Multi-layered Security Technologies

for hyper-connected smart cities

A EU-Japan collaboration

M-Sec goals

We aim to leverage **Cloud, IoT, device, BigData, blockchain, and end-end security** technologies to build innovative smart city applications.

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

Fujisawa, Japan

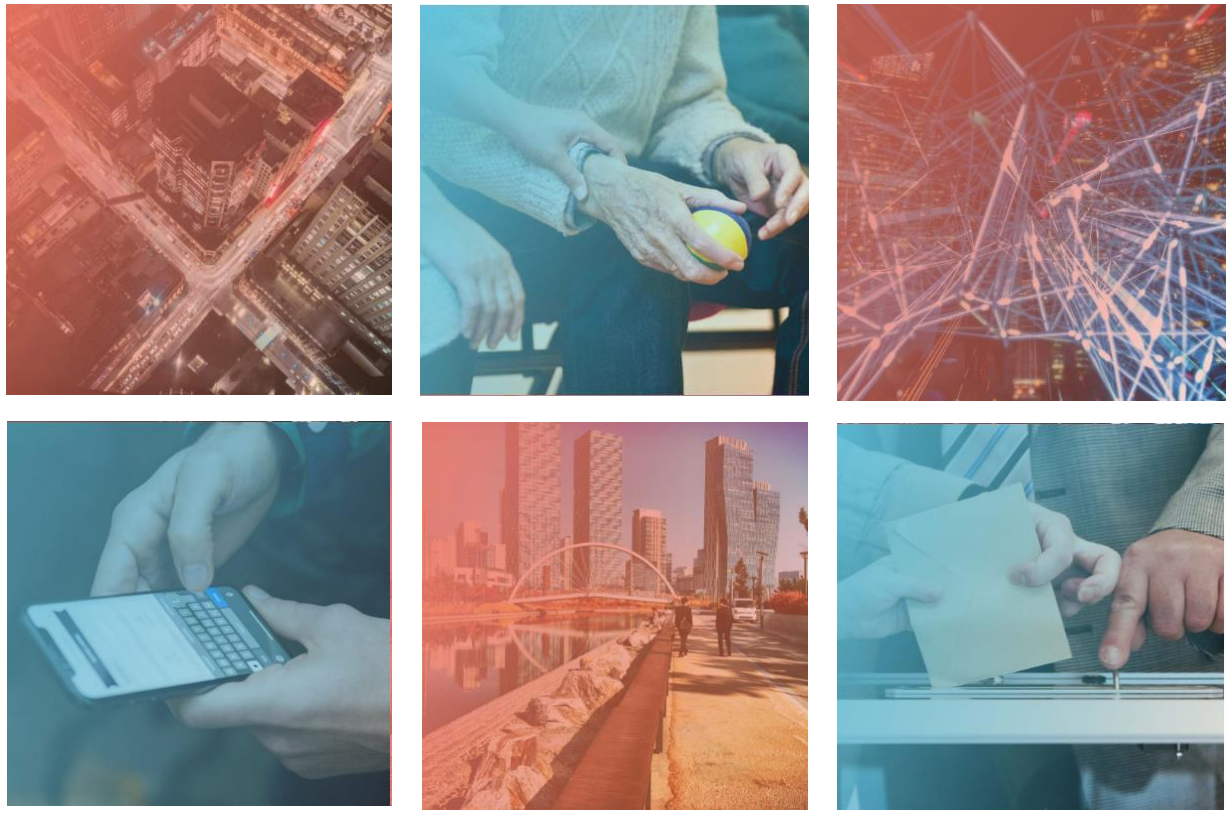
A pioneer in citizen wellness tech, natural disaster protection and sustainable energy, Fujisawa stands out as one of Japan's most innovative cities.

Santander, Spain

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

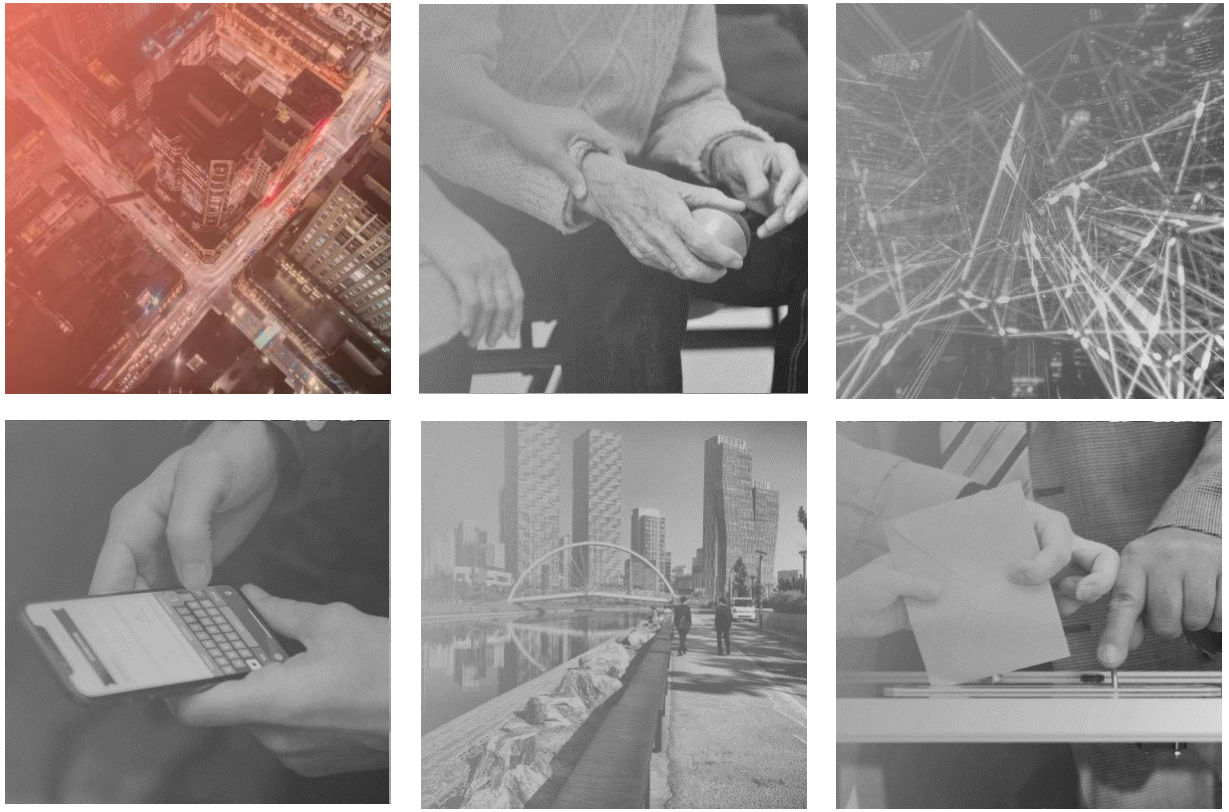
Testing six unique ‘Use Cases’

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: Reliable IoT Devices

Santander

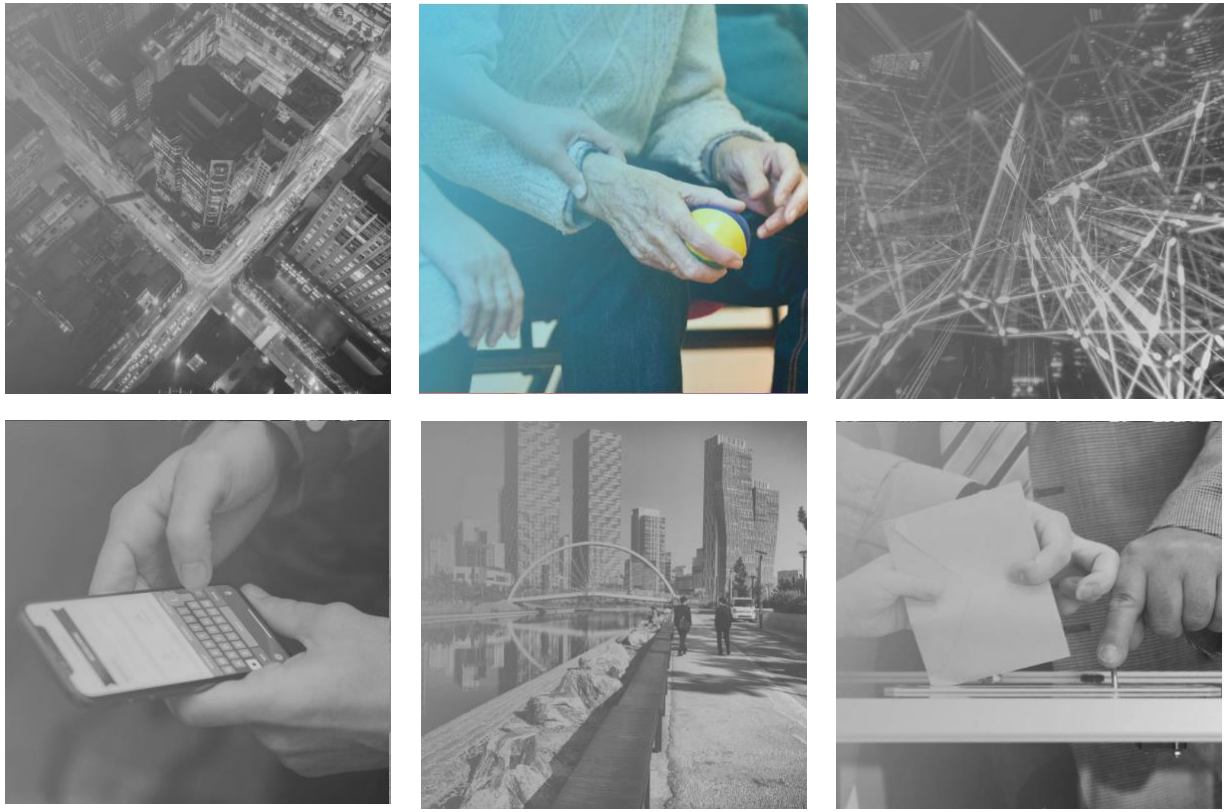


Problem:
Increasing numbers of anonymous attacks on IoT device networks

M-Sec Solution:
Hide and anonymize servers, create secure and authentication-mandatory techniques, protect communications between smart meters (water) and servers

Use Case 2: Well-being

Santander



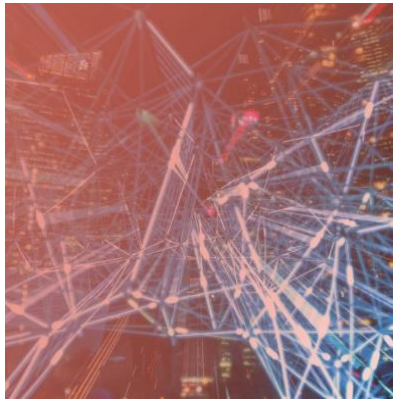
Problem:
Barriers against ageing populations participating society: falling, being unwell, needing regular medical checks or being isolated.

M-Sec Solution:
Using cloud & edge, mobile, tracking and medical devices so the elderly can self-manage and share their health status

Use Case 3: Environment Monitoring

Fujisawa






Problem:
The sensors and devices that help citizens optimize their environment, avoid traffic, adjust the air quality, and even stay safe when a natural disaster hits can be sensitive to attack

M-Sec Solution:
Encrypt and anonymise data collection and storage, use citizens as sensors, use the M-Sec marketplace to leverage the blockchain mechanism

Use Case 4: Hyper-connected citizen care

Fujisawa



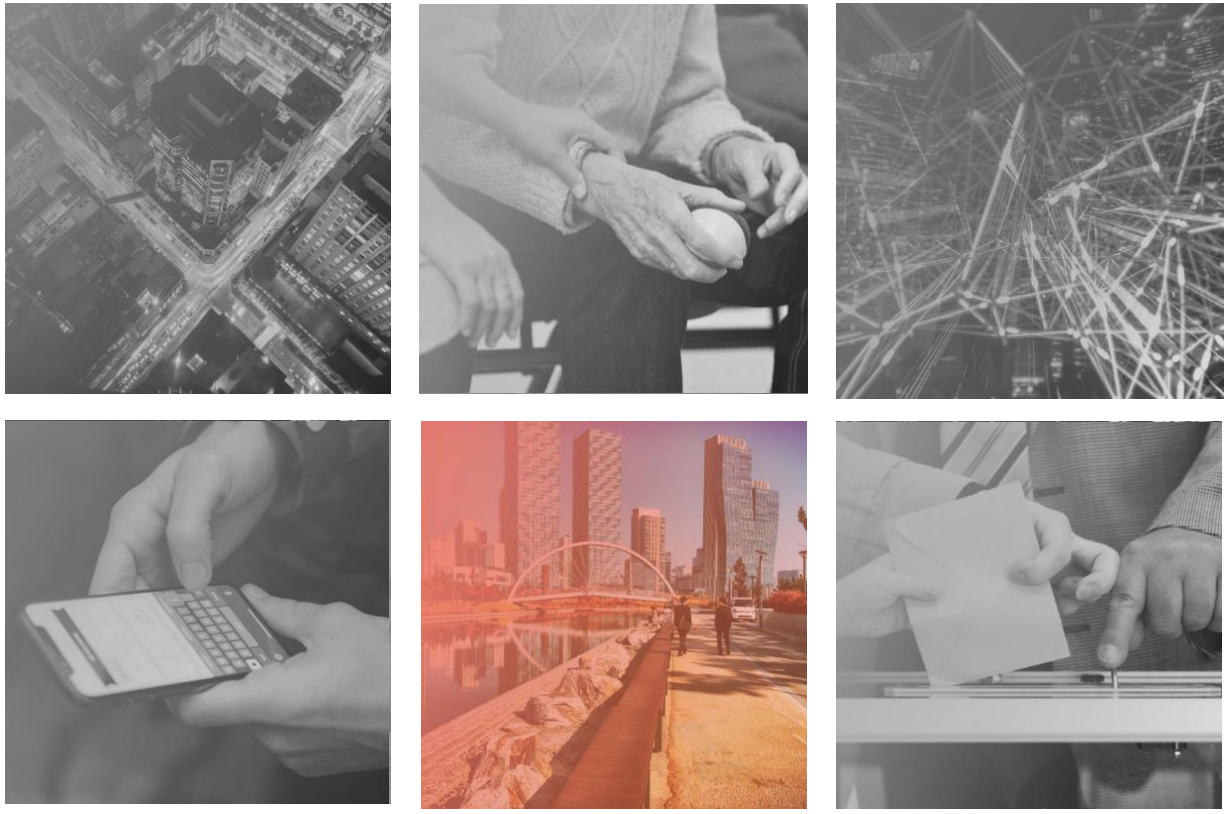



Problem:
Governments need support to provide a stable service, as well as ensuring the security and authenticity of data, and protecting personal information.

M-Sec Solution:
Collecting data from “human sensors”, encrypting and anonymising data, using the M-Sec marketplace

Use Case 5: A marketplace of IoT services

Fujisawa/Santander



Problem:
In the modern day there are few opportunities for citizens to play and connect, in the coldness and anonymity of the urban environment

M-Sec Solution:
Create playful solutions, such as novel walking traffic counter, playful air quality sensor, smart parking animation, etc., added to the city IoT network

Use Case 6: Citizens as sensor

Fujisawa/Santander



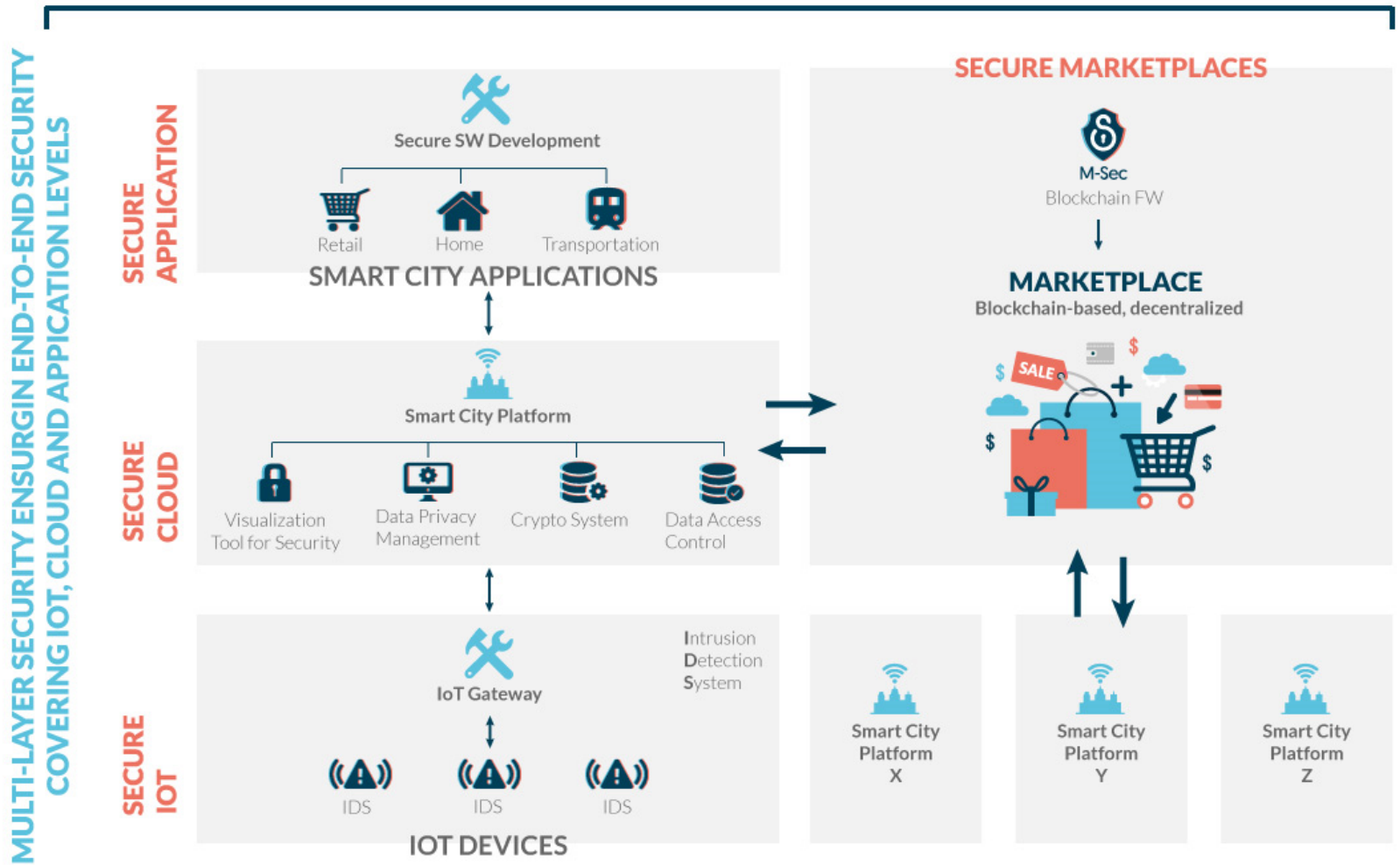



Problem:
Governments need support collecting more accurate and further reaching data sources on the state of the city and its services at any given time

M-Sec Solution: Through innovative smartphone apps, the citizen will be a “sensor”, sending data about incidents related to infrastructure, parks, traffic and other issues.

M-SEC ARCHITECTURE

Enabling Secure Sharing, Dealing and
Intereaction among Cities



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.

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).