Company Presentation

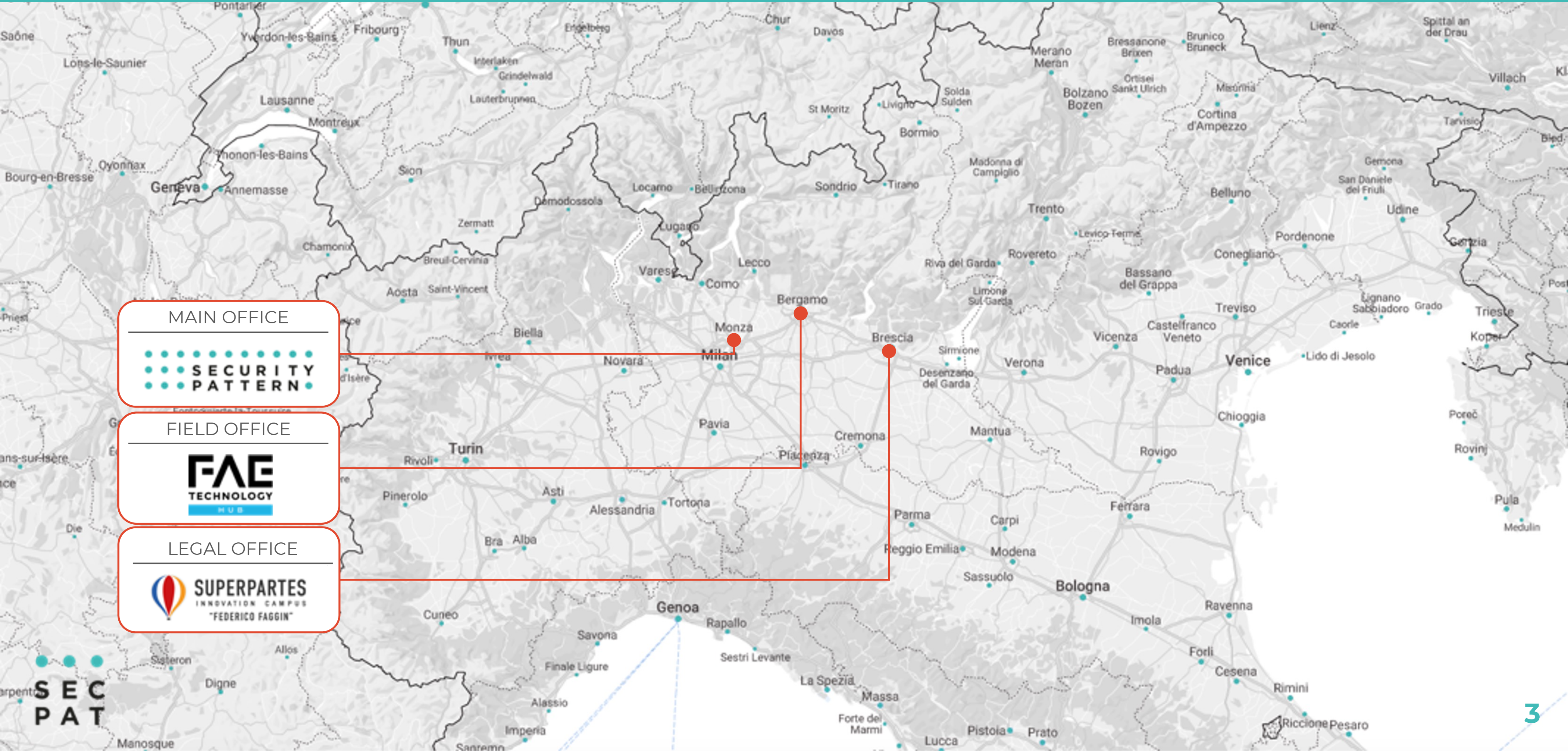
Jan. 2022

Mission

We help creators of intelligent connected devices to **design**, **implement** and **operate** their systems with a **sustainable security level**

SEC PAT

Where we are



SEC PAT

Who we are: the team

Matteo Giaconia
Senior System Engineer

Alberto Battistello
Senior Security Engineer

Lorenzo Nava
Security Engineer

Stefano Cristalli
Senior Security Engineer

Gabriele Quagliarella
Security Expert

Maria Chiara Molteni
Security Engineer

Marta Fornasier
Security Engineer

Fabiana Gaffurini
Administrative Manager

- Engineer - M.Sc.
- Ph.D.
- Author of SHA-3
- Patents / Certs
- Master

SEC PAT

Who we are: the partners

25+

Guido Bertoni
CEO

4

Filippo Melzani
CTO

4

Massimo Ratti
DevOps Manager

1

Manuel Crotti
Business developer

- Engineer - M.Sc.
- Ph.D.
- Author of SHA-3
- Patents / Certs
- Master

SEC PAT

Partner programs

- We are partner of major productors of secure elements

SEC PAT

Typical product cycle

- Development cycle from few months up to some years
- Life cycle on the market of some years up to 10+ years
- Security spans on the entire life of the device

Security is a Process

- A single SW or HW component is not going to solve security problems
- What is secure today might be broken tomorrow
- Security is a combination of
  - Hardware
  - Software
  - Procedures

SEC PAT

Our offer

- Consultancy
- Development
- Training

In the field of **security** for embedded devices, IoT, industrial and automotive.

SEC PAT

Security Pattern's reference markets

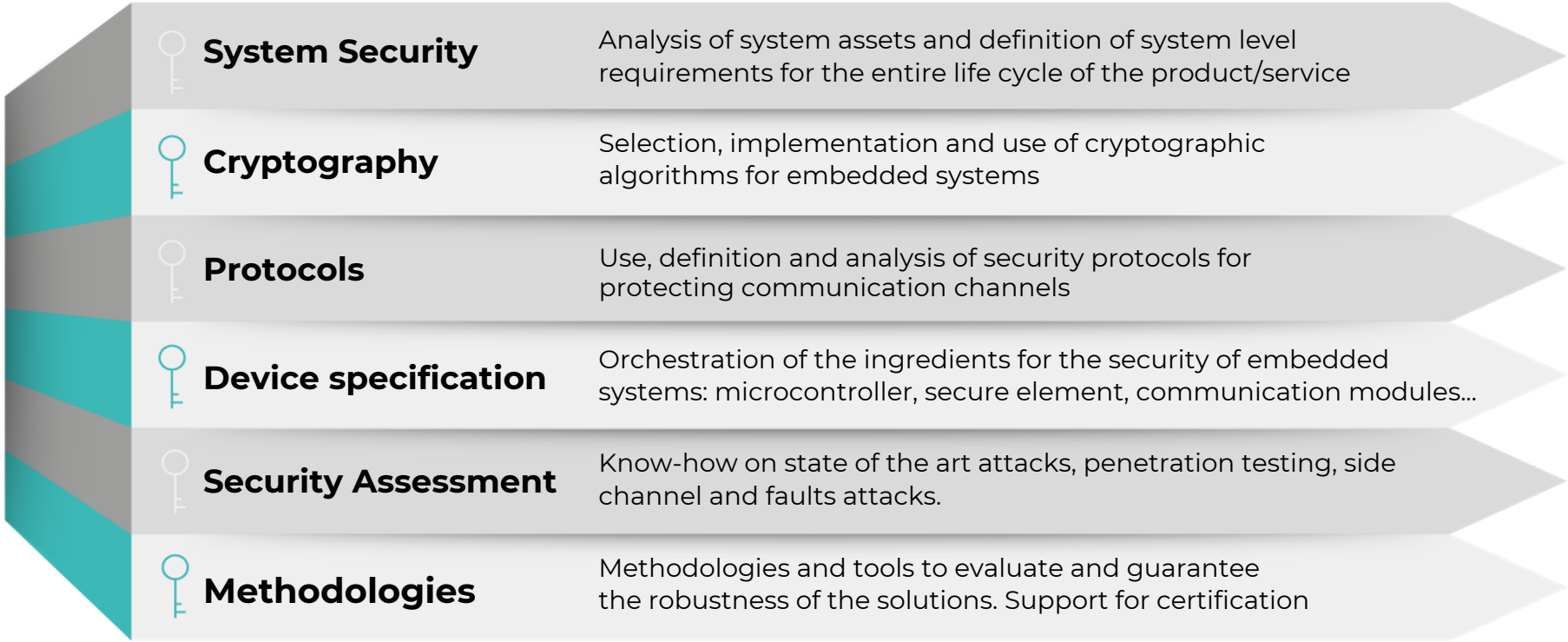
- IIoT
  - Industrial automation
  - Utilities
  - Automotive
  - Medical
  - ...

- IoT
  - Smart building
  - Home automation

- Misc.
  - Consulting
  - FW development
  - Government/Defense

SEC PAT

Key competencies



SEC PAT

The case of ISA/IEC 62443

- Reference security standard for IACS
- Our offer:
  - **Course with qualified trainers**
  - **GAP analysis**
  - **Security Assessment**
  - **Consulting and development for certification path**

The case of Alexa Built-in

- Amazon defines a set of security requirements and mandate security test from accredited laboratories
- Our offer:
  - Support customer in understanding technical and procedural requirements
  - Drive development for applying requirement
  - Develop production flow relying on IoT Secure Suite
  - Setup vulnerability management process
  - Perform PenTesting before the lab
    - all test of labs passed at first run!
  - Provide Upgrade and Vulnerability reporting service (SUM)

SEC PAT

Security Pattern offering for Security Assessment

Security Assessment Offer

- Understanding the security of a device/service, including but not limited to penetration testing
- It can be focused to some well defined field, like
  - Industrial Control systems: ISA/IEC 62443
  - Security and Safety for electrical appliances IEC-60335
  - Consumer IoT: ETSI 303 645: “Cyber Security for Consumer Internet of Things: Baseline Requirements”
  - Amazon Alexa
  - Cloud security guidelines: CSA Security Guidance 4.0
  - Common Criteria or FIPS140

SEC PAT

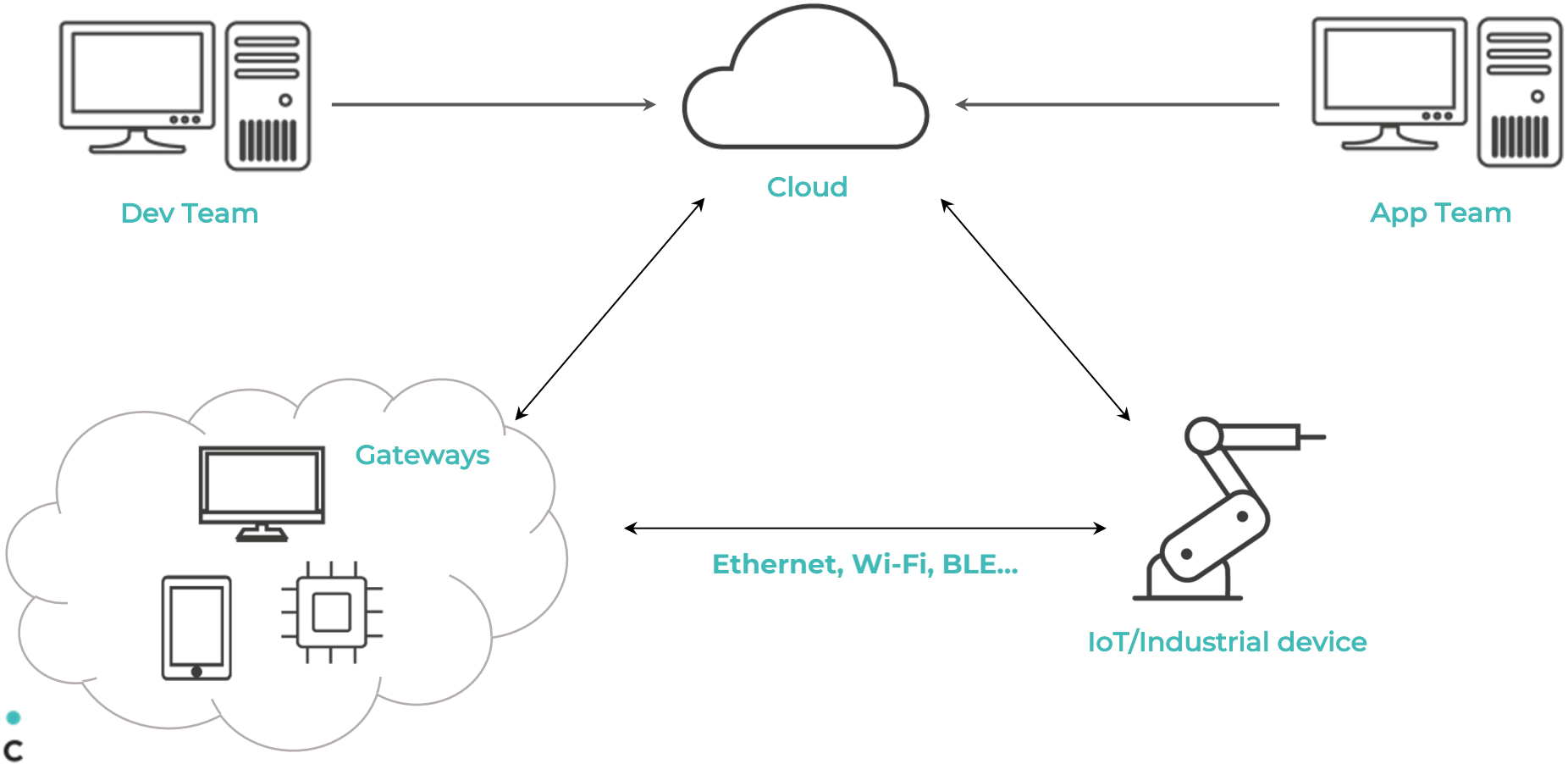
Stages of Security Assessment

- System analysis
  - Main entities and use cases in the system are analysed in order to find possible threats
- System configuration and code review
  - Hardware configurations and source code are analysed in order to follow best practices and to prevent main vulnerabilities
- Penetration testing
  - Devices in the system are analysed in order to extract sensitive information or induce misbehaviours
- Reporting

SEC PAT

IoT Security:
the big picture

The big picture



SECPAT

Security Objective

- Identify users and devices
  - Who is who
- Provide secure services
  - Data streams
  - Manage device firmware
- Rely on standard components as much as possible
  - Public key cryptography, certificates and PKI

SEC PAT

IoT Secure Suite
Key ingredients

SECPAT

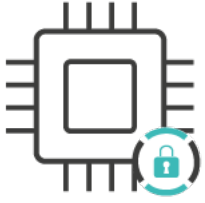
IOT SECURE SUITE®

The key ingredients

IOT SECURE SUITE®

PKI with dedicated CA

Smart Key provisioning process



Secure Key storage architecture

Secure FOTA

#1: PKI with dedicated CA

IOT SECURE SUITE

- State-of-the-art **PKI** with X.509-v3 standard certificates
- Ad-hoc **key ceremony**
- CA's private keys securely stored
- Secured procedure for device certificates generation

- Definition of PKI structure and its configuration
- Safe and reliable set up of PKI through key ceremony
- CA's sensitive data securely stored on HW Secure Token/HSM

SECPAT

#2: Smart key-provisioning process

IOT SECURE SUITE

- Each device is provisioned with a unique set of keys
  - For secure device authentication
  - For secure firmware upgrade
  - Application-specific keys
- The key-provisioning process is secured

- Fine-grained device identification
- Device strong authentication
- Secure data exchange between devices and cloud

SECPAT

#3: Secure key storage architecture

- Hardware protection of sensitive data
  - Platform-specific security mechanisms
  - Secure Element (SE)
- SE safely stores secrets and private data
- SE enables secure exchange with other system elements

- Non-clonable device
- IP protection

#4: Secure FOTA

- The firmware is encrypted and signed
- The devices can determine whether the firmware is genuine or not

- Firmware over-the-air accessible only to genuine devices
- Only genuine firmware can be installed on devices

ISO 27001

SECPAT

ISO 27001 - Overview

- Implementation and review of **Information Security Management Systems (ISMS)** according to the standards' requirements

- Assistance in the following domains:
  - Scope and perimeter identification
  - Risk assessment and treatment
  - Resource management
  - Documentation structure
  - Performance evaluation and continual improvement

SEC PAT

ISO 27001 - Implementation

- Through iterations with the client, we cover all aspects of **definition**, **implementation** and **refinement** of an ISMS
- At the end of our process, the ISMS is ready for a certification of **ISO 27001 compliance**

ISO 27001 - Cloud

- Cloud services and infrastructure are a typical use case for ISO 27001 implementation and compliance checking

- We provide a series of specific services relative to this domain. Examples:
  - Vulnerability assessment
  - Penetration testing
  - Expert review of infrastructure and configuration (containers, orchestrators, cloud platform) and application code (cloud services, web applications)

SEC PAT

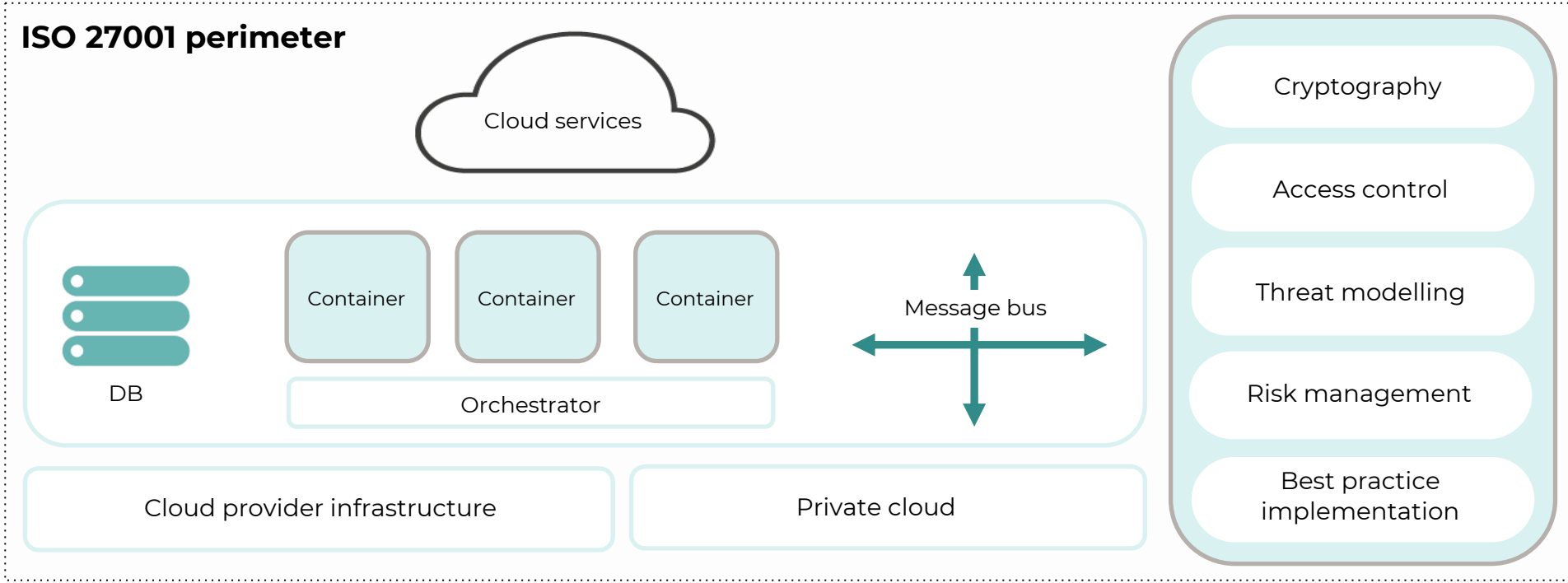
ISO 27001 - Cloud

- All activities are tailored to the client's specific scenario
- We select the relevant domains from the **CSA Security Guidance 4.0**, applying best practices and recommendations
- We follow the risk management approach of ISO 27001 to provide and implement a series of controls for risk mitigation

SEC PAT

ISO 27001 - Cloud

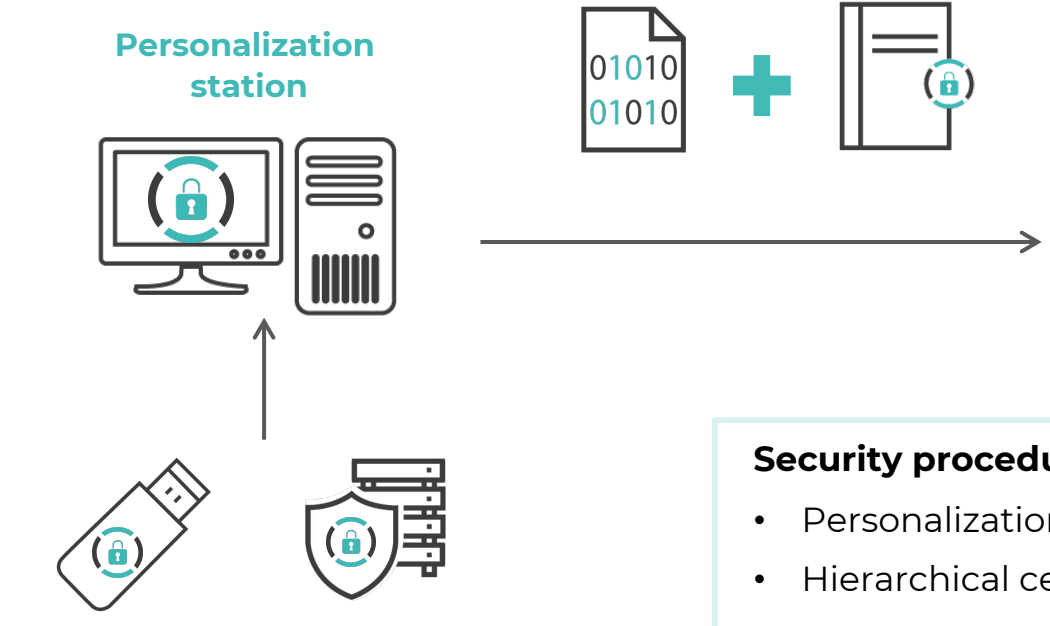
- End goal: a holistic view of cloud security, with no relevant domain left out



Smart Key provisioning

SEC
PAT

Smart Key provisioning process

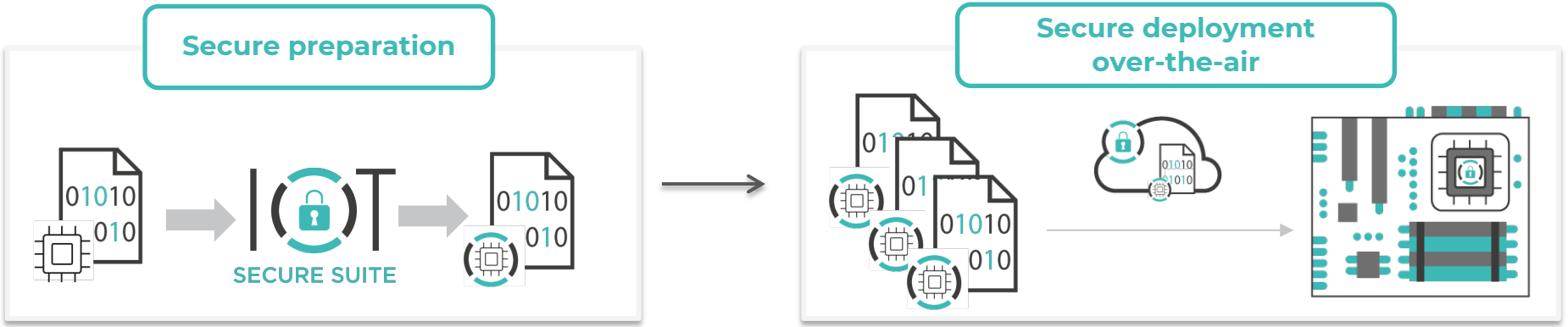


Security procedures

- Personalization performed in a secured line
- Hierarchical certificate management
- Personalization software with native interface for Secure Token/HSM

Secure FOTA

Secure FOTA



Security procedures

- Firmware update is encrypted
- Firmware update is signed with the Development Team's private key
- Devices authenticate, decrypt and install only genuine upgrades

Thank you!

hello@securitypattern.com