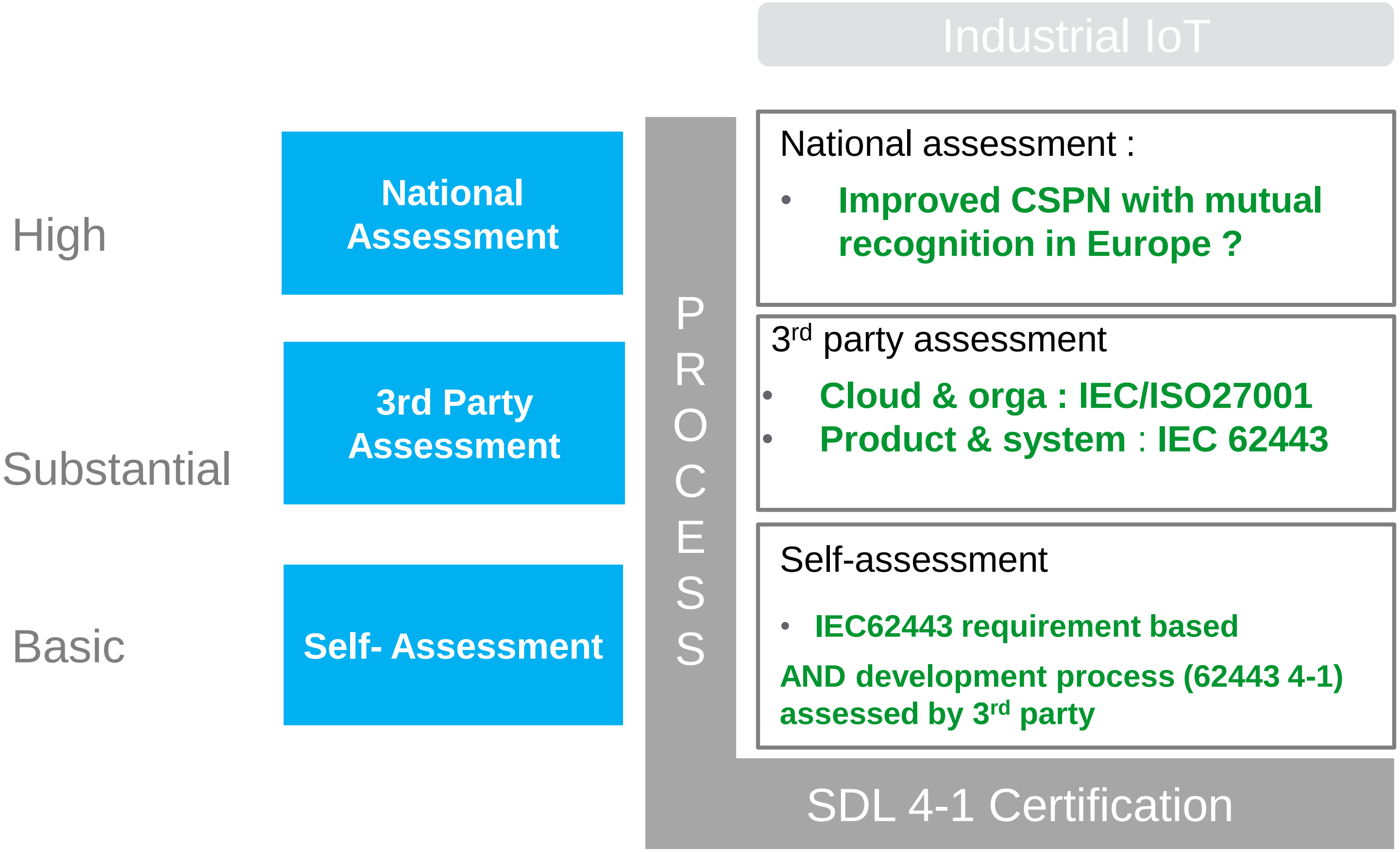
IEC

ISO

GDPR

…

EU Cyber Act scheme : proposal



Industrial IoT

High

National Assessment

Substantial

3rd Party Assessment

Basic

Self- Assessment

PROCESS

National assessment :

- **Improved CSPN with mutual recognition in Europe ?**

3rd party assessment

- **Cloud & orga : IEC/ISO27001**
- **Product & system : IEC 62443**

Self-assessment

- **IEC62443 requirement based**

AND development process (62443 4-1) assessed by 3rd party

SDL 4-1 Certification