CONFERENCE AMUSEC

08 APRIL 2021 – MARSEILLE

AMUSEC
AIX-MARSEILLE CYBER SECURITY FORUM

MEDICYNE

MEDICAL CYBERSECURE NETWORK

Cysec – Switzerland
Insight SiP – France

EUROSTARS PROJECT

CYSEC

Experts in Cyber-security, Cryptography, Offensive-defensive schemes in response to data leacks and hacks rise

- **Established in 2018**
  - ✓ Founded by actual CEO, COO and CTO
  - ✓ Core team of PhD and MSc from EPFL
  - ✓ Strong Industrial Background: ID Quantique, KUDELSKI, NAGRA, STMicroelectronics
  - ✓ Unique set of core competencies in
    - Cryptography : including post-quantum schemes
    - Secure Implementation: Operating System and Secure Execution Environment design
    - Offensive attacks: in-house lab for security assessments
  - ✓ Fab-less company

- **Locations**
  - ✓ Switzerland – HQ & Dev. team
    App. Development capabilities in Lausanne
    OS Development capabilities in Zurich

INSIGHT SIP

Experts in RF System-in-Package (SiP) and Antenna-in-Package (AiP) in response to ultra miniature wireless solution demand

- **Established in 2005**
  - ✓ Founded by actual CEO and CTO
  - ✓ Core team of PhD and MSc from National Semiconductor
  - ✓ Electromagnetic simulation, antenna design and µW & RF circuit theory skills
  - ✓ Unique set of design techniques & industrialization expertise
  - ✓ Fab-less company

- **Locations**
  - ✓ Europe – HQ & Technical team in Sophia-Antipolis ●
  - ✓ North America – Subsidiary in Denver ●
  - ✓ Asia – Sales office in Tokyo ●
  - ✓ Global network of distributors ●
  - ✓ Manufacturing – Taiwan & Philippines ●

Security Issues

Today's Situation

- **Medical devices being Hacked**
  - ✓ **Imaging Systems** like C-Arms, CT scanners and MRI's are considered to be one of the easiest targets
  - ✓ **Infusion Pumps** are medical devices that deliver fluids, including nutrients and medications, into a patient's body in a controlled manner. The FDA has logged 56.000 reports of negative incidents since 2005 with infusion pumps
  - ✓ **Pacemakers** that use wireless communications can be vulnerable to hacker attacks and could cause life-threatening malfunctions. The FDA has issued an alert about security flaws in 465.000 pacemakers that use radio frequency communications
  - ✓ **Patient Monitors** are used to check heartbeat, oxygen levels, and blood pressure. McAffee's security researchers have shown that it is possible to hack into the medical network through a patient monitor and falsify a patient's vital signs.

Today's Situation

- **Type of Attacks**
  - ✓ **Malware and ransomware** are often used by criminals to shut down individual devices.
  - ✓ **Data Breaches** give criminal access to health records.
- **Type of Security Issue**
  - ✓ **User Practice Issues** make up 41% of all security issues relating to medical IoT devices.
    - These include rogue applications and browser usage, including risky internet site visits.
  - ✓ **Outdated OS/SW** make up 33% of security issues
    - This includes running legacy OS, obsolete applications, and unpatched firmware.

HACK A MEDICAL DEVICE?

Famous example in 2011:
https://www.youtube.com/watch?v=avf5XF8yS60

Jay Radcliff a diabetic researcher shows on stage at the Black Hat how he was able to hack in his own Medtronic insulin pump and kill himself
https://venturebeat.com/2011/08/25/insulin-pump-hacker-says-vendor-medtronic-is-ignoring-security-risk

Since then, many other manufacturers and devices have shown vulnerabilities potentially killing patients

Devices targeted by researchers were insulin pumps and pacemakers

Johnson & Johnson

MiniMed®
Advancing solutions in diabetes

Medtronic

HOW TO HACK A MEDICAL DEVICE?

Example on the MiniMed pump

Hackers take advantage of the fact that the pump's communications aren't encrypted.

Methodology:

1. Reverse engineer the simple encoding and validity checks meant to protect the signal, enabling an attacker to capture the fob's commands.
2. Use readily available, open source software to program a radio that masquerades as a legitimate MiniMed remote
3. Send commands that the pumps will trust and execute.
4. After establishing that initial contact, control that radio through a simple smartphone app to launch attacks

https://www.wired.com/story/medtronic-insulin-pump-hack-app/

HOW TO HACK A MEDICAL DEVICE?

Example on an Insulin Pump

Barnaby Jack from McAfee succeeded in taking control of both an insulin pump's radio control and vibrating alert safety mode.

- Jack's hacking kit included a **special piece of software and a custom-built antenna** that has a scan range of 300 feet and for which the operator does not need to know the serial number.
- Medtronic insulin pumps, equipped with small radio transmitters allowing medics to adjust function, can become easy prey to this hacking invention that scans around for insulin pumps.
- Once the hacker sets foot in the targeted machine, he can then disable the warning function or/and make it disperse 45 days worth of insulin all at once – a dose that will potentially kill the patient.

https://resources.infosecinstitute.com/hcking-implantable-medical-devices/#gref

HOW TO HACK A MEDICAL DEVICE?

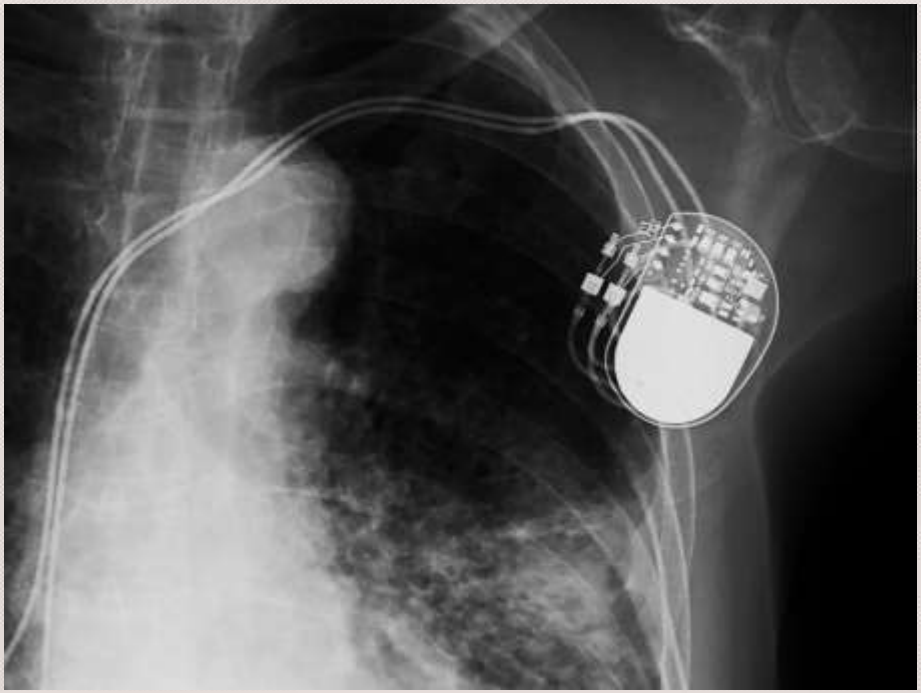
Example on Medtronic Pacemakers

The attack resembles those made against car key fobs

The researchers took advantage of vulnerabilities in Medtronic's software delivery network, which health care professionals use to tune implanted pacemakers: **authentication issues** and **lack of integrity checks**.

The researchers were able to install **tainted updates to take control of the programmers, and then spread to implanted pacemakers**

These issues could be solved with simple **"digital code signing“ — a way of cryptographically validating the legitimacy and integrity of software.**



https://www.wired.com/story/pacemaker-hack-malware-black-hat/

MEDICAL HACKS IN THE REAL WORLD

- **THERE HAVE BEEN NUMEROUS HACKS REPORTED ON MEDICAL DATA** (health records) targeting hospitals with hackers entering via the classic methods of hacking into IT infrastructure (phishing, etc.) getting access to emails and network servers and then installing a ransomware. Millions of patients are affected worldwide with their data disclosed and dozens of hospitals are reported victims of such incidents

https://www.modernhealthcare.com/cybersecurity/november-reported-healthcare-breaches-exposed-570000-patients-data

- **BUT THERE HAVE BEEN NO MEDICAL DEVICE SECURITY INCIDENTS.. YET**
  The FDA “has not received any reports of patient harm directly linked to a medical device cybersecurity incident.”
  Nothing.. publicly disclosed.
  However, everybody agree that the risks are high and the lack of incidents is due to.. Luck

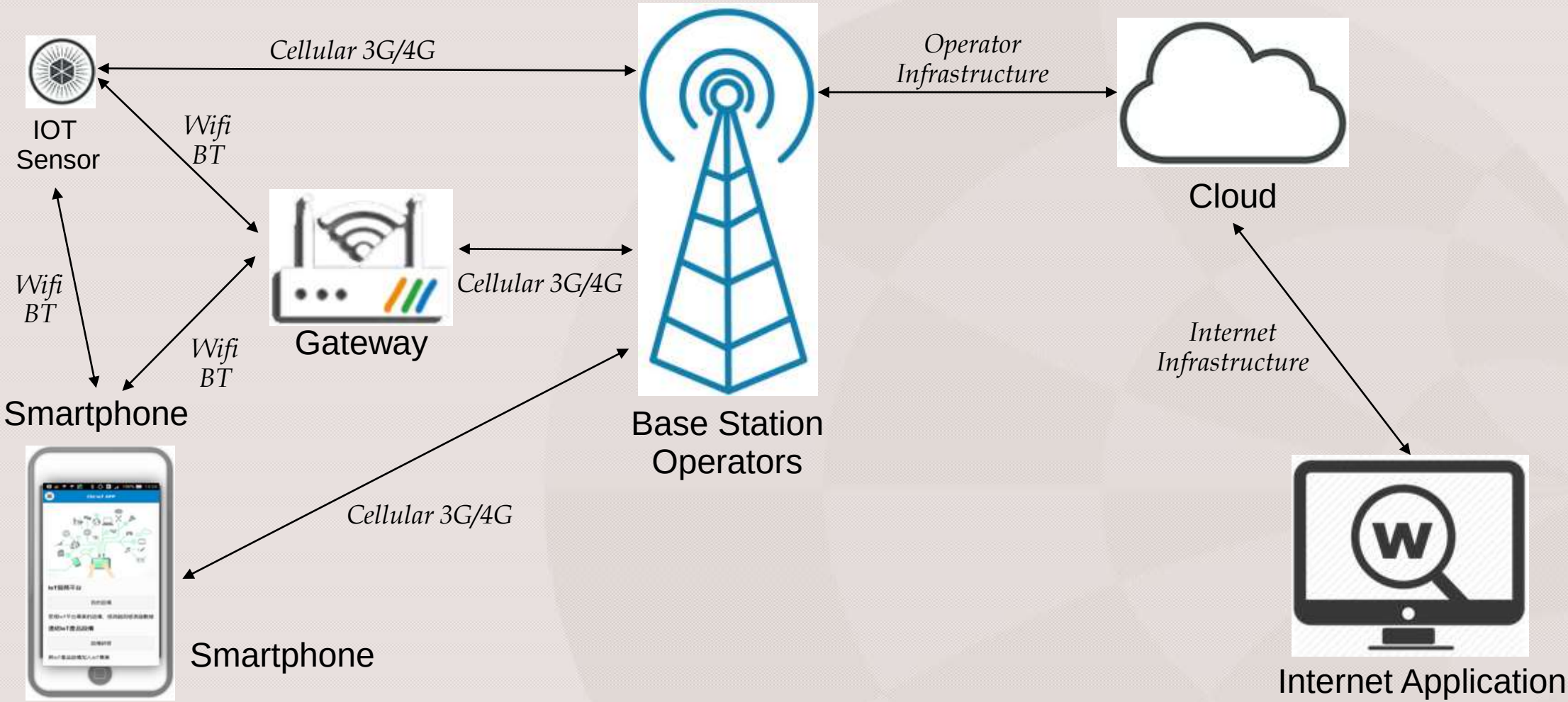
https://securityboulevard.com/2020/01/the-journey-to-better-medical-device-security-still-slow-still-bumpy/

Today's Situation

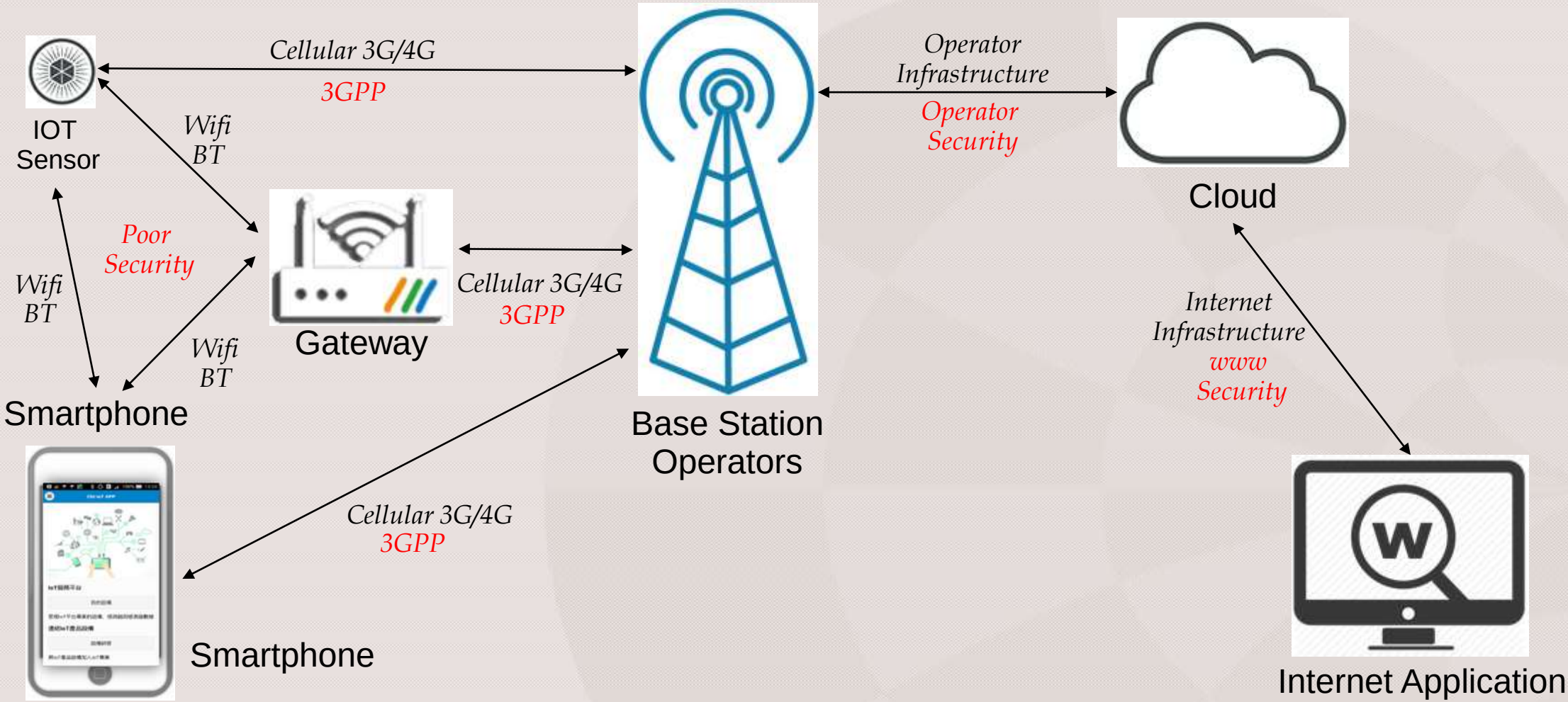
Medical IoT Devices	Level of Criticity to Attacks
Real Time Health Monitoring	Medium
Smart Vital Sensing for Rescue Services	Medium
Medical Asset Tracking	Low
Connected Pipettes	Low
Intravenous Pumps	High
ECG	Medium
Pacemakers	High
Glucose Monitoring	Medium
Insulin Pumps	High
Brain Stimulator	High
Smart Implanted Protheses	High
Smart External Protheses	Medium
Hearing Aids	Medium
Assisted Orthodontia	Low


problem
analysis
solution

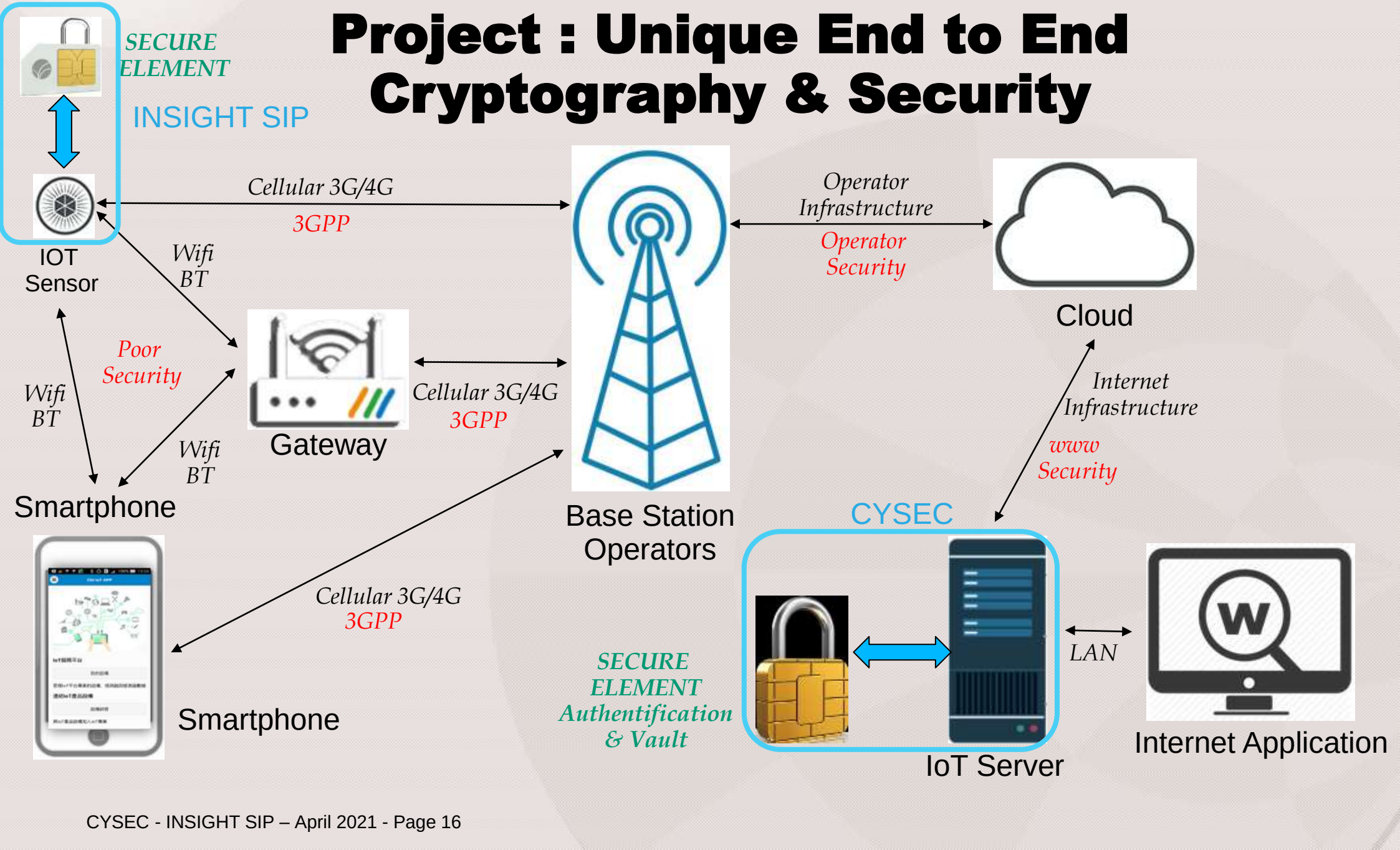
Today Situation



Today – Security is Managed at Different levels



Project : Unique End to End Cryptography & Security



Project MEDICYNE

- **Goal**
  - ✓ Provide END to END security for IoT data transfer and data storage

- **Main Features**
  - ✓ Security process independent of data transmission method (wires, wireless, Bluetooth, Wi-Fi, Cellular, other)
  - ✓ Secure element embedded inside miniature radio module in the IoT device
  - ✓ High level controls for crypto keys and data

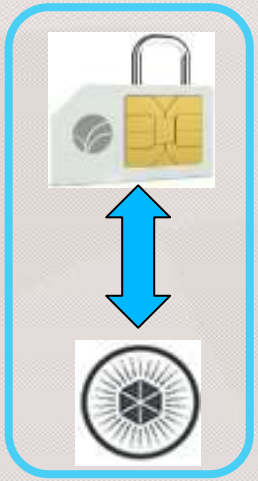
- **Market**
  - ✓ IoT for medical


SOLUTION

END to END Cryptography & Security

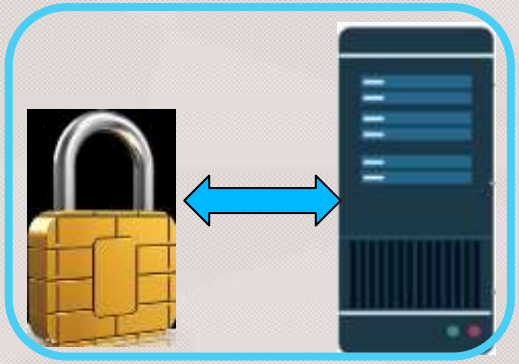
- ✓ IOT RF SIP Module including
  - Complete RF System – Radio, Matching, Filters & Antenna
  - Strong computing capacity
  - Large memory
  - Independent High-performance Secure Element

- ✓ IOT Data Sever including
  - Device Authentication – PKI
  - Key Management - KMS
  - Firmware Signature – FOTA
  - Software Integrity
  - Data Encryption
  - Secure Secret Storage
  - Secure Applications



SECURE ELEMENT

IOT Sensor



SECURE ELEMENT Authentification & Vault

IoT Server

SiP Module Advantages

- Designed by RF specialist with leading chipset manufacturer
- Offers fully embedded connectivity solutions

1 SoC Inside
- ✓ WLCSP wireless SoC and multiple analog and digital functions

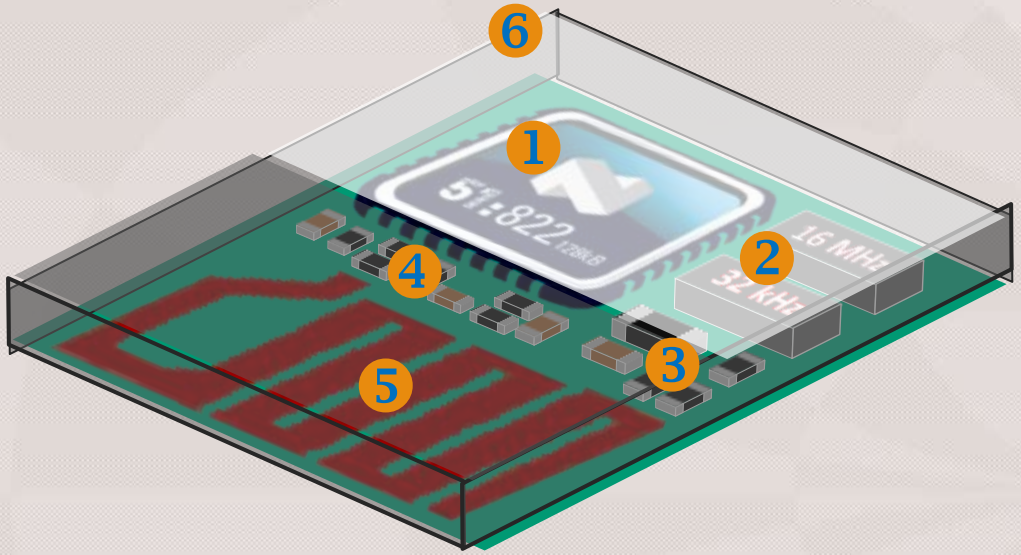
2 Both crystals included
- ✓ Radio & Synchronization
- ✓ Reduced power consumption

3 Power supply decoupling
- ✓ For both DC-DC enable or disable operating mode

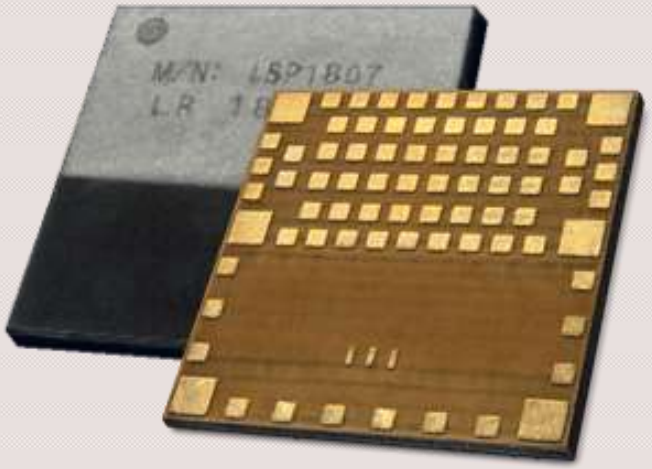
4 Antenna matching circuit

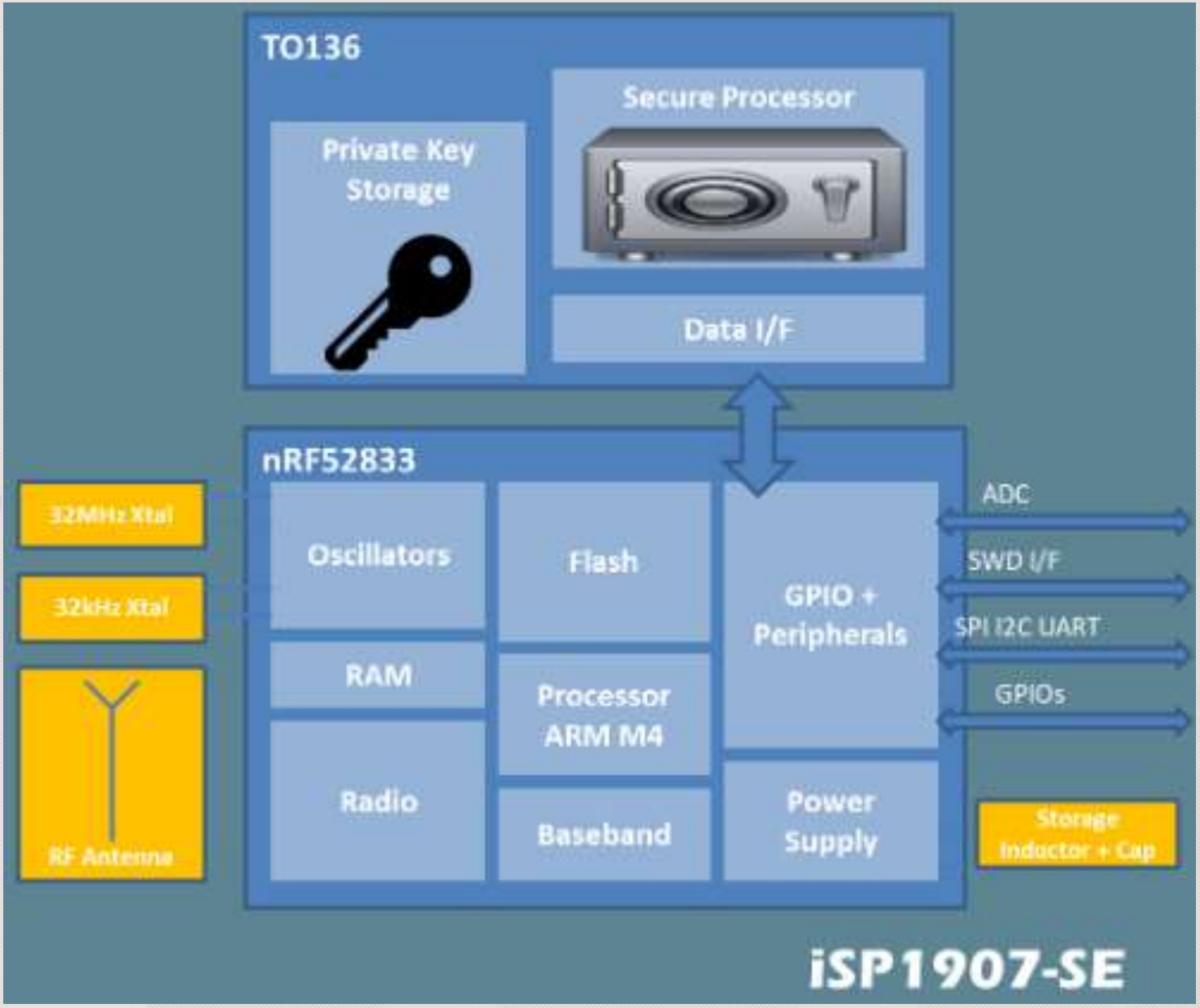
5 Integrated Antenna
- ✓ Proprietary integrated antenna
- ✓ Offering best reproducibility and best in class performance
- ✓ Relatively insensitive to environment

6 Integrated shielding avoiding external metallic covers
- ✓ Reduces height and size



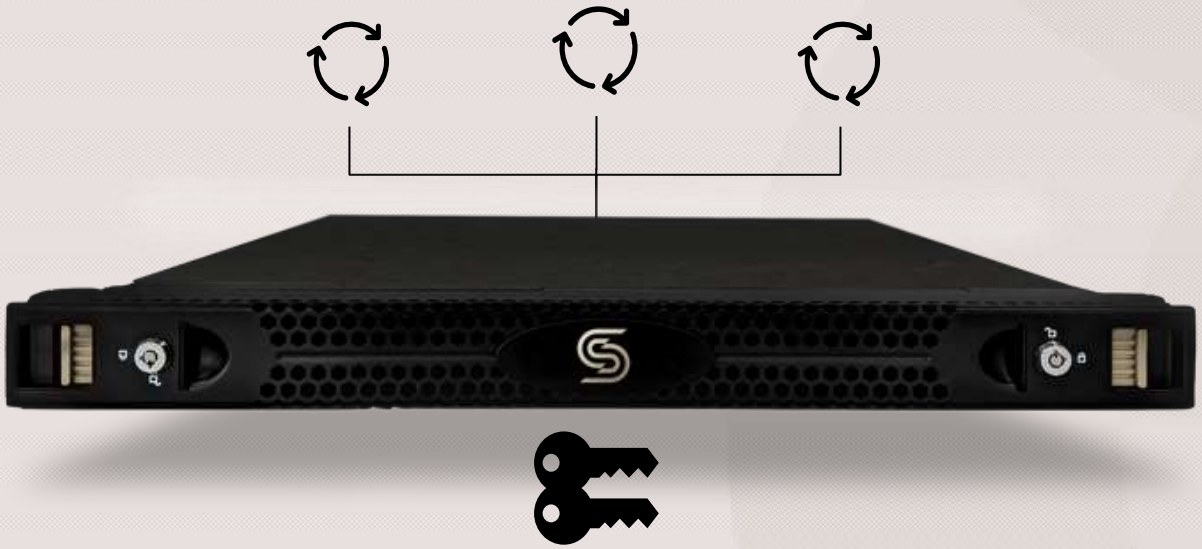
SECURE BLE RF MODULE





ARCA the 1st all-in-one Trusted Execution Environment

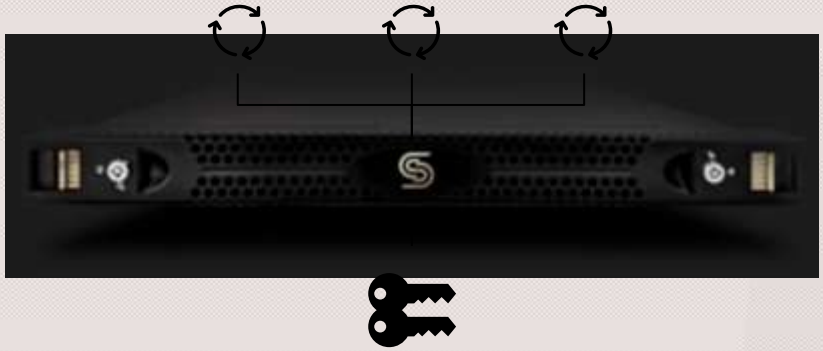
RUNNING
Critical Applications



STORING
Secrets in a Hardware Security Module (HSM)

- Simple “all-in-one” architecture
  - → More secure
- Easy to add / remove applications
  - → More flexible
  - → Easier and less costly deployment
- Easy to adapt crypto algorithms
  - → More Secure
  - → More sustainable

Applications in ARCA can be deployed either On Premises or As A Service (SaaS)



ON PREM

Own and physically host your machines and customize the set of applications according to your business and security needs

SaaS

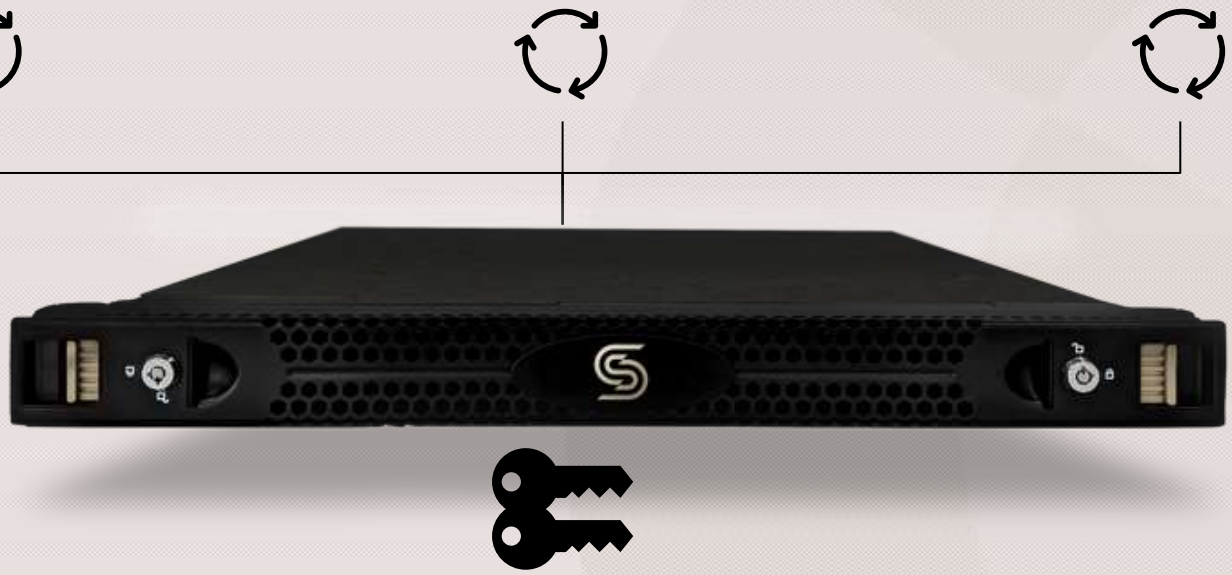
Enjoy the flexibility and the freedom of the cloud while still benefiting from the highest level of hardware security located in Switzerland

3 applications allowing a complete protection of connected devices

Authentication (PKI)

Firmware Signature (FOTA)

Key Management (KMS)



Keys stored in a Hardware Security Module (HSM)

- Device Authentication
- Software Integrity
- Data encryption
- Secure Secrets Storage
- Secured application

MEDICYNE PROJECT DETAILS

- **24 months R&D program Started August 2019**
- **Supported by Eurostars/Eureka European Program**
- **Steering Committee representing Companies specialized in Medical IoT solutions**
  - ✓ Insulin Pumps
  - ✓ Brain Simulators
  - ✓ Brain Fluids Pressure Control
  - ✓ Real Time Health Monitoring

MEDICYNE PROJECT
STEERING COMITEE

- ✓ Chris Barratt – Insight SiP, Sophia Antipolis, France
- ✓ Dr Riccardo Bonfanti – San Raffaele Hospital, Milan, Italy
- ✓ Dr Valeria Carobin – Franziskus Hospital Munster, Germany
- ✓ Yacine Felk – Cysec Lausanne, Swiss
- ✓ Pierre-Mikael Legris – PRYV, Morges, Swiss
- ✓ Kim Rochat – Medidee, Lausanne, Swiss

Any Question ?

... Feel free to contact us

michel.beghin@insightsip.com
yacine.felk@cysec.systems