Multi-layered Security Technologies

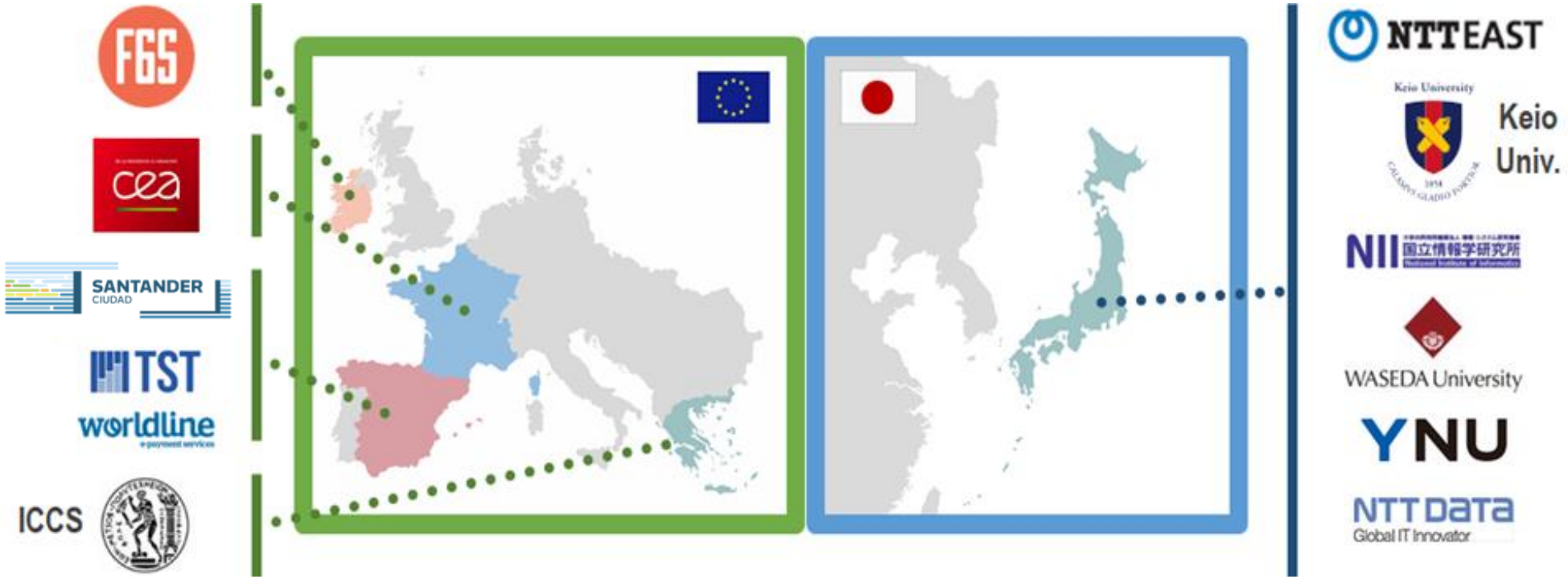
for hyper-connected smart cities

A EU-Japan collaboration

Vanessa Clemente
WLI
vanessa.clementenunez@worldline.com

Webinar, 16 June 2020

The Consortium as a whole

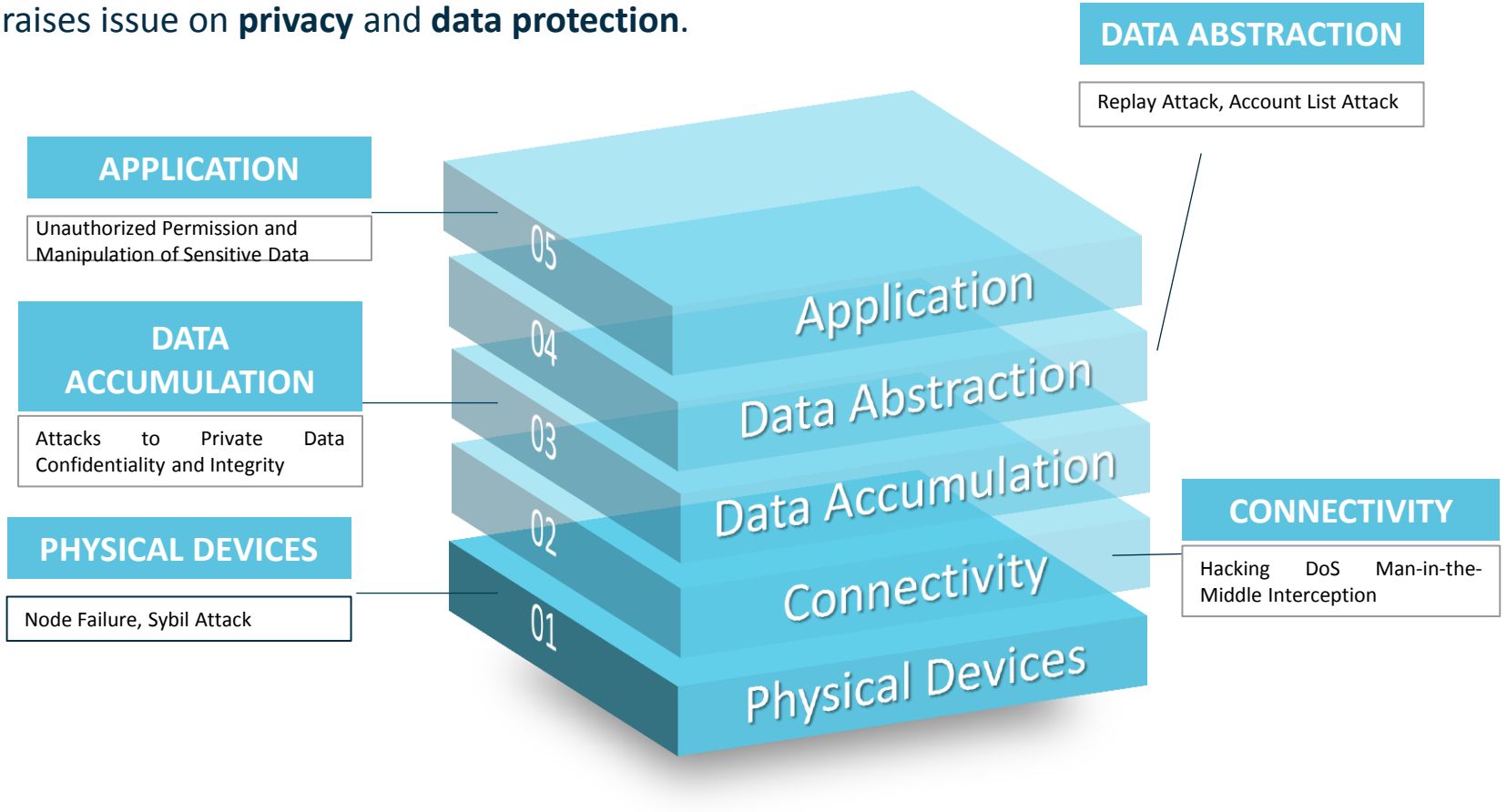


Problem Overview

- Smart city platforms are mainly **centralized IoT/Cloud infrastructures**, therefore;
  - **Inefficient** in handling actuation and control over sensors and physical devices.
  - Prone to "**complete failures**" since they dispose with **centralized** control by a limited number of administrative entities
  - **Inflexible** in the incorporation of innovative applications and new business models

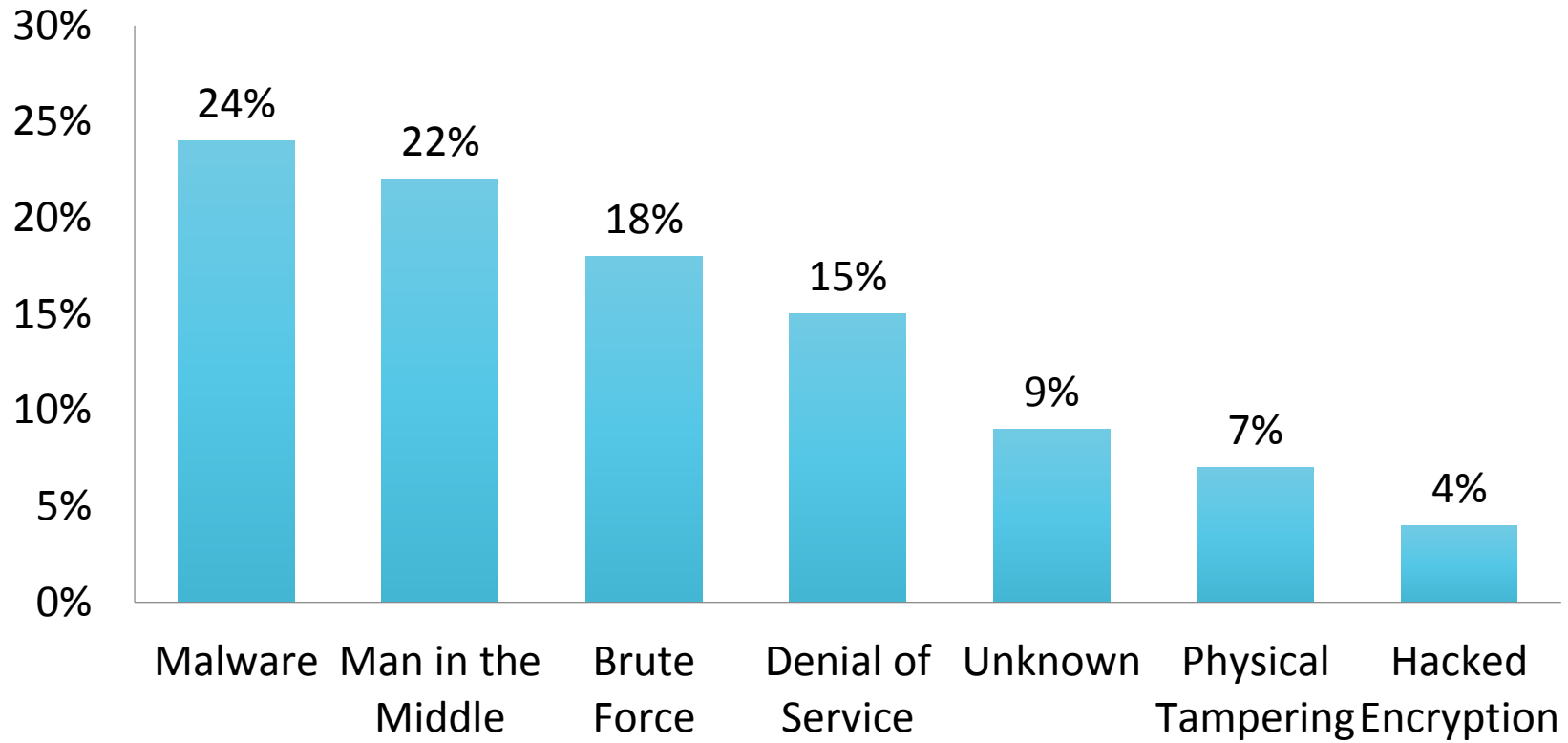
Problem Overview

- In modern smart city applications there is an emerging **need of end-to-end security** since many data sources may contain sensitive information that raises issue on **privacy** and **data protection**.



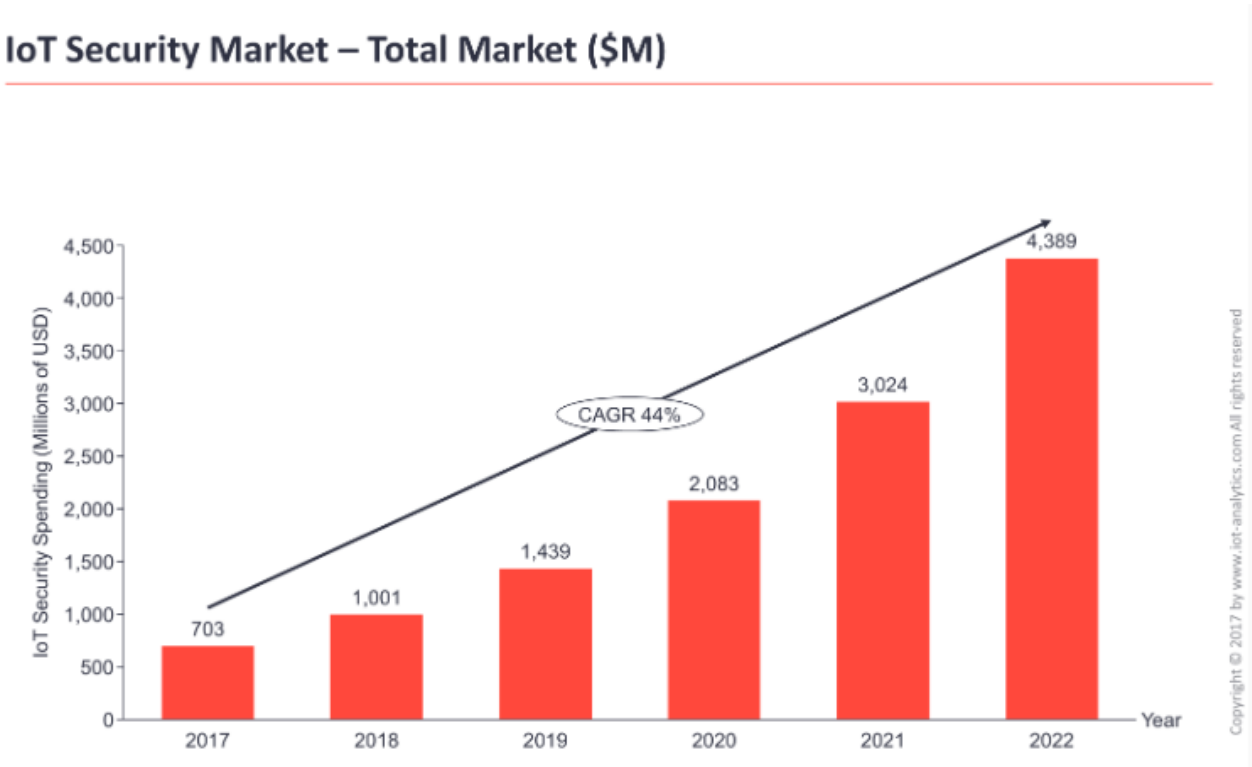
IoT Security Breaches

- According To the IoT Analytics Press Research, the most common IoT breaches that happened between 2015-2017 were caused by malware (24%), followed by human's factor "man in the middle" (22%), brute force (18%) and denial of service (15%).



Source: IoT Analytics Press Research

IoT Security Market Growth



Source: IoT Analytics Press Research

SMART CITY is one of the fastest growing segment for IoT security.

IoT SECURITY SPENDING was currently at $703M for 2017 and the fast growing market (CAGR of 44%) is forecast to become almost a $4.4B opportunity by 2022.

One of the dominant trends is increased **AUTOMATION OF IoT SECURITY TASKS**

Drivers for Security Enhancements

INCREASED USE OF IOT

- New forecast from International Data Corporation (IDC) estimates that there will be 41.6 billion connected IoT devices, or "things," generating 79.4 zettabytes (ZB) of data in 2025.
- As the number of connected IoT devices grows, the amount of data generated by these devices will also grow.

NEW REGULATIONS & POLICIES

- Governments across the globe is focusing on implementing stringent regulations regarding data security and privacy.
- Various regulations have been introduced to strengthen the security of IoT devices and avoid misuse of data such as GDPR.

HIGH NUMBER OF RANSOMWARE ATTACKS

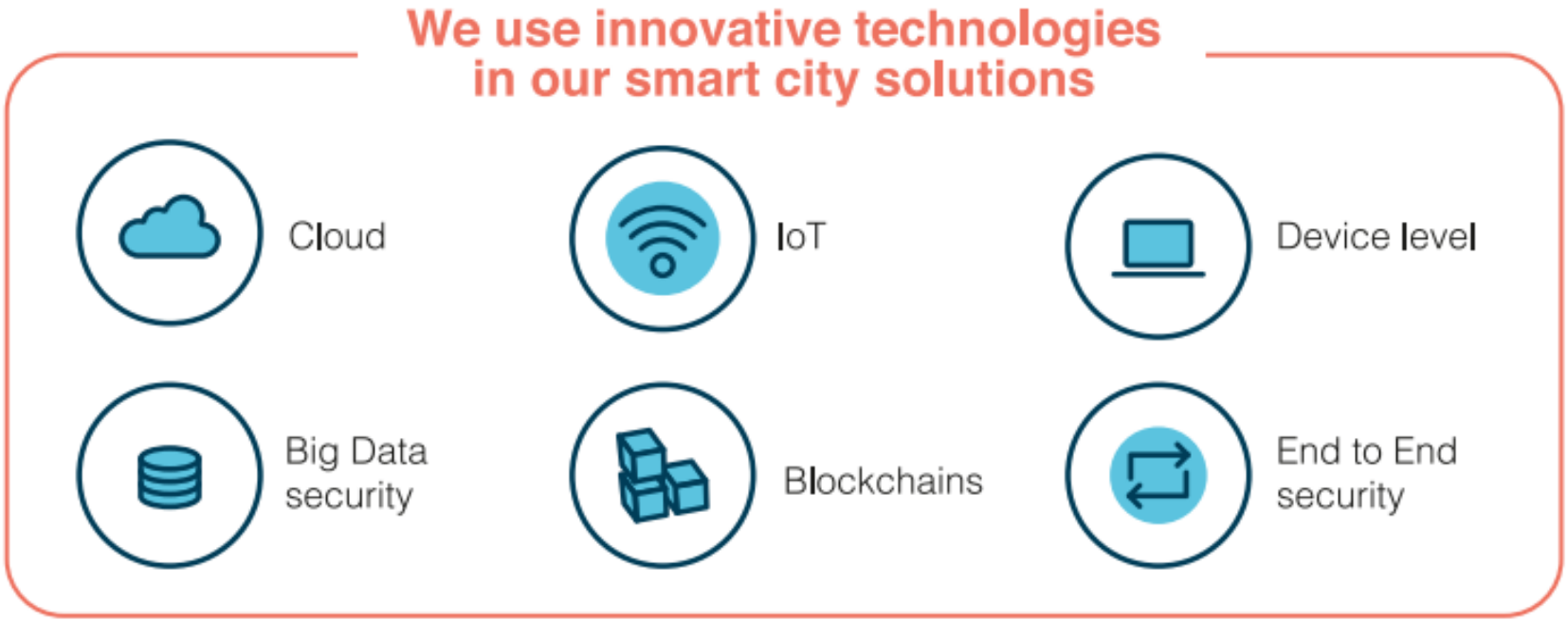
- The rise in the adoption of IoT has increased the potential of cyberattacks. Cybercriminals seek to exploit susceptibilities in smart devices manufactured with poor security practices.
- It is estimated that over 30 million IoT attacks were done in 2018, an increase of 200% than that recorded in 2017.

TECHNOLOGIES ADVANCEMENTS

- New emerging technologies such as blockchain, Artificial intelligence, Machine Leaning, etc. will facilitate the developments of new solutions focused on protecting end to end IoT Applications.

M-Sec goals

We aim to research, develop, deploy and demonstrate **Multi-layered Security Technologies** to ensure hyper connected smart cities and empower IoT stakeholders with an innovative platform which leverages **Cloud, IoT, device, BigData, blockchain, and end-end security,** upon which they can build innovative smart city applications.



Expected results

M-Sec IoT infrastructure

Through this **trusted** infrastructure, IoT stakeholders will be empowered to develop and operate new IoT applications for smart cities.

M-Sec Smart City Ecosystem

City governments, researchers, businesses, startups and developers will be connected and given access to a **complete set of tools**.

M-Sec Marketplace

Our open market of applications, data and services will facilitate the **exchange of value and information** between IoT devices and people through virtual currencies.

M-Sec Replication Plan

Learn how to **replicate the M-Sec** approach in your city. Our revenue model will guarantee the return on investment and all M-Sec benefits.

M-Sec Mission & Vision

Mission	Develop an end to end secure IoT platform upon which stakeholders can build innovative smart city applications on top of it while enabling the creation of liquid markets with profitable business models for IoT stakeholders.
Vision	Lay the foundation for the adoption and creation of new IoT Security Standards & Mechanisms

What M-Sec is offering?

Open Source & Flexible Architecture

A **market-ready open source software**, combining components that enhances end to end IoT security on each of the IoT layers (device, cloud, application).

M-Sec Ecosystem

A community with expert partners on several technologies where links among incubators, business networks, universities and developers communities are provided to **share IoT challenges and findings.**

MarketPlace of IoT Data

Exchange and monetize IoT data ensuring **anonymity, reliability and trustworthiness** of the available resources.

User Centered Design

New Applications & Business Models Developed based on a collection of end users requirements.

A secure, tested and validated Framework

M-Sec **end-to-end secure components** have been developed **to go beyond compliance of GDPR&PIPA** and avoid potential IoT attacks on each of the ecosystem layers. Tested through **five different use cases running on Europe & Japan**.

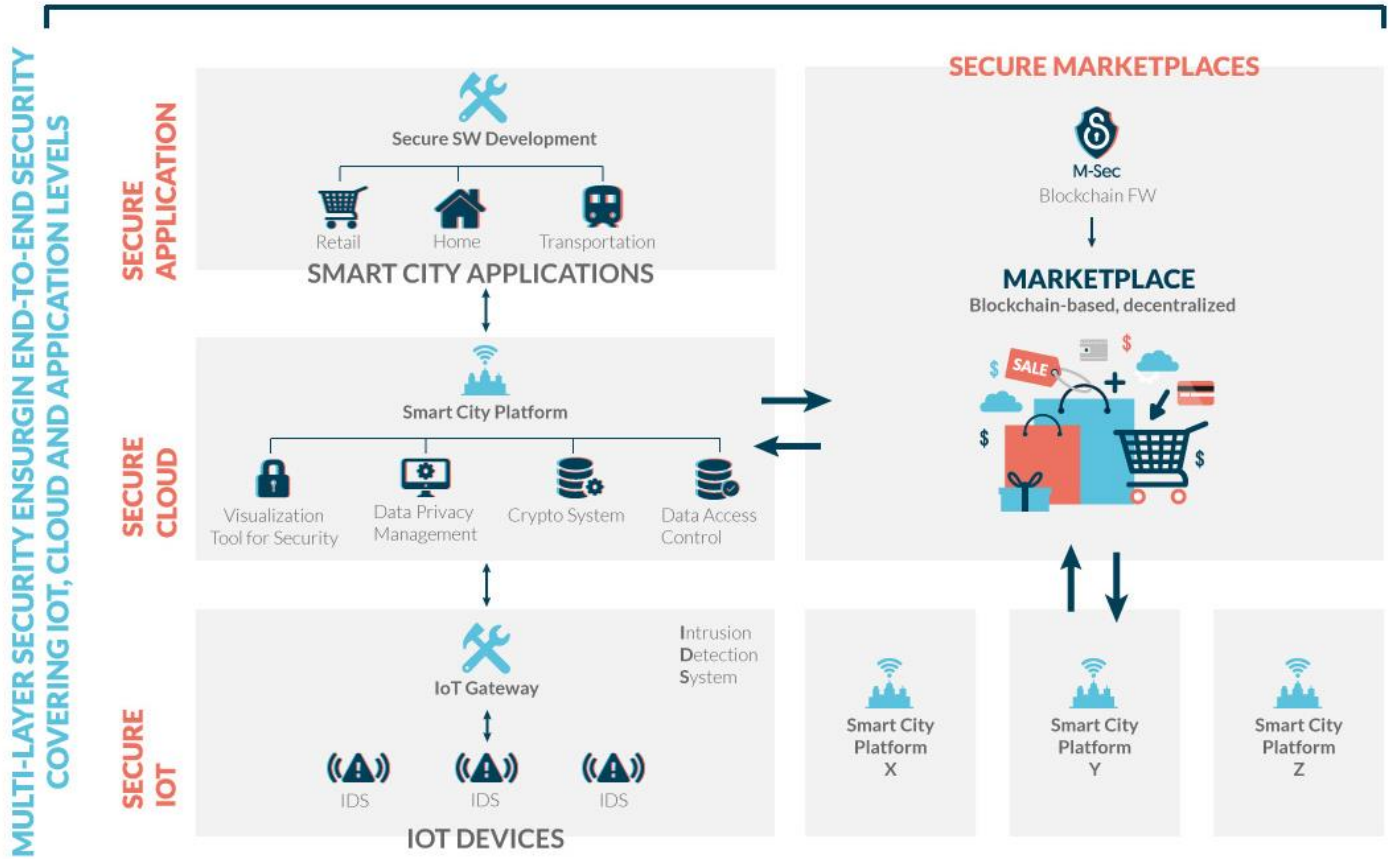
Access to Project Outcomes

Access to a set of tools , guidelines to develop secure applications and Projects Results based on Partners Research (risks and threats analysis, state of the art of technologies such as blockchain, IoT protocols).

Value Proposition

- M-Sec technology can improve the quality of life in cities, help councils and city governments, by **safeguarding their infrastructures through our Secure IoT Framework**.
- **M-Sec through its two cross border Use Cases (EU&JP) will validate interoperability, efficiency and data protection principles and strength collaboration and cooperation beyond the borders among countries**.
- M-Sec enables to focus on what is specific to add security on the smart IoT applications, making **development much faster and compliance with regulations.**
- **Access to Project Outcomes** based on deeply Research on security risks & Threats on the IoT Ecosystem as well as UCs evaluation.
- The modular nature of M-Sec means that is **possible to re-architect as the need changes**
- **Freemium Model where to experiment** with M-Sec secure components. Access to APIs and Manuals for integrations.
- Through our **Strong Community**, it is possible to share experience with other stakeholders
- **Possibility to participate** (or even speak) **at M-Sec events** and establish contacts with industry and other stakeholders.
- **Opportunity to stimulate policy innovation** regarding IoT technologies.
- **Awareness and insights on effective Data Protection regulation .**
- **Practical and proven solutions** to develop Data Protection standards on the IoT Ecosystem.

M-Sec Architecture



M-Sec Framework

M-Sec Applications


Park Guide


Home Monitoring


Environment Monitoring


Citizen as Sensor


MarketPlace IoT Data


Development & Security Designing Tools

Security Analysis Tool / MTSA

YNU Honeypot


Secure City Data Access

Eclipse sensiNact platform (and Studio)

KEIO SOXFire


Privacy Managament Tool

Ganonymizer


Secure & Trusted Storage

Crypto Companion DB

Quorum Blockchain framework & Blockchain middleware


IoT Data MarketPlace

IoT Marketplace

T&R Model engine/tool


Secure Devices

Secured components for devices

IoT Intrusion Detection System

Monitoring & Visualisation Tool

Security Management Tool

End to End Security

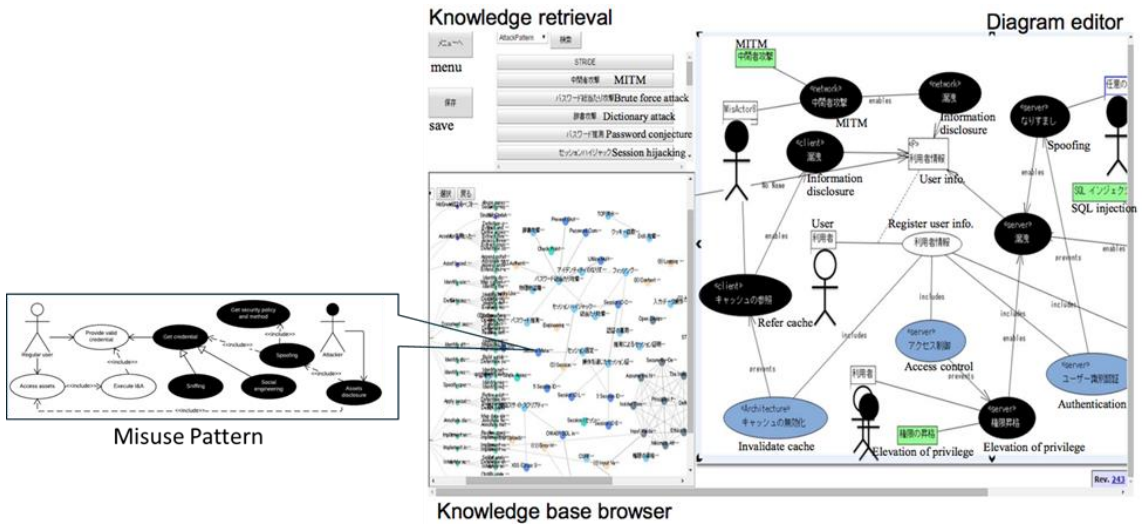
Development & Security Designing Tools

Development & Security Designing Tools

Security Analysis Tool / MTSA

YNU Honeypot

We propose a framework for building a body of knowledge and constructed a knowledge base for secure software development. We provide **security requirements modeling support system (Security analysis tool) and A Modal System Transition Analyzer to eliminate both human errors in designing the application logic and a wide number of tests** performed to verify the security level.

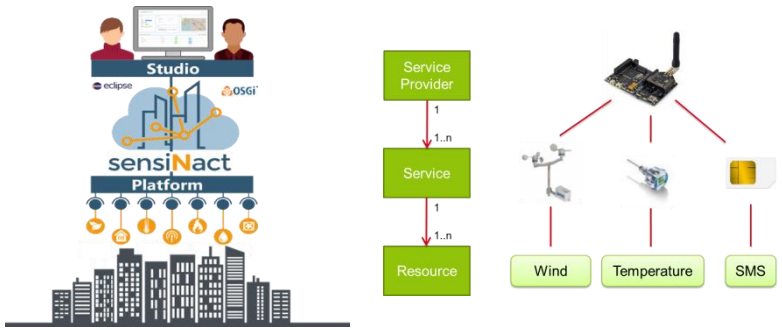


Secure City Data Access & Privacy Management Tool

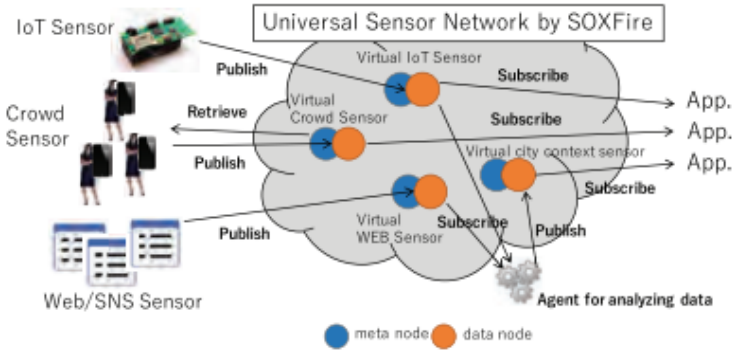
Secure City Data Access | Eclipse sensiNact platform (and Studio) | KEIO SOXFire

Privacy Managament Tool | Ganonymizer

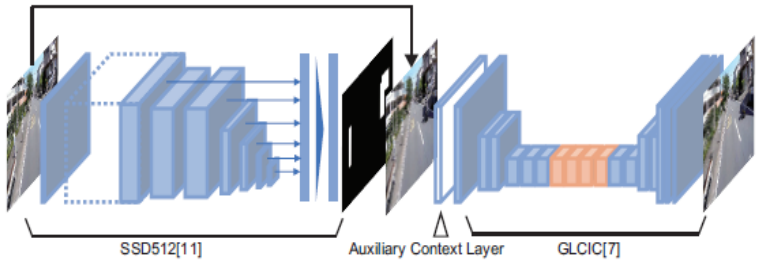
- **SensiNact** is designed to allow those platforms to **interoperate**, thus **coexist** and **benefit** from the richness of the variety. SensiNact, **provides a fine grained security mechanism to allow access to services by only authentified and authorised entites.**
- **KEIO SOXFire** can provide **practical distributed and federated infrastructure for IoT sensor data sharing among various users/organizations** in a way that is scalable, extensible, easy to use and secure while preserving privacy.
- In situations where **image (photo/video) data** is used in various IoT application use cases such as smart cities, personal information is often a problem. **GANonymizer is a technology that automatically deletes personal information contained in such images using AI technology.**



Eclipse SensiNact Platform



Keio SOXFire



Ganonymizer

Secured&Trusted Storage & IoT Data Marketplace

Secure & Trusted Storage

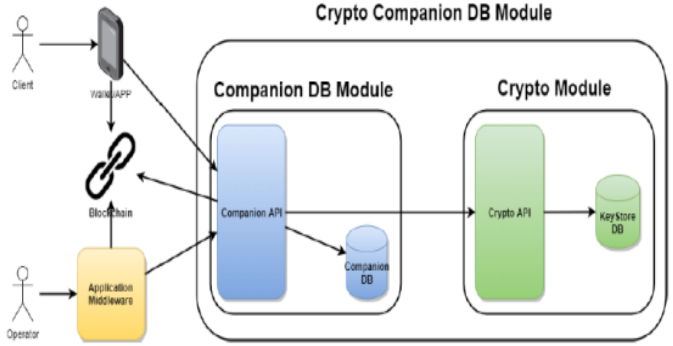
- Crypto Companion DB
- Quorum Blockchain framework & Blockchain middleware

IoT Data MarketPlace

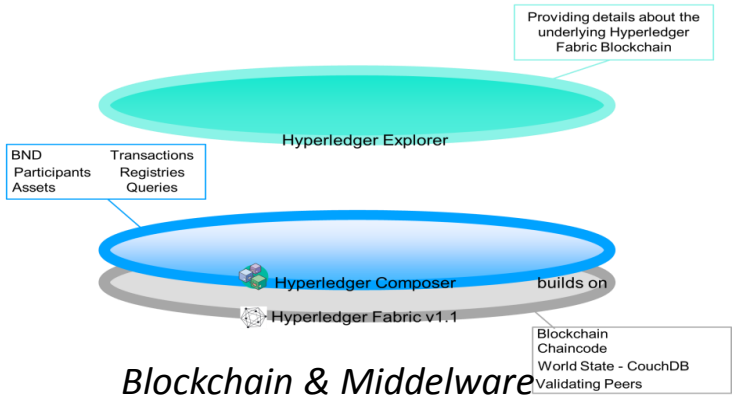
- IoT Marketplace
- T&R Model engine/tool

A parallel system to the blockchain for the encrypted storage where sensitive data is encrypted together with a hash. Thanks to the **M-Sec Blockchain and Middleware it is possible the synergy between on-chain and off-chain data and access control**, through enhanced Transactions and Meta-data handling, providing anonymity through the Know Your Customer service and enabling the extension of the system with higher-level services such as Trust & Reputation Management, Proof of Location mechanisms, etc.

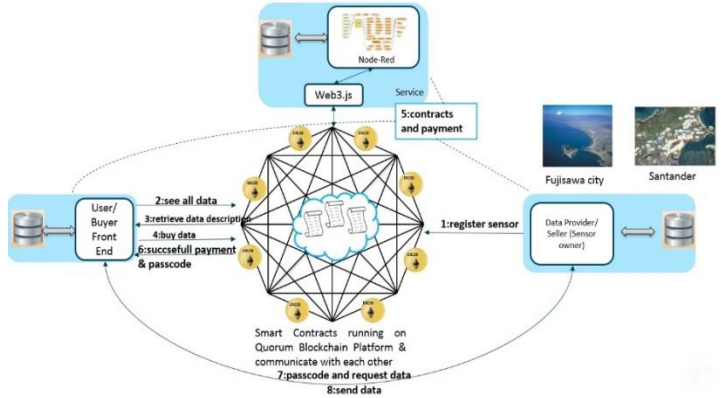
For anonymized data, The **M-Sec IoT Marketplace allows users to exchange information through the use of virtual currencies**, allowing real-time matching of supply and demand. The marketplace uses a **T&R Model Engine, enhancing security and making it possible to evaluate the actual content being shared**, thus ensuring the trustworthiness of the several actors participating in the exchange or sharing of information, data and services.



Crypto Companion DB



Blockchain & Middelware



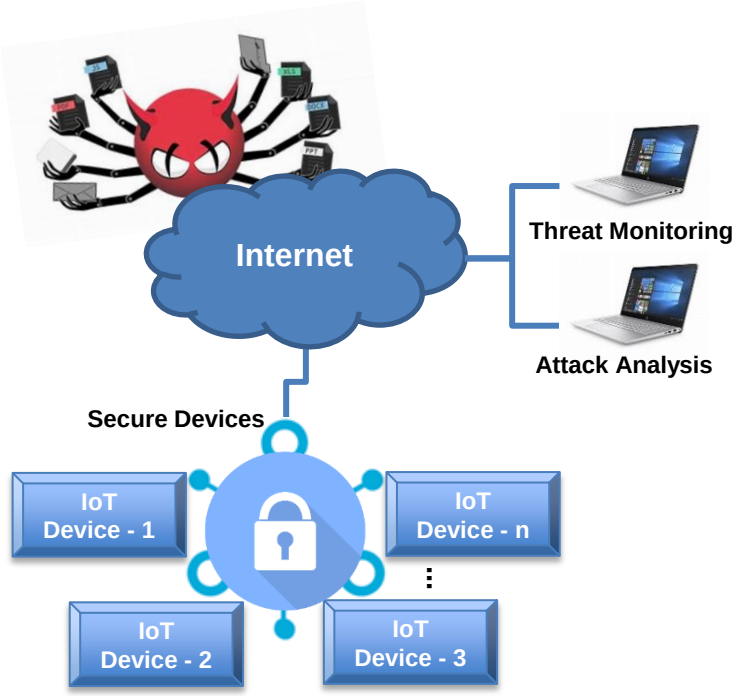
IoT MarketPlace & T&R

Extended Security for Devices

Secure Devices

- Secured components for devices
- IoT Intrusion Detection System
- Monitoring & Visualisation Tool

- Ensure confidentiality, integrity, and availability
- Ensure security of IoT devices using defense-in-depth mechanisms and threat monitoring
- Secure elements for authentication and encryption
- Provides multi-layered security against malicious activities and policy violations



Extended Security for Devices

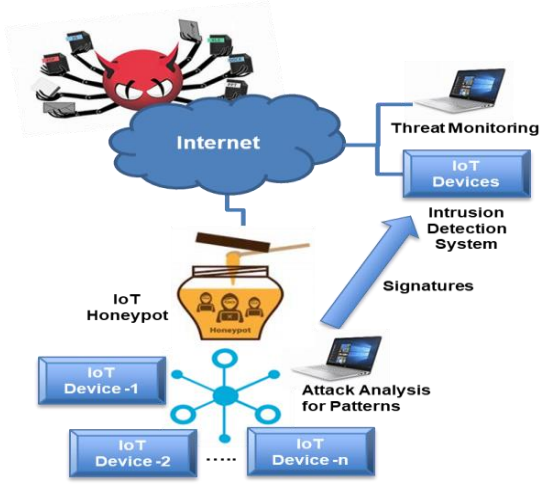
Secure Devices

Secured components for devices

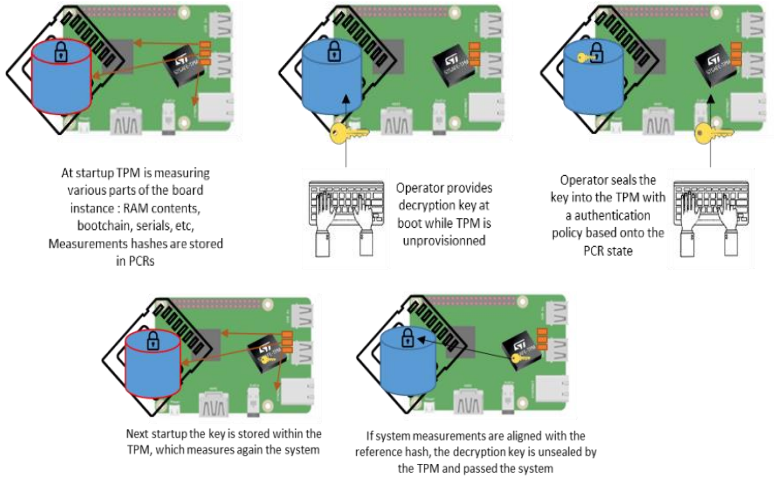
IoT Intrusion Detection System

Monitoring & Visualisation Tool

Protect vulnerable IoT devices from malicious activities using **defense-in-depth mechanisms and threat monitoring**, thereby providing multi-layered security against policy violations and cyber attacks, along with security health-checks



Secure element to handle the integrity of the device during the boot process and the authentication and encryption for external communication channels.

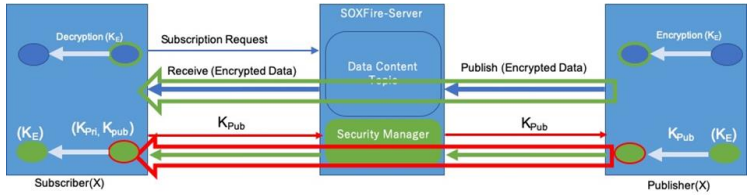


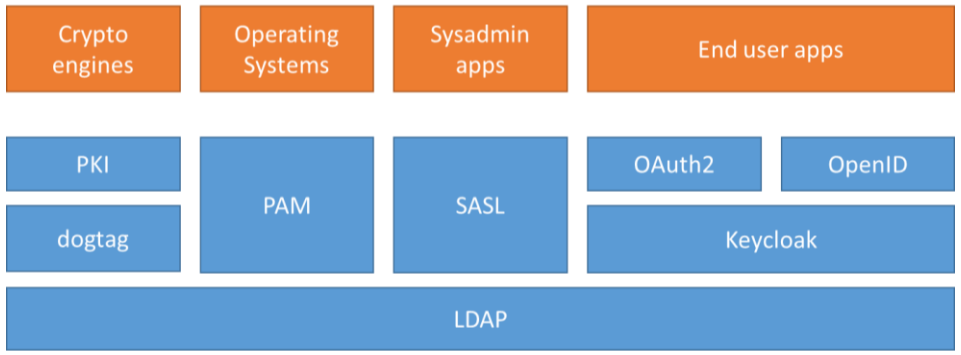
End to End Security

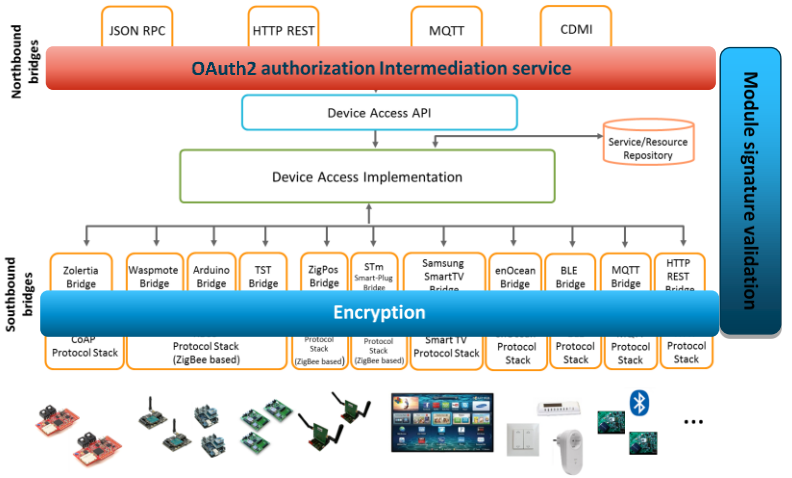
End to End Security

- Security Management Tool
- End-to-end Encryption Middleware for SOXFire
- sensiNact - Secured IoT Middleware

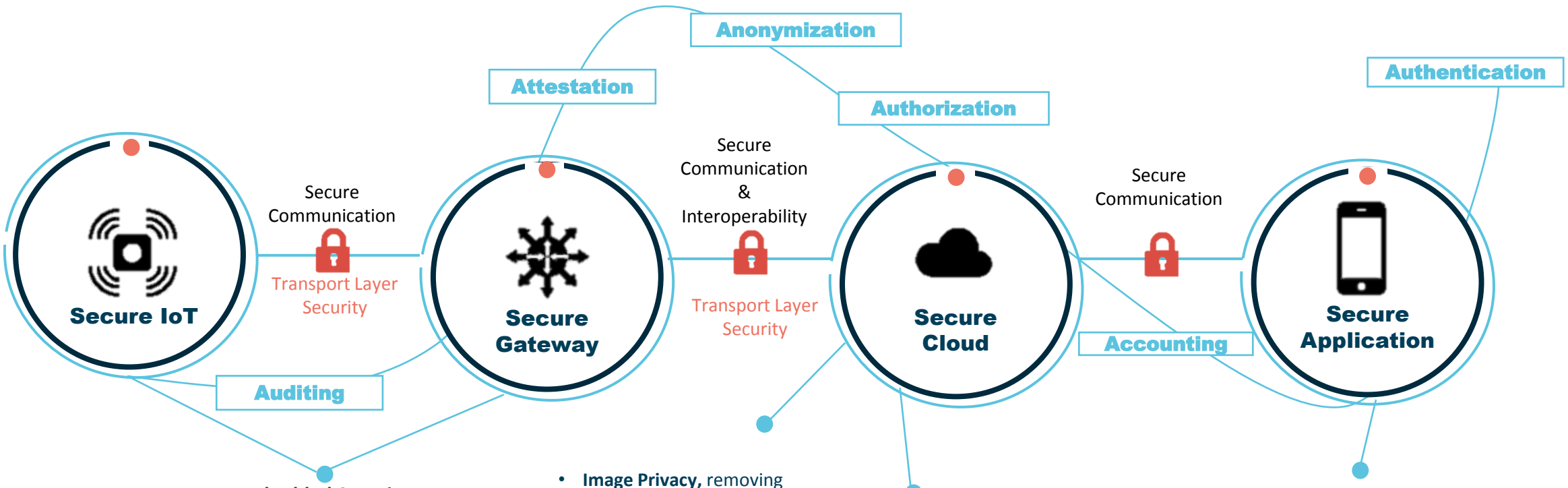
Security Management Tool to provide interoperable AAA (authentication, accounting, authorization) in an interoperable way. Middleware such as SOXFire and sensiNact can then use mutually this security management tool to authenticate devices, data from devise, end-users and cloud core component to build trust over the architecture.







Advancing to end-to-end IoT Security Application



Embedded Security

- **Remote attestation platform**
- **Trusted Platform Module**
- **Intrusion Detection System**

- **Image Privacy,** removing personal data in streaming
- **Visualization Tool for threat monitoring & health check**
- **Abstraction layer** to hide the heterogeneity of IoT devices
- **Exchange data with the anonymous subscription function.**

Secure, robust , distributed and encrypted data Storage

- Parallel system to the blockchain for the encrypted storage of personal Data
- Blockchain and Middleware Services provide a distributed ledger environment with enhanced capabilities related to content sharing and security enhancement

Application Security Guidelines & Vulnerability Assessment

- **Security Analysis Tool framework** for building Secure Applications
- **A Modal System Transition Analyzer** to eliminate both human errors in designing the application logic and a wide number of tests performed to verify the security level.

Our **new IoT applications** will be tested across **two smart cities**

Fujisawa, Japan

A pioneer in citizen wellness tech, natural disaster protection and sustainable energy, Fujisawa stands out as one of Japan's most innovative

Santander, Spain

A global leader in citizen-oriented technologies, Santander has developed its own "city brain" platform to manage all urban facilities.

Testing five unique ‘Use Cases’

M-Sec aims to facilitate **diverse areas of smart city life**, from improving the wellbeing of growing elderly populations, to monitoring rubbish collection, to creating playable city ‘games’.





Use Case 1: Secured IoT devices to enrich strolls across smart city parks

Santander

PARK GUIDE WEB APP

PARK INFO & ALERTS

ENVIRONMENT AND PRESENCE MONITORING

IoT HW SECURITY

ALARMS SET-UP

GAMING FEATURES

What is the Use Case about?

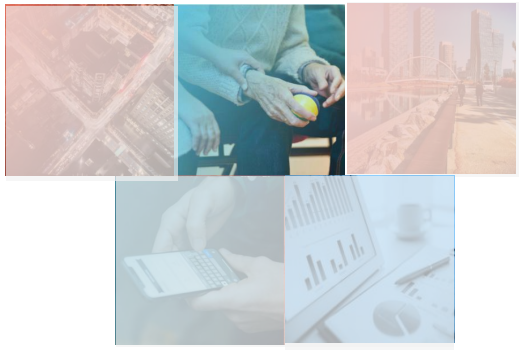
The deployment of different IoT devices in selected areas of a park near downtown Santander will feed the Park Guide application, allowing citizens and visitors to obtain information that enriches their park strolling experience and the Municipality officers to **monitor closely these spots and perform complete evaluations that will derive in taking effective actions** based on knowledge and alerts obtained from the measurements collected.

Problem Overview:

This Use Case involves **offering reliable data related with the overall environmental status and occupancy in specific areas of the park.** Attackers can tweak the values register by sensors and in the end trigger erroneous actions from the Municipality side. Therefore, **data security and integrity is the main issue on the applicability and scalability of this solution.**

M-Sec Benefit:

Novel HW security features implemented in M-Sec **will prevent IoT devices from external attacks** and the introduction of blockchain techniques will contribute to foster the participation of end users and thus improve the system effectiveness.



Use Case 2: Home Monitoring Security System for Ageing People

Santander

What is the Use Case about?

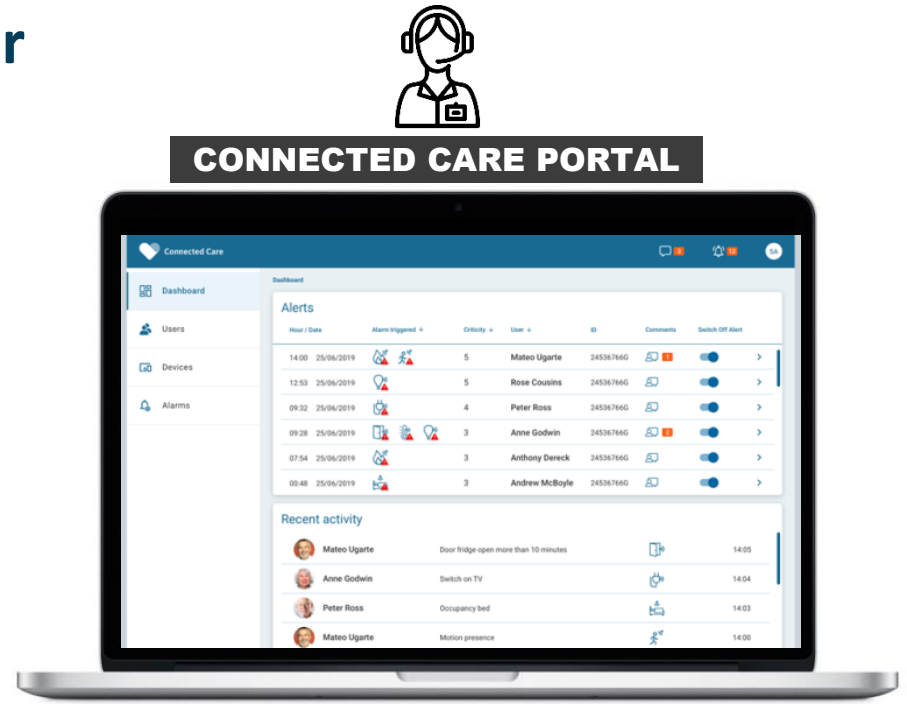
Our solution is based on the Connected Care Platform, allowing **Tele-assistance operators to be able to monitor elderly homes with the aim to improve the quality of life of elderly people living alone** and conduct decision-making based on rules and alerts configured upon the activity collected by different home sensors.

Problem Overview:

This Use Case involves **processing sensitive data such as the activity happening in a specific use's home.** Sensors to be deployed, have a lot of personal information that an attacker can use to track, for instance data generated from a motion sensor. Therefore, **data security and integrity is the main issue on the applicability and scalability of this solution.**

M-Sec Benefit:

By using M-Sec, it is possible to go beyond compliance of GDPR by adding additional security measures to prevent external attacks that may lead to erroneous actions from end-users . **This Use Case benefits for instance of a parallel encrypted system for data storage (CCDB) connected to the blockchain to ensure data tamper proof.**



Use Case 3: Secure and Trustworthy Mobile Sensing Platform

Fujisawa

What is the Use Case about?

This use case provides a client application that allows **urban environment monitoring** entities (for example local governments) **to visualize spatially and temporarily dense environmental data** such as air quality, temperature/humidity,, garbage disposal amount, unimpaired road marks,…

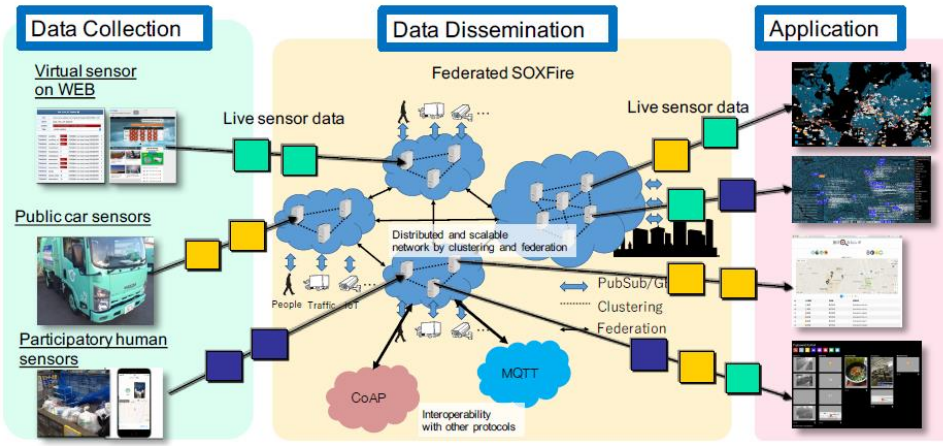
Problem Overview:

In order to share data between cities on the smart city platform, privacy protection and security assurance mechanisms are indispensable, but existing platforms still have problems in privacy protection and security assurance.

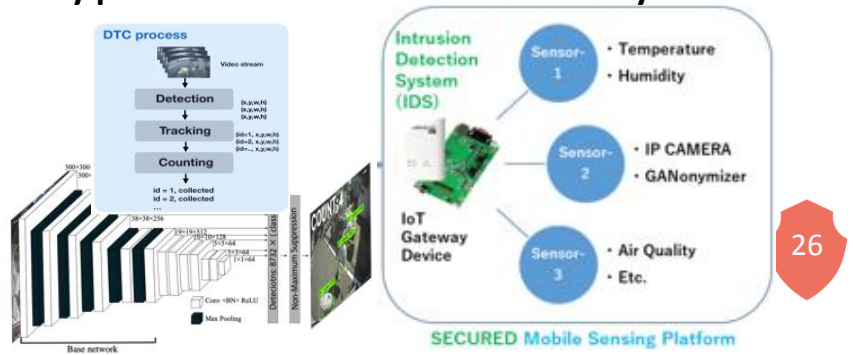
M-Sec Benefit:

For protect privacy, **GANonymizer** that can automatically delete privacy information from image data such as camera images often handled by smart city platforms is supported.

For security protection, multi-layer security protection is implemented at each layer as follows. The **point-to-point encryption mechanism** (TLS) between the IoT device and the cloud, the **advanced authentication mechanism** in the cloud, and the end-to-end sensor data stream distribution are protected by a **lightweight encryption mechanism**. and this system will be made configurable and manageable by a **security management tool**.



Privacy protected and Secured enhanced by M-Sec assets



Use Case 4: Secure Affective Participatory Sensing of City Events

Fujisawa & Santander

What is the Use Case about?

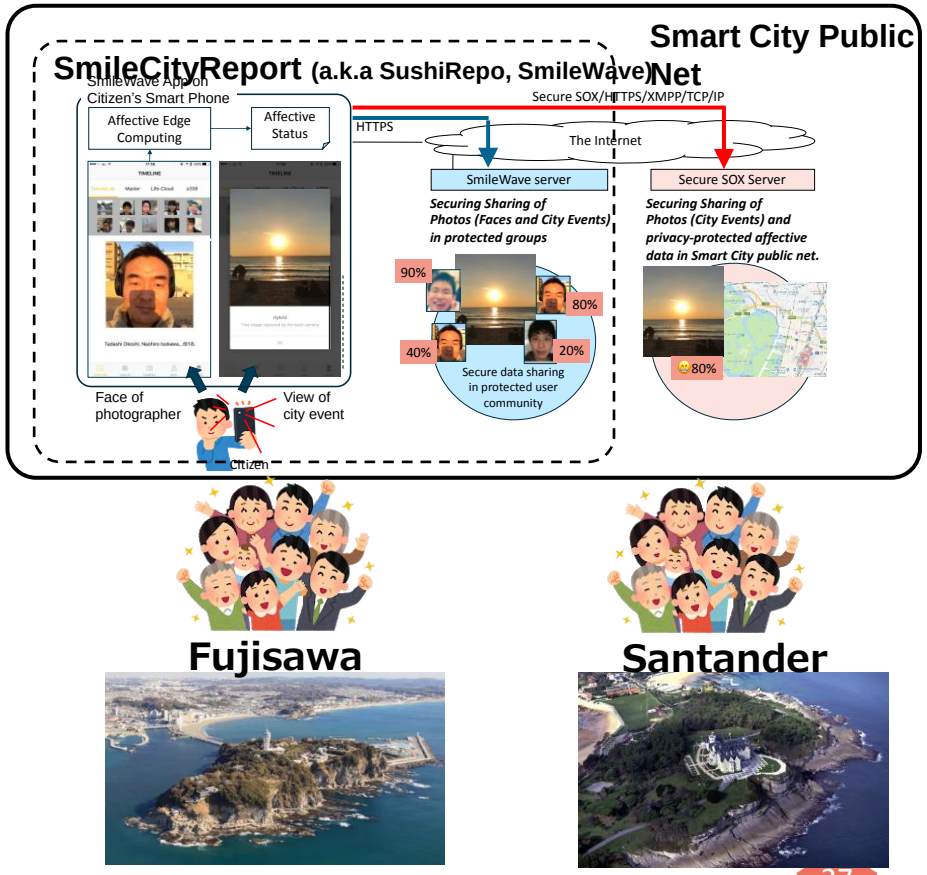
This UC4 explores the possibility of secure sharing on citizen's affective information and information on the city, by using **"SmileCityReport" an application that allows to exchange photos of specific themes (i.e city spot, gastronomy, etc.).**

Problem Overview:

In the existing smart city platform, it is difficult to realize an environment where citizens can **exchange information and participate with peace of mind from the viewpoint of privacy protection and security protection.**

M-Sec Benefit:

We develop a **privacy-protected mobile participatory sensing platform** in which citizens can share information on their neighborhood (city) with corresponding affective status information attached, and where such information is shared securely among the citizen's community and publicly with an appropriated privacy-protection mechanism.



Fujisawa

Santander

Use Case 5: Smart City Data Marketplace with Secure Multi-Layer Technologies.

Fujisawa & Santander

What is the Use Case about?

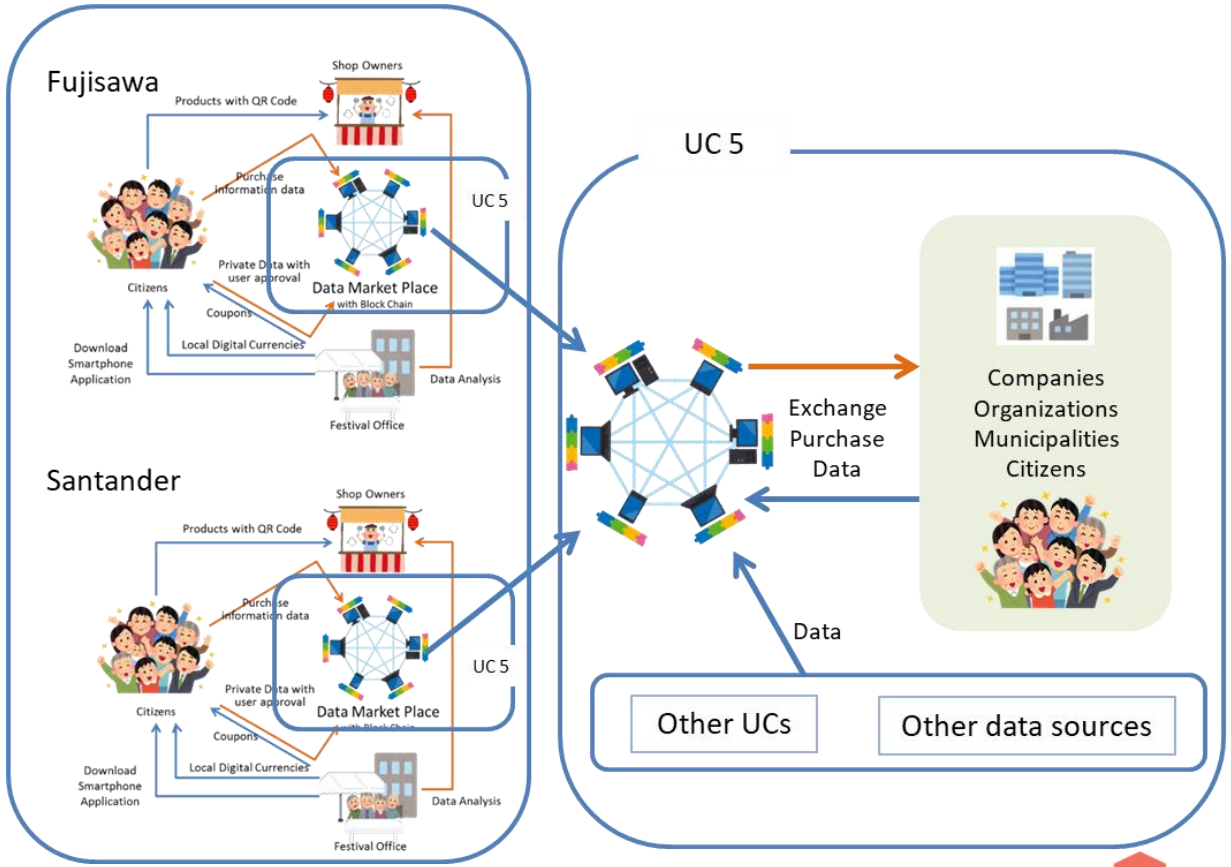
This UC5 is to build an **M-Sec marketplace** where data collected during field trials in each use case can be traded in both Japan and Europe while **ensuring security on all layers** through blockchain and other mechanisms.

Problem Overview:

This UC will handle all sorts of data including **personal data** which needs to **be prevented from falsification** and be traded **in a secure environment**, and also need to **avoid attacks to the blockchain** and the actual marketplace.

M-Sec Benefit:

The **marketplace** needs to be operated in a secure environment **using M-Sec which will consider the security requirements of GDPR and PIPA.** Indicatively, M-Sec has conducted a lot of **research on coupling encrypted databases with blockchain technologies**, thus making the synergy of off-chain and on-chain storage and processing of data possible, a characteristic which enhances security considerably, while still **ensuring data reliability and users' privacy**. Also, the integration of a Trust and Reputation system within the blockchain implementation is considered.

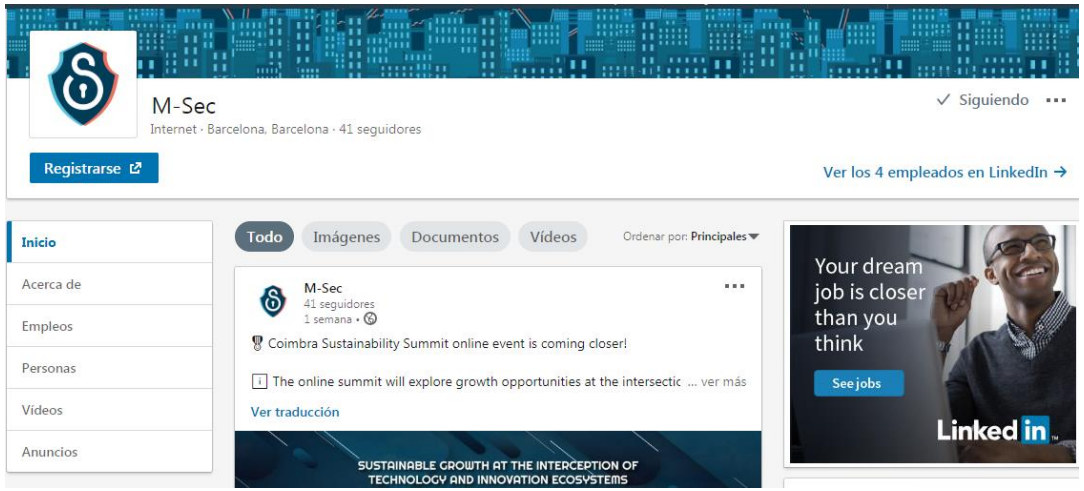


Do you want to know more?

www.msecproject.eu

….and don’t forget to follow us on

linkedin.com/company/msecproject



@MSecProject

Multi-layered Security Technologies

for hyper-connected smart cities

Thank you!

www.msecproject.eu

www.f6s.com/iot

@MSecProject

linkedin.com/company/msecproject

The M-Sec project is jointly funded by the European Union's Horizon 2020 research and innovation programme (contract No 814917) and by the Commissioned Research of National Institute of Information and Communications Technology (NICT), JAPAN (contract No 19501).