Keyfactor
Tech Days
2023

Supply Chain Security for IoT

Laurent MASSON

Chief Technical Officer

Trusted Objects

Agenda

IoT devices manufacturing process:

- What vulnerabilities, threats and risks?
- How to secure each step of manufacturing?
- matter use case:
  secure provisioning of a generic MCU

MCU

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

Vulnerabilities and Risks

IoT device manufacturing process

Vulnerabilities, threats and risks

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

SecurityHQ | IBM

IBM X-Force Threat Intelligence Index 2022

→ Download Report

*“The **manufacturing** industry **became** the **top target** of **cyber attackers** in 2021 according to IBM’s 2022 Threat Intelligence Index”.*

Top cause of data loss for manufacturers: Malware

23% of the most serious incidents*

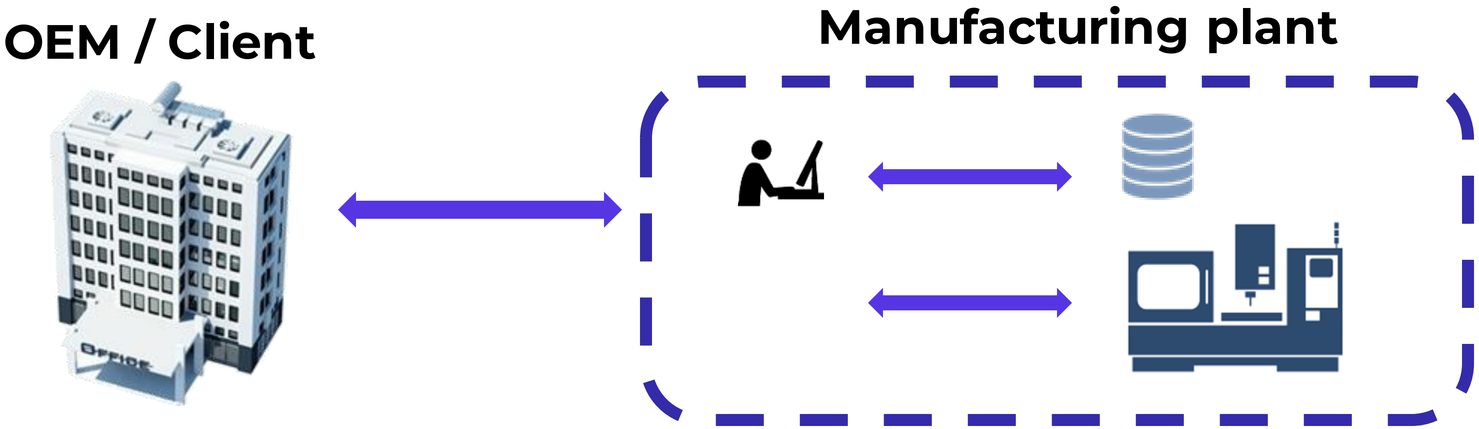
** Kaspersky Lab survey*

Why cyber attacks at the manufacturing stage?

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

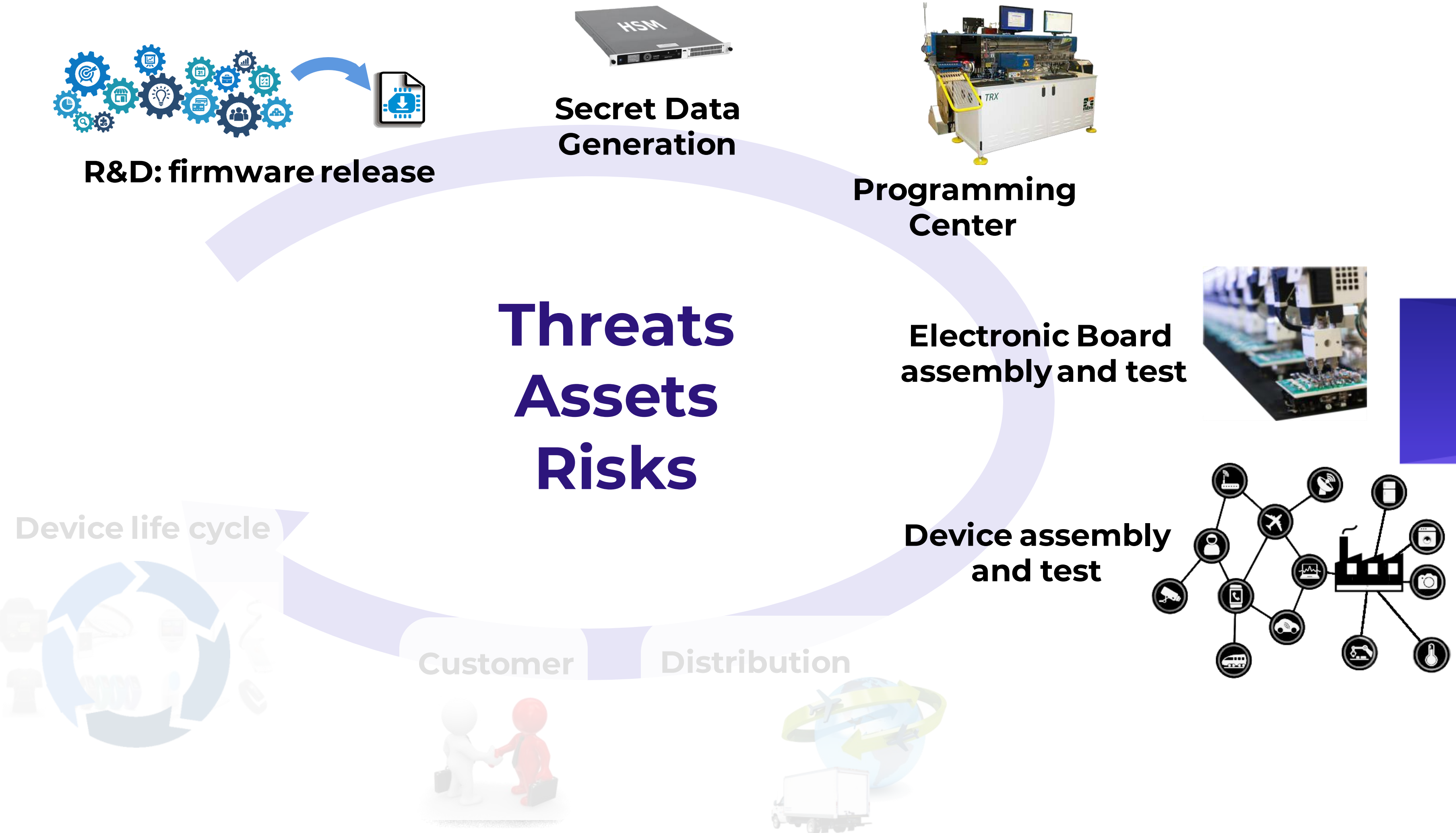
- **Manufacturing** organizations **store confidential** information **of their clients**
- **OEM assets/IPs** can be exploited for **reverse-engineering** and **sold to competitors**
- OEM products can be **cloned** (overproduction)
- Attacker targeting OEM device **safety** or **misuse**



Firmware and Secret data journey

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case



R&D: firmware release

Secret Data Generation

Programming Center

Electronic Board assembly and test

Device assembly and test

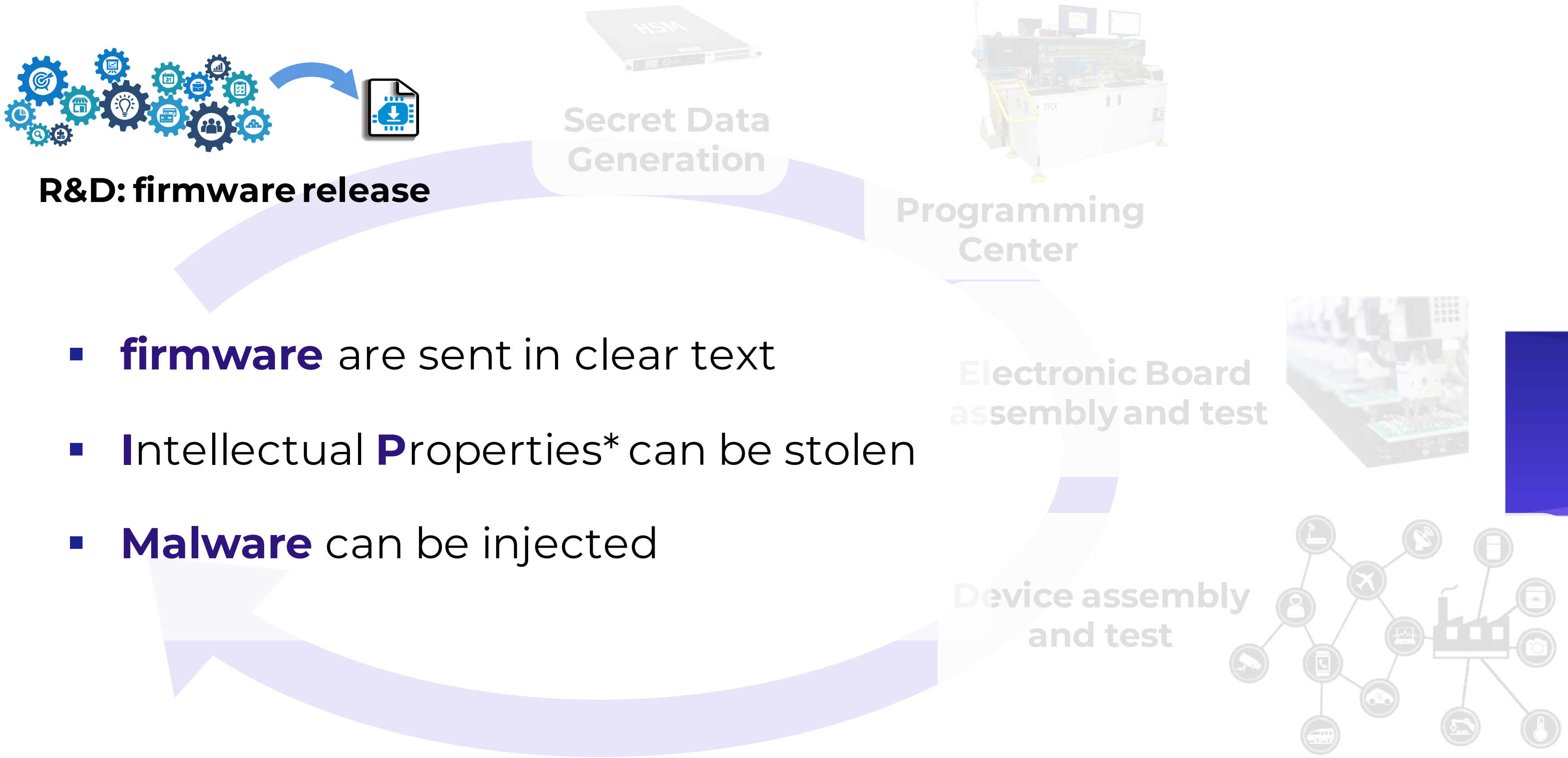
Distribution

Customer

Device life cycle

Threats
Assets
Risks

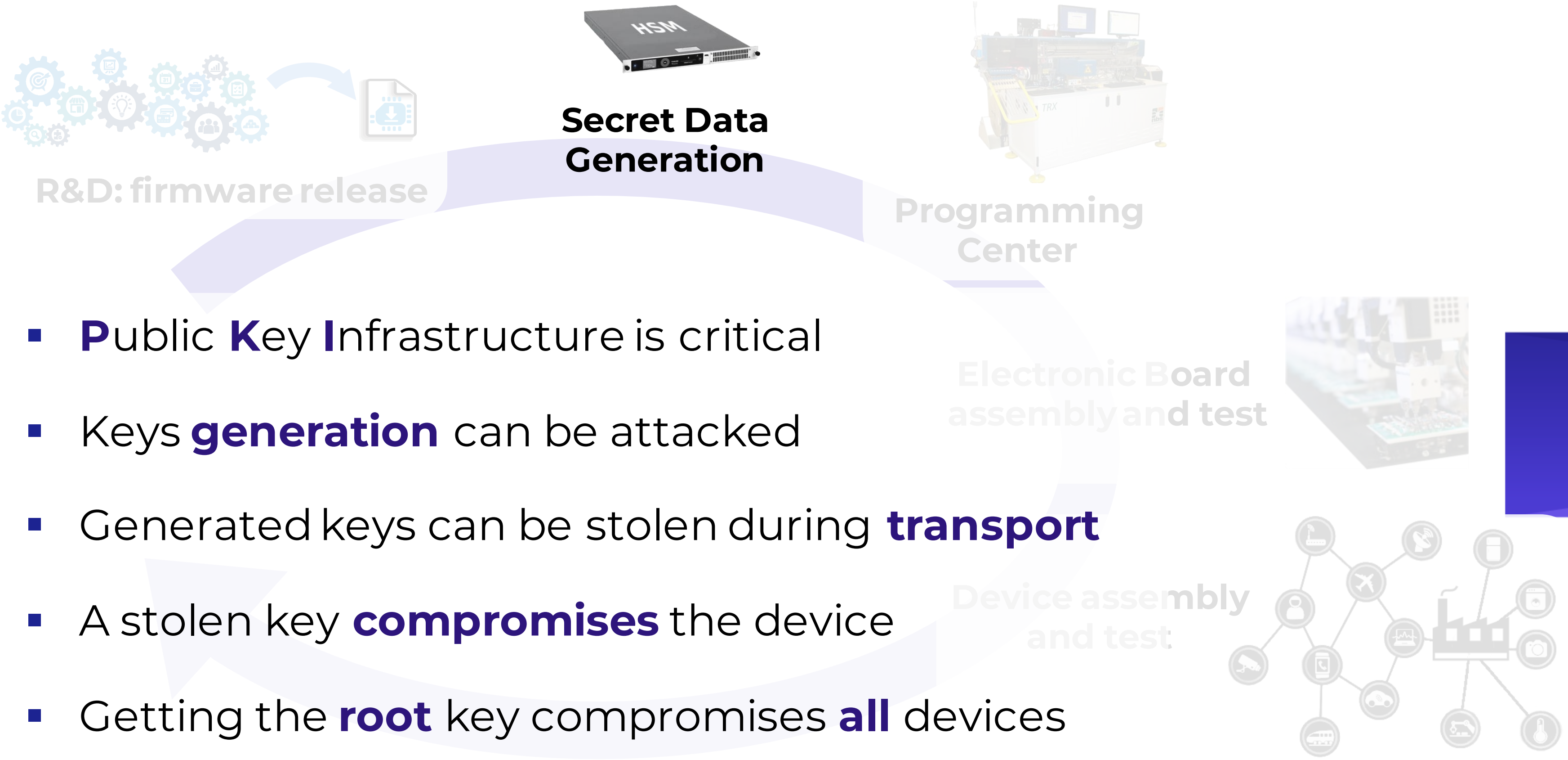
Firmware and Secret data journey



- **firmware** are sent in clear text
- **I**ntellectual **P**roperties* can be stolen
- **Malware** can be injected

** OEM Intellectual property (IP): any information giving a company competitive advantage (software, firmware, keys, secret data…)*

Firmware and Secret data journey



- **P**ublic **K**ey **I**nfrastructure is critical
- Keys **generation** can be attacked
- Generated keys can be stolen during **transport**
- A stolen key **compromises** the device
- Getting the **root** key compromises **all** devices

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

Firmware and Secret data journey

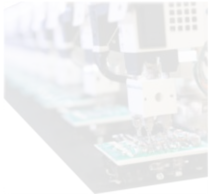
Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

R&D: firmware release

Secret Data Generation

Programming Center



Electronic Board assembly and test

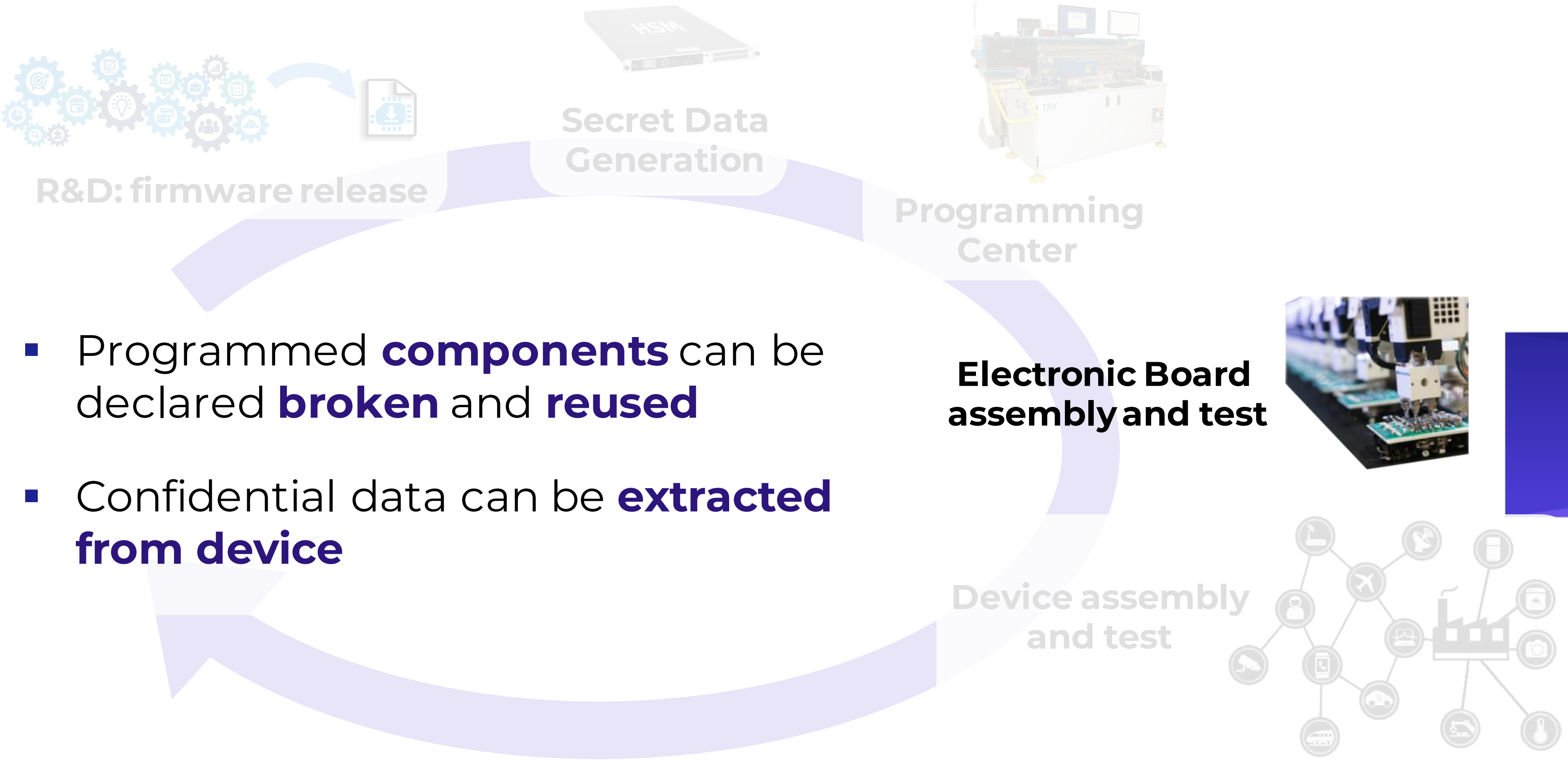
Device assembly and test

- **Confidential** data are **stored** on the manufacturer **computer**, and can be sent to **competitor** easily
- Can be **reused** for **overproduction** or **cloning**
- Confidential data can be **read** on **programming machine**

Firmware and Secret data journey

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

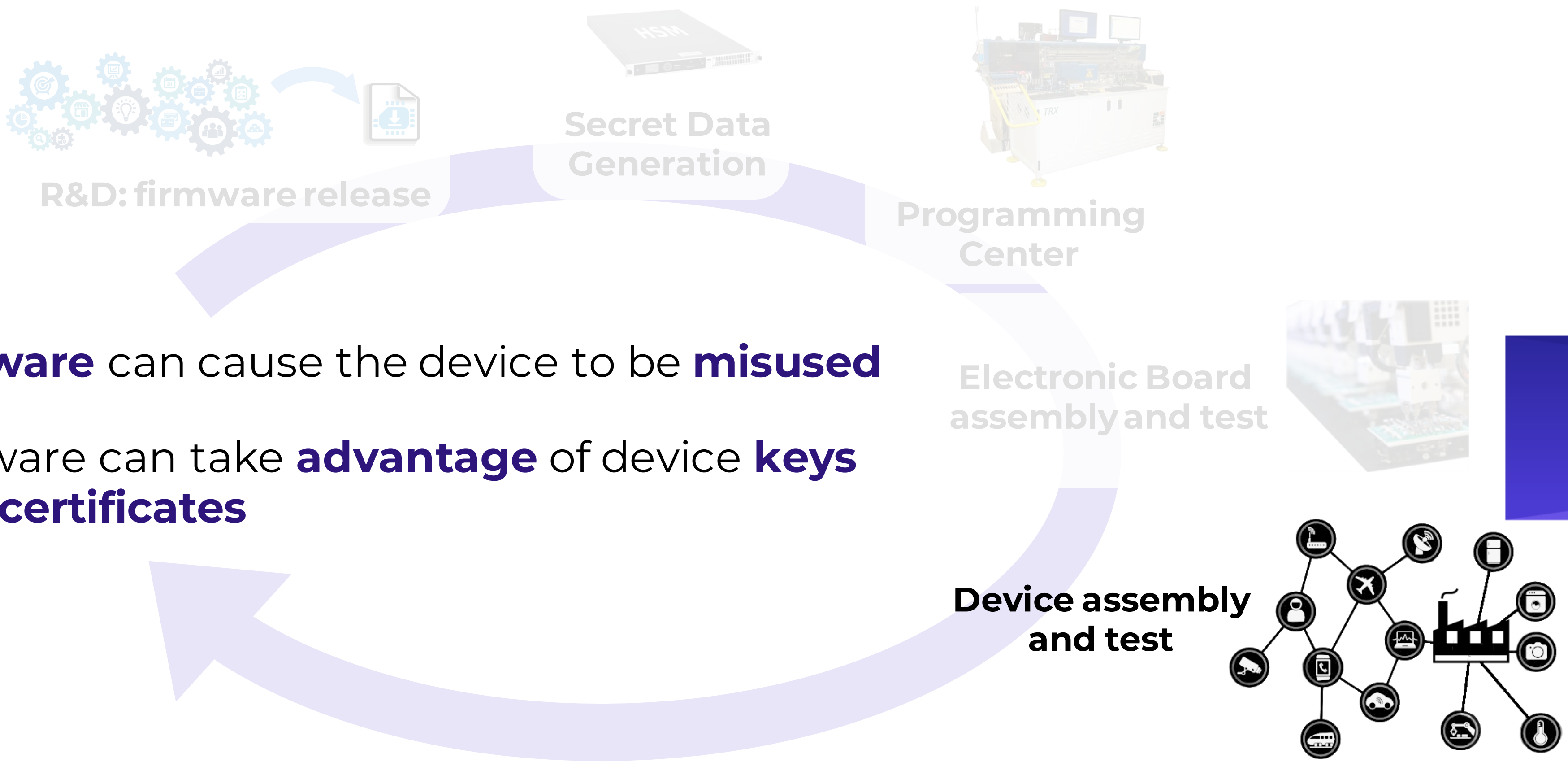


- Programmed **components** can be declared **broken** and **reused**
- Confidential data can be **extracted from device**

Firmware and Secret data journey

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case



- **Malware** can cause the device to be **misused**
- Malware can take **advantage** of device **keys** and **certificates**

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

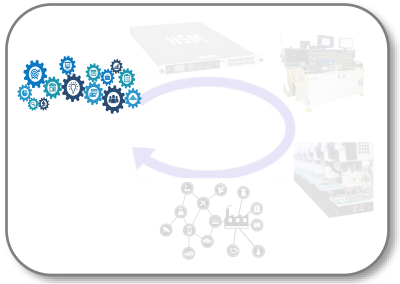
How to secure

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

How to secure manufacturing?

At firmware generation and transport stage



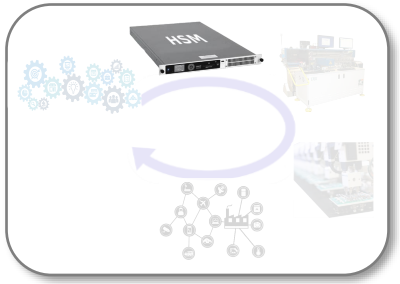
- **Firmware package must be encrypted**
  - Prevent Intellectual Property theft
  - Prevent cloning
- **Firmware package must be signed**
  - Ensure integrity of the firmware
  - Prevent Malware injection

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

How to secure manufacturing?

At keys and certificates generation and transport stage



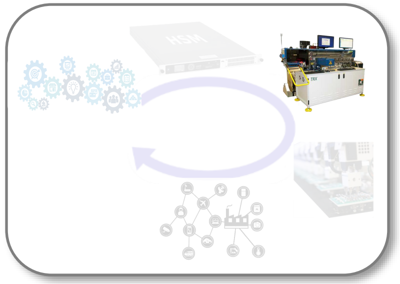
- **Secure the root CA**
  - Protect Root CA private key in HSM
  - Physically secure the location. Limit, control, monitor and audit access
  - Setup a strong and secure backup and Setup a disaster recovery plan
- **Define PKI tree carefully**
  - Use Root CA only to sign intermediate CA
  - Use dedicated Intermediate CA for each product type, batch, or location
- **Keys / certificates generation by HSM**
  - Ensure quality of the generated keys
  - Protect the root private keys (for Certificate Authority key)
- **Secret Keys must be encrypted (wrapped)**
  - Protect keys during transport
- **Keys must be diversified**
  - Only one device compromised if one key is compromised

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

How to secure manufacturing?

At Programming center



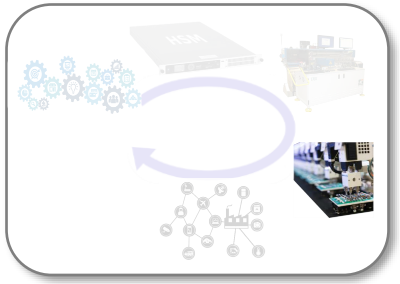
- **Use black-box at programming center**
  - No file stored by manufacturer
  - Secure transport of Firmware and IP from R&D to Blackbox
  - Full control of number of components programmed
- **Delegate keys generation to specialist**
  - State-of-the-art PKI management, with disaster recovery plan
  - Full control of number of keys generated

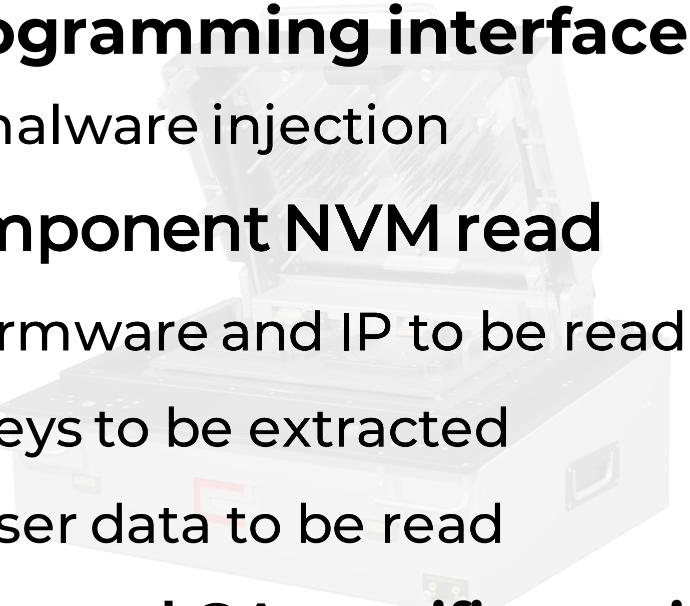
Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

How to secure manufacturing?

At Electronic Board assembly and test





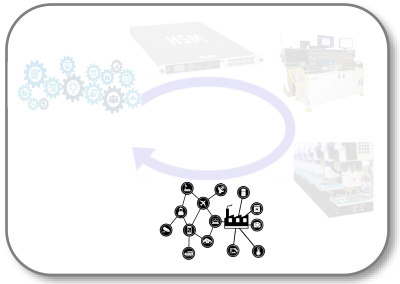
- **Disable programming interface**
  - Prevent malware injection
- **Disable component NVM read**
  - Prevent firmware and IP to be read-back
  - Prevent keys to be extracted
  - Prevent user data to be read
- **Protect keys and CA certificates in Secure Element**
  - Prevent keys to be extracted
  - Prevent CA certificate to be replaced by hacker

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

How to secure manufacturing?

At device assembly and test



- **Build a whitelist**
  - Only devices that succeeded test are in whitelist
  - Server filters devices on whitelist
  - Valid component declared “broken” can’t connect to cloud services
- **Sign firmware for secure boot**
  - Prevent any malware injection
  - Protect the firmware update mechanism
- **On the field activation**
  - Use on-the-field activation to prevent cloned devices

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

Use Case

matter

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

matter - Introduction

- **Industry-unifying standard to connect IoT devices**
  - Supported by **major actors** of IoT

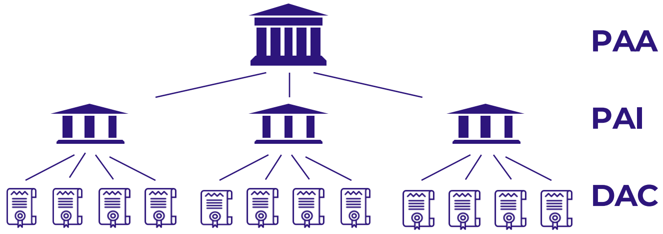
amazon
somfy
IKEA
HUAWEI
LG
Google
NORDIC SEMICONDUCTOR
SAMSUNG
infineon
life.augmented
tuya
legrand

  - Provides a **common** communication language for IoT devices
  - Reliable and **Secure**

matter requirements for devices

- **Integrate software**
  - Matter stack
  - Application Firmware

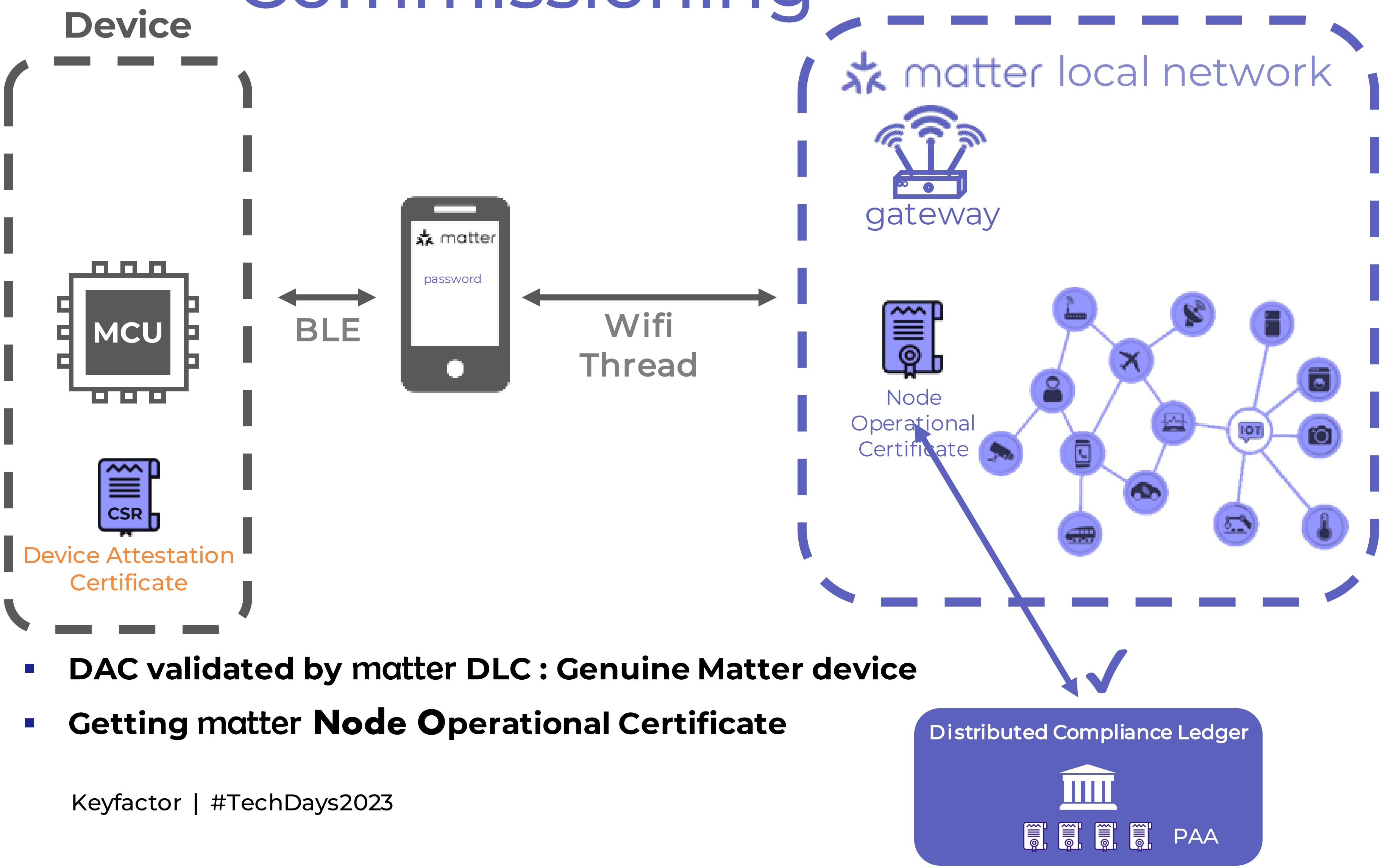
- **Define Matter IDs**
  - Define Vendor ID (VID)
  - Define Product ID (PID)



- **Define PKI**
  - Choose robust and reliable PKI infrastructure
  - Define your product CA (PAI)
  - Generate Device Attestation Certificate (DAC)
- **Inject certificates in the device**
  - Inject DAC and PAI certificates in the device's microcontroller
  - Protect the private key from reading, the CA key from writing

matter provisioned data usage

Commissioning


Device
MCU
CSR
Device Attestation Certificate
BLE
matter
password
Wifi
Thread
matter local network
gateway
Node Operational Certificate
IOT
✓
Distributed Compliance Ledger
PAA

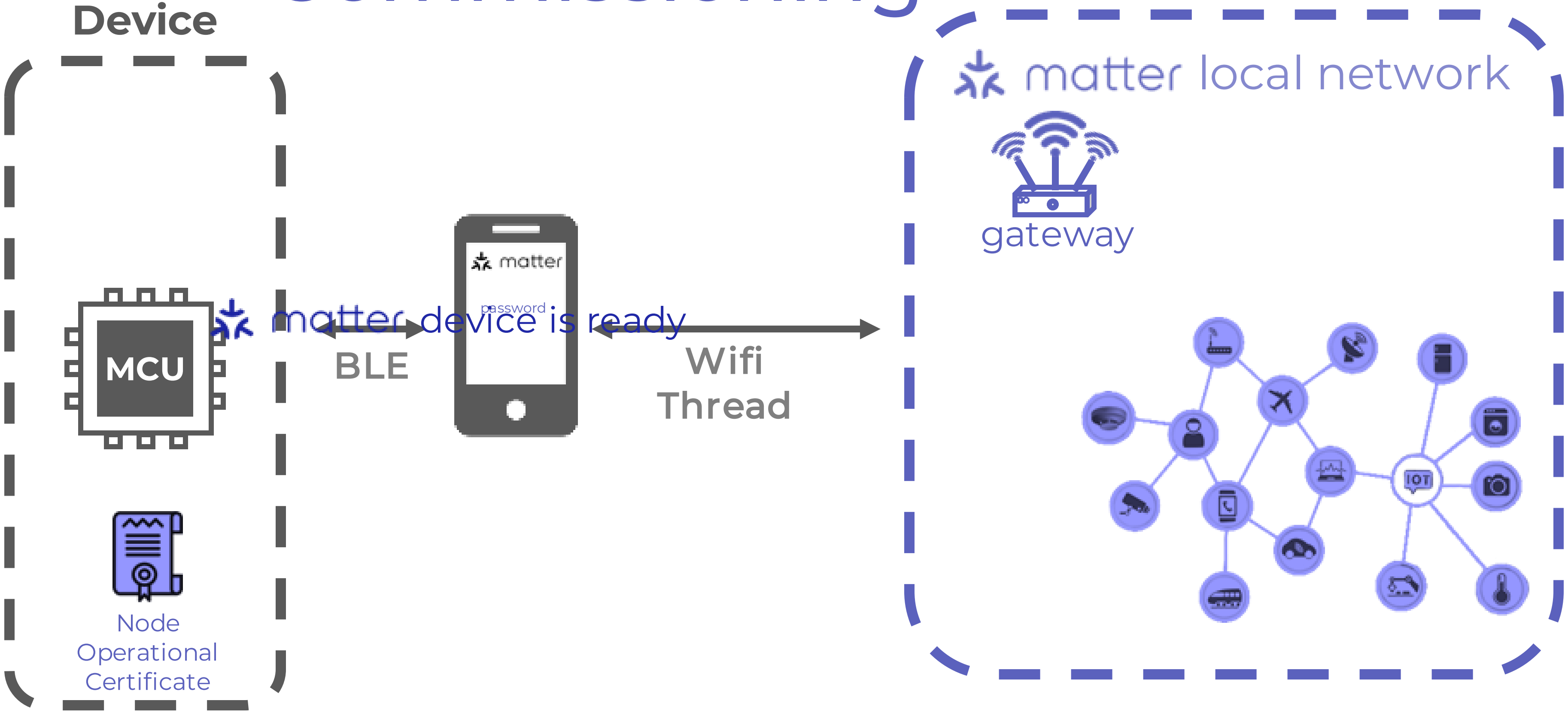
- **DAC validated by matter DLC : Genuine Matter device**
- **Getting matter Node Operational Certificate**

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

matter provisioned data usage

Commissioning



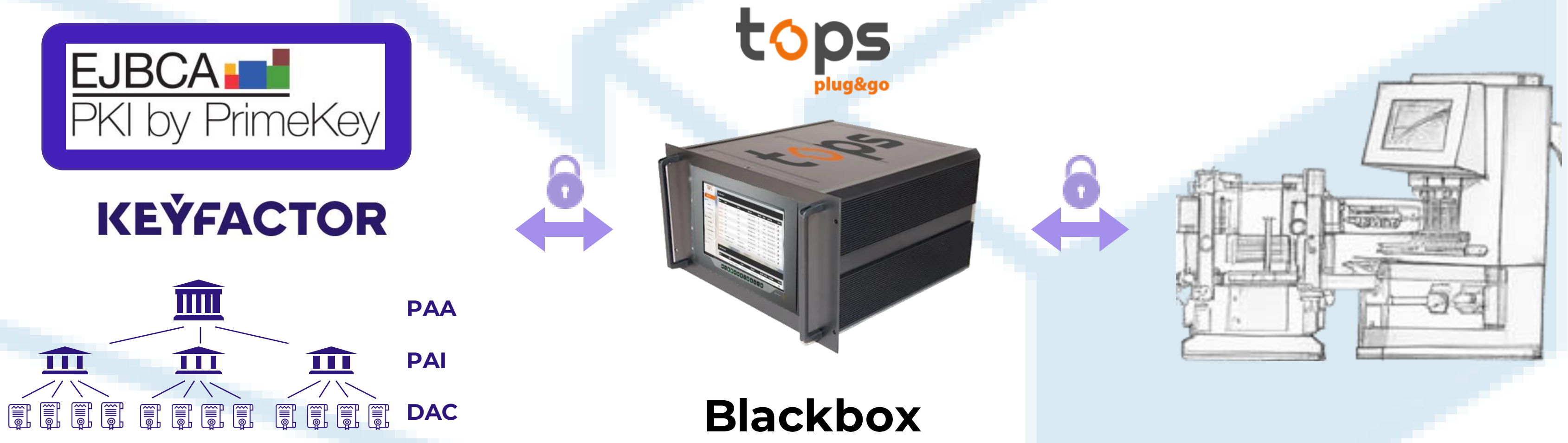
- **DAC validated by matter DLC : Genuine Matter device**
- **Getting matter Node Operational Certificate**

matter issues to solve

- **Generate Device Attestation Certificates**
  - How to use best in class technology and process
  - How to protect keys and certificates before programming
- **Inject keys and certificates in device**
  - How to protect keys and certificates during injection
  - How to protect keys and certificates in the device
- **Integrate application firmware and matter stack**
  - How to protect IPs
  - How to prevent from Malware injection

matter manufacturing solution

- **Keep production control in manufacturing center**
  - Install a blackbox in manufacturing center
- **Generate Certificates**
  - Use professional PKI system
  - Use the blackbox to control keys generation and transport to components

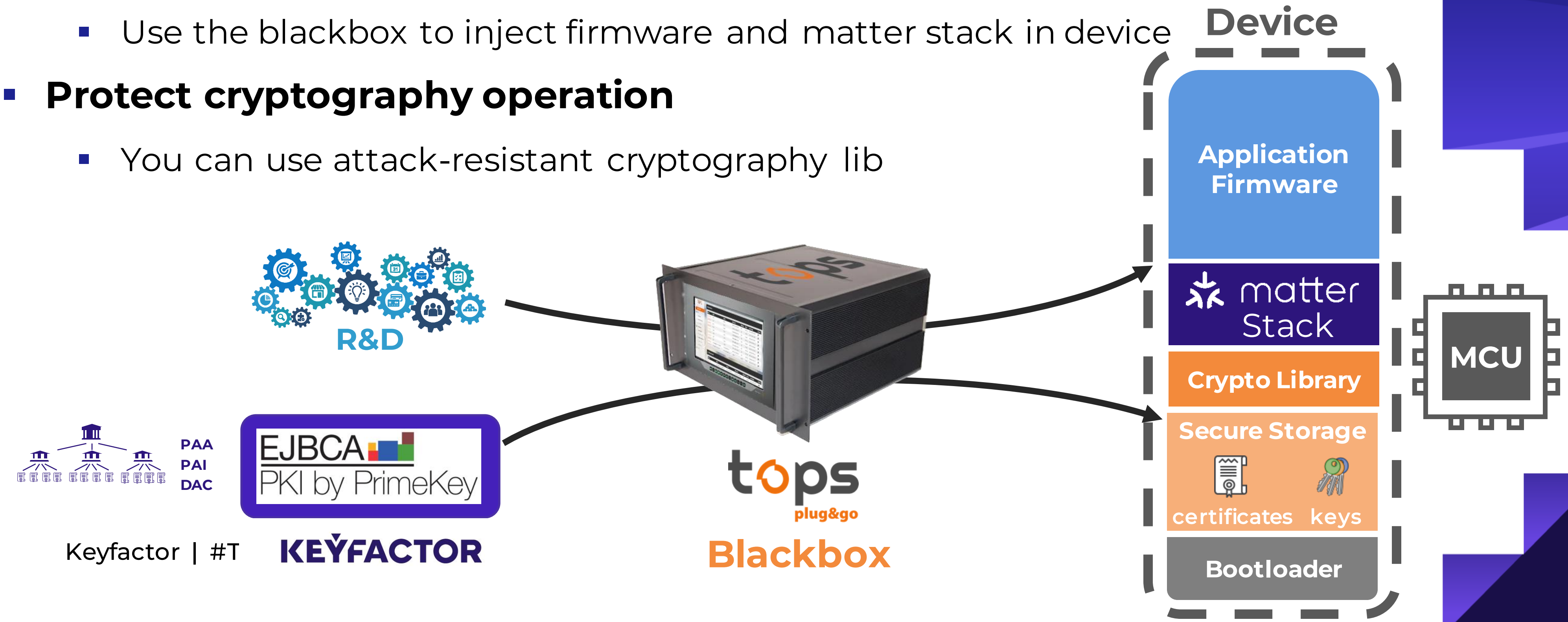


Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

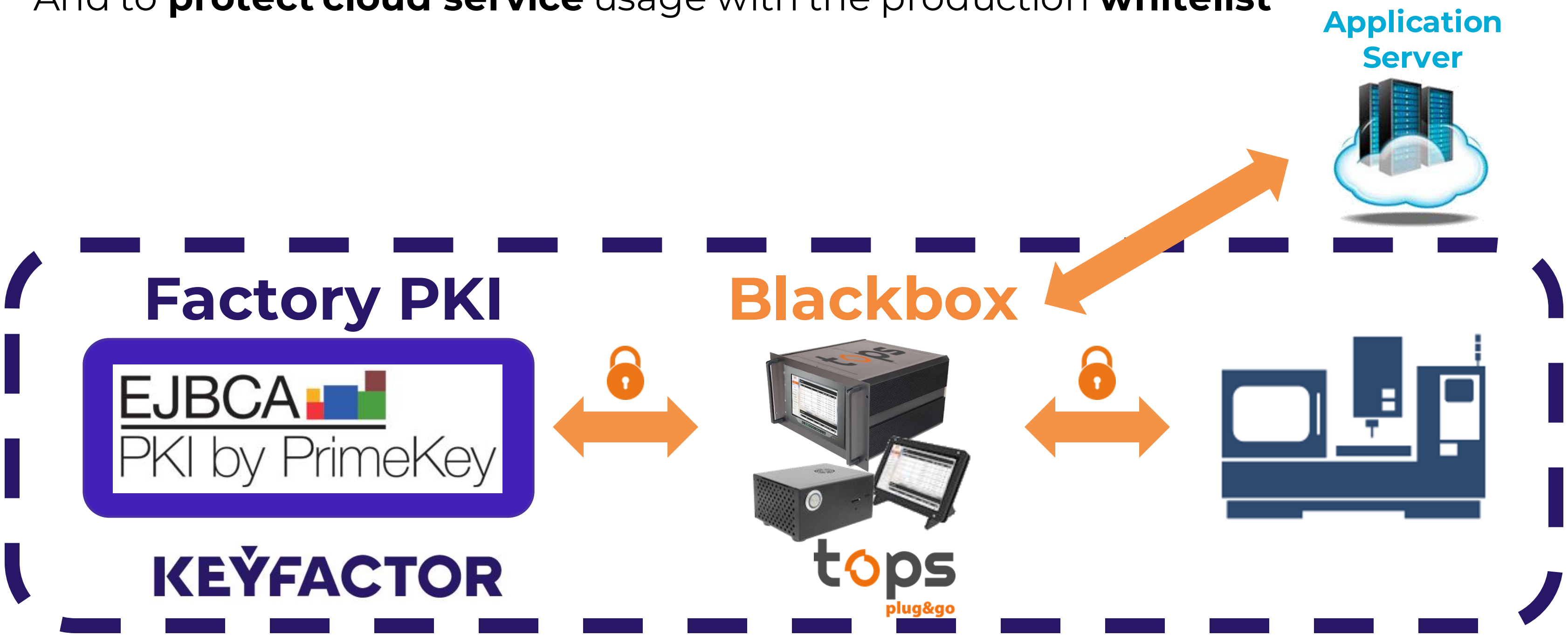
matter manufacturing solution

- **Inject keys and certificates in device**
  - Use blackbox to inject keys and certificate in the device
  - Use secure storage solution to store keys and certificates
- **Integrate application firmware and matter stack**
  - Send encrypt firmware and matter stack from R&D to blackbox
  - Use the blackbox to inject firmware and matter stack in device
- **Protect cryptography operation**
  - You can use attack-resistant cryptography lib



matter manufacturing solution

- Protect **firmware** and **I**ntellectual **P**roperties
- Protect **D**evice **A**ttestation **C**ertificate and private **keys**
- **Full control** of devices **production**
- And to **protect cloud service** usage with the production **whitelist**



Demo available

Q&A

Q&A

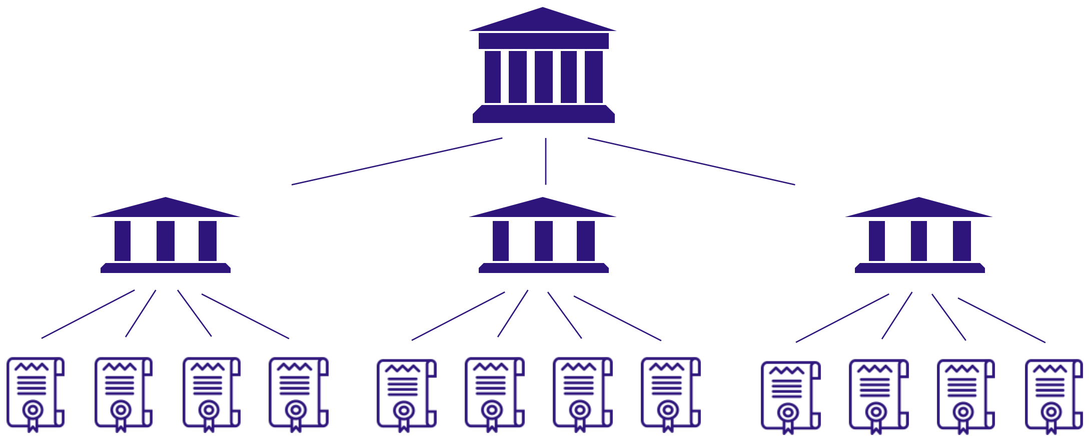
Backup

Agenda

- Vulnerabilities and Risks
- How to secure
- Use Case

matter devices manufacturing

- **Required PKI**

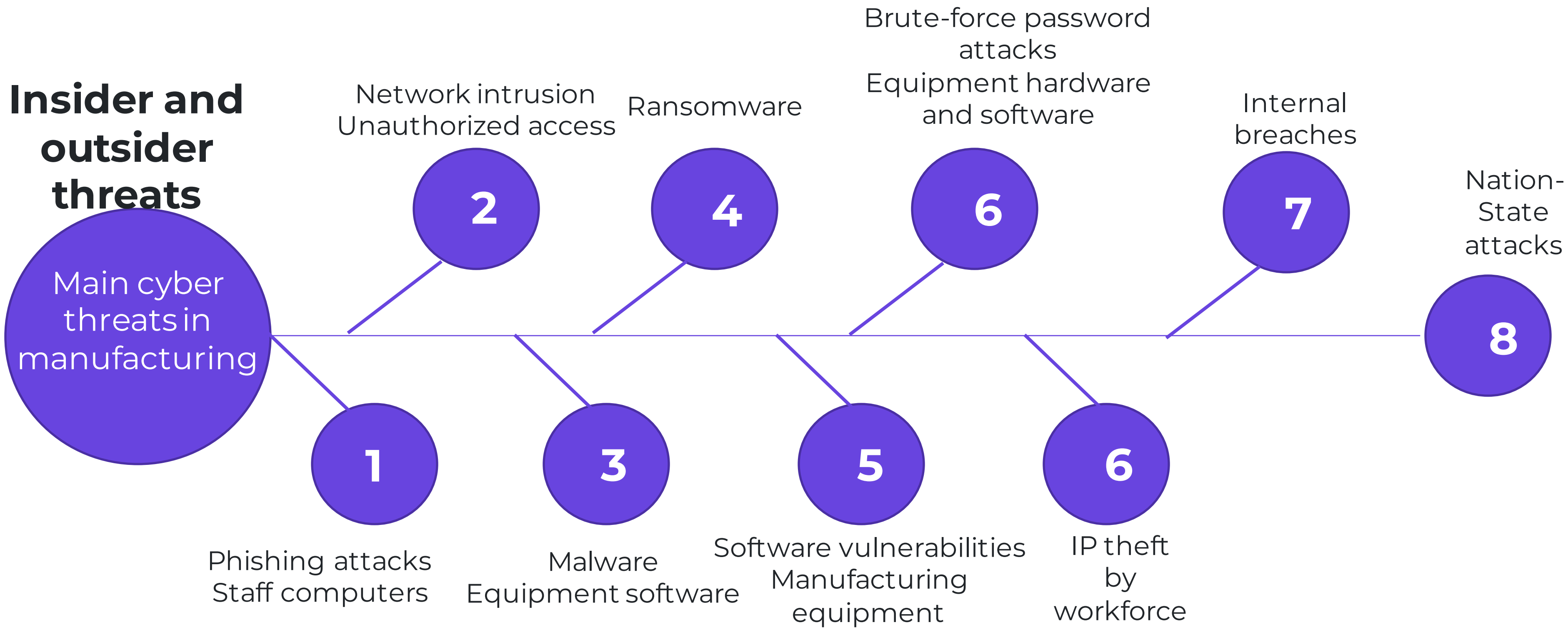


Certificate Authority (PAA)

Intermediate CA (PAI)

Device Attestation Certificates (DAC)

Threats and vulnerablities at manufacturing



Insider and outsider threats

Main cyber threats in manufacturing

1 Phishing attacks
Staff computers

2 Network intrusion
Unauthorized access

3 Malware
Equipment software

4 Ransomware

5 Software vulnerabilities
Manufacturing equipment

6 Brute-force password attacks
Equipment hardware and software

6 IP theft by workforce

7 Internal breaches

8 Nation-State attacks

RISQUE = MENACE * VULNARIBILITE * IMPACT
(attaque: concrétisation d’une menace et nécessite l’exploitation d’une vulnérabilité)