How to transform a tiny medical device into a secure one in easy steps

Geert-Jan Schrijen, Georgios Selimis, Vincent van der Leest

IoT Security Foundation Conference 2019

INTRINSIC ID™

Intrinsic ID's work in developing and deploying unique microchip fingerprint technology for new markets is supported by

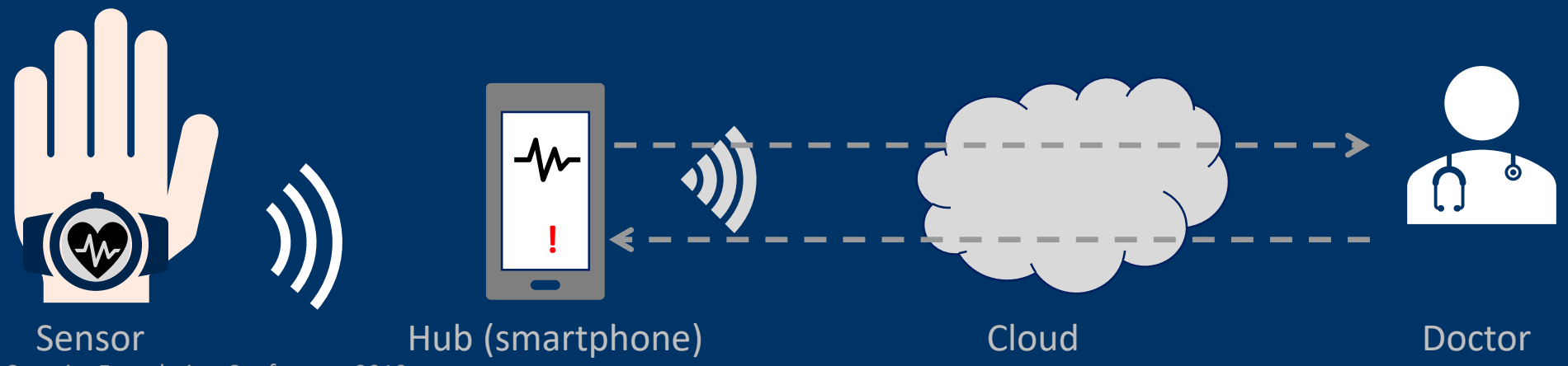
INSTET

A project funded under European Commission Project Grant Agreement ID: 811509

HORIZON 2020

Introduction

- Remote human body monitoring allows users to track their own conditions, eliminates need for repeated doctor visits and supports customized treatment plans
- High level architecture:
  - Sensor digitizes the input (e.g. heart rate, glucose level, blood pressure…) and pre-processes data
  - Data is transmitted to hub/gateway (e.g. smartphone) via local wireless connection such as Bluetooth Low Energy
  - Gateway forwards data to cloud service where Doctor can connect to, analyze the data, and communicate to the patient (e.g. via a smartphone app)



Advantages of devices bring security concerns

Medical devices in the past	Medical devices today
Devices are connected physically	Devices are connected wirelessly to patients
Obtained data is stored on paper	Data is stored on cloud
Devices are physical products	Devices include HW, SW and health information
Care is administrated at a healthcare location	Care is available to patients through apps
Physical access is needed to view health data	Health data can be accesses anywhere

Security concerns

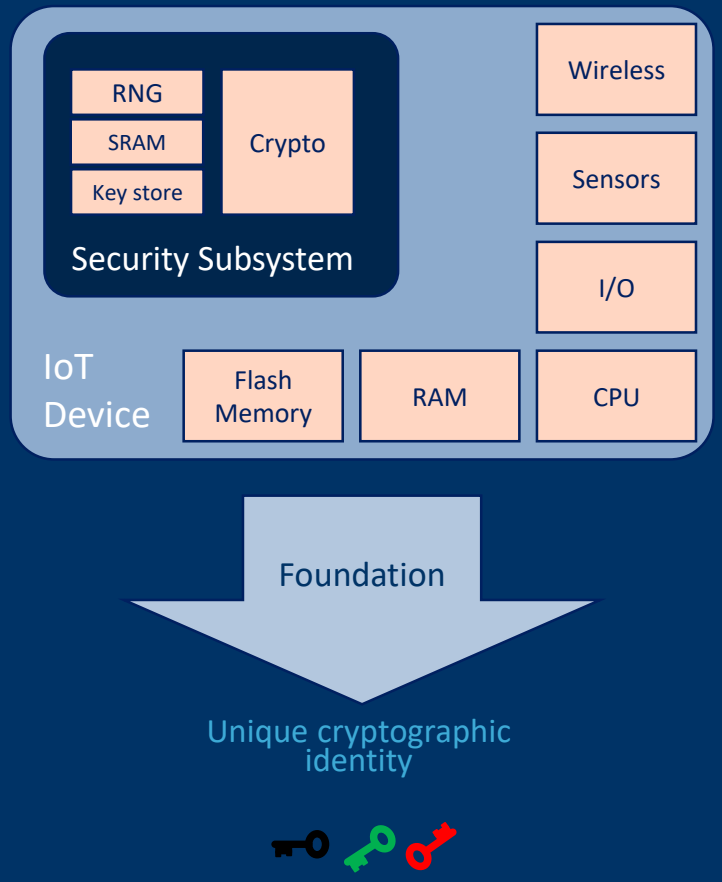
Patients could be harmed

Protected health data could be lost

Lost trust in connected devices

We need a security subsystem that…

- Protects the device's identity, manages cryptographic keys
- Operates in a separate security domain (isolated from user code and apps)
- Is universal; can be rolled out onto a wide variety of MCUs including retrofitting existing devices
- Provides cryptographic services for
  - Device security
  - Device authentication
  - Secure communication



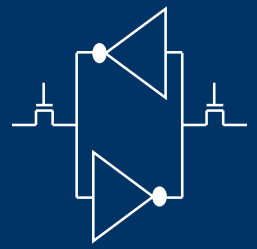
Foundation: from nanoscale variations to keys

1

Process Variation

Deep sub-micron variations in the production process give every transistor slightly random electric properties

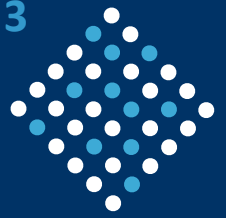
2



SRAM Start-up Values

When the SRAM is powered on this randomness is expressed in the start-up values (0 or 1) of SRAM cells

3



Silicon Fingerprint

The start-up values create a highly random and repeatable pattern that is unique to each chip

4

SRAM PUF Key

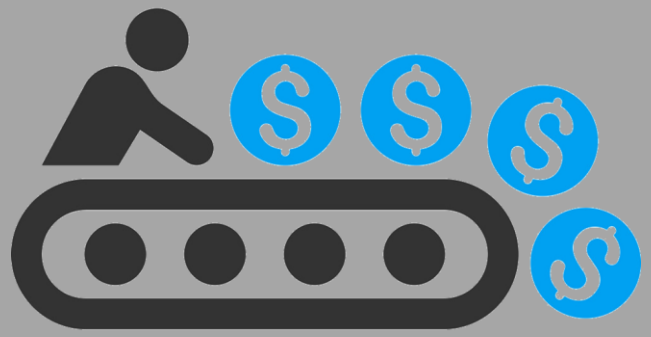
The silicon fingerprint is turned into a secret key that builds the foundation of a security subsystem

Device Security

Valuable IP and Sensitive Data should be protected from…

Theft & Reverse Engineering

Cloning

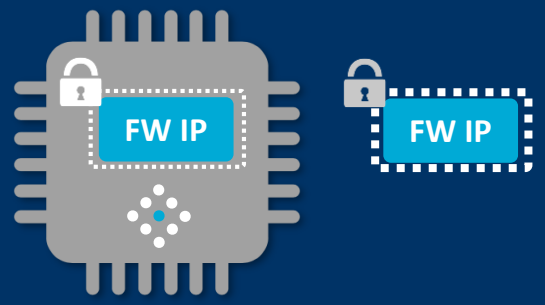


Over-Production

Device Security: IP Protection Based on SRAM PUF

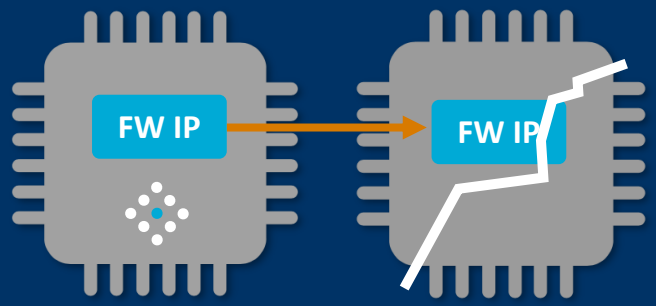
Anti-Reverse-Engineering/ Secure data storage

Firmware IP is encrypted with an SRAM PUF-derived encryption key that is locked to the hardware instance of the device.



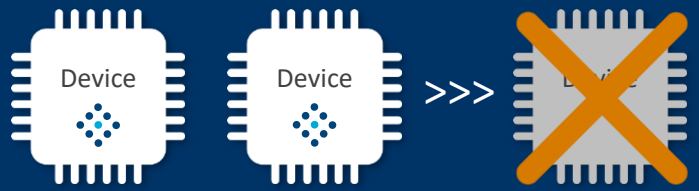
Anti-Cloning

When the firmware IP tied to a device by SRAM PUF is copied to other device instances, these rogue devices cannot unlock the IP and use it, since they have different hardware fingerprints.



Anti-Overbuilding

The number of SRAM PUF enrollments in devices can be limited to protect against overbuilding.



Device Authentication

Why is it important?

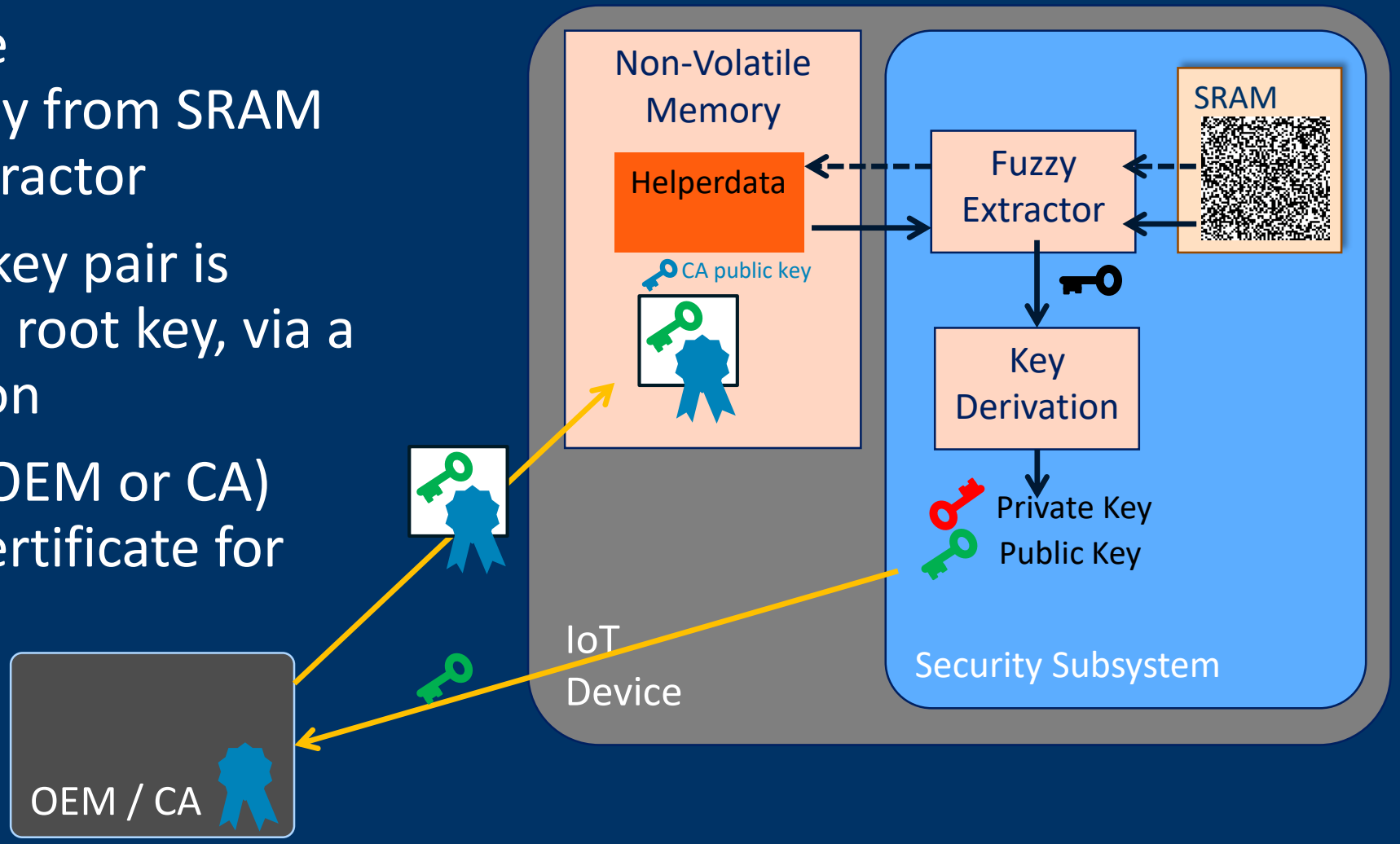
Medical Data is Sensitive & Private

M2M, no Human User

Passwords can be Stolen or Forged

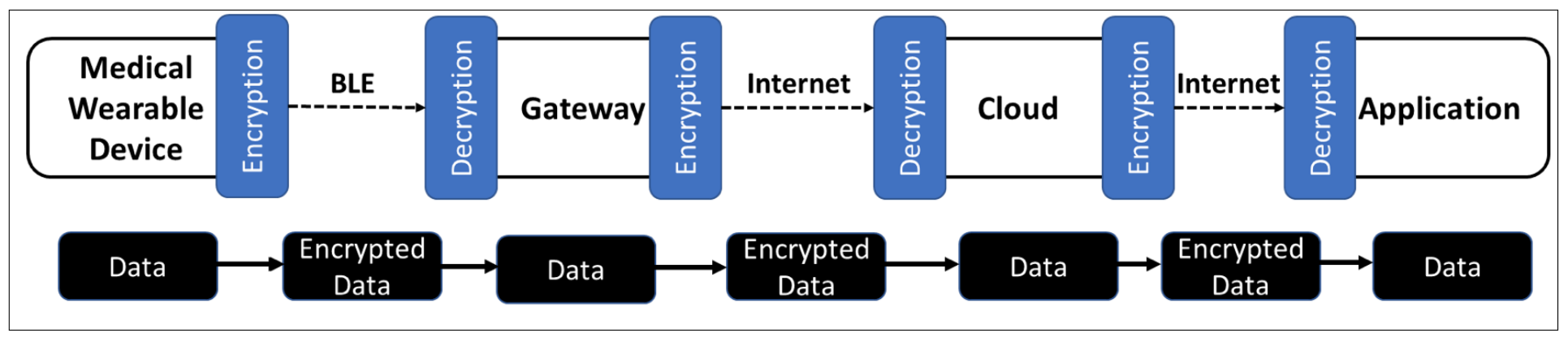
Authentication with strong chip identity

- Extract device-unique cryptographic root key from SRAM PUF using a Fuzzy Extractor
- Asymmetric identity key pair is derived from the PUF root key, via a key derivation function
- A trusted party (e.g. OEM or CA) creates an Identity Certificate for the device public key



Secure Communication

- A typical device to cloud system consists of multiple sequential links with various connectivity mechanisms between device and cloud service
- Every connectivity mechanism uses its own link encryption

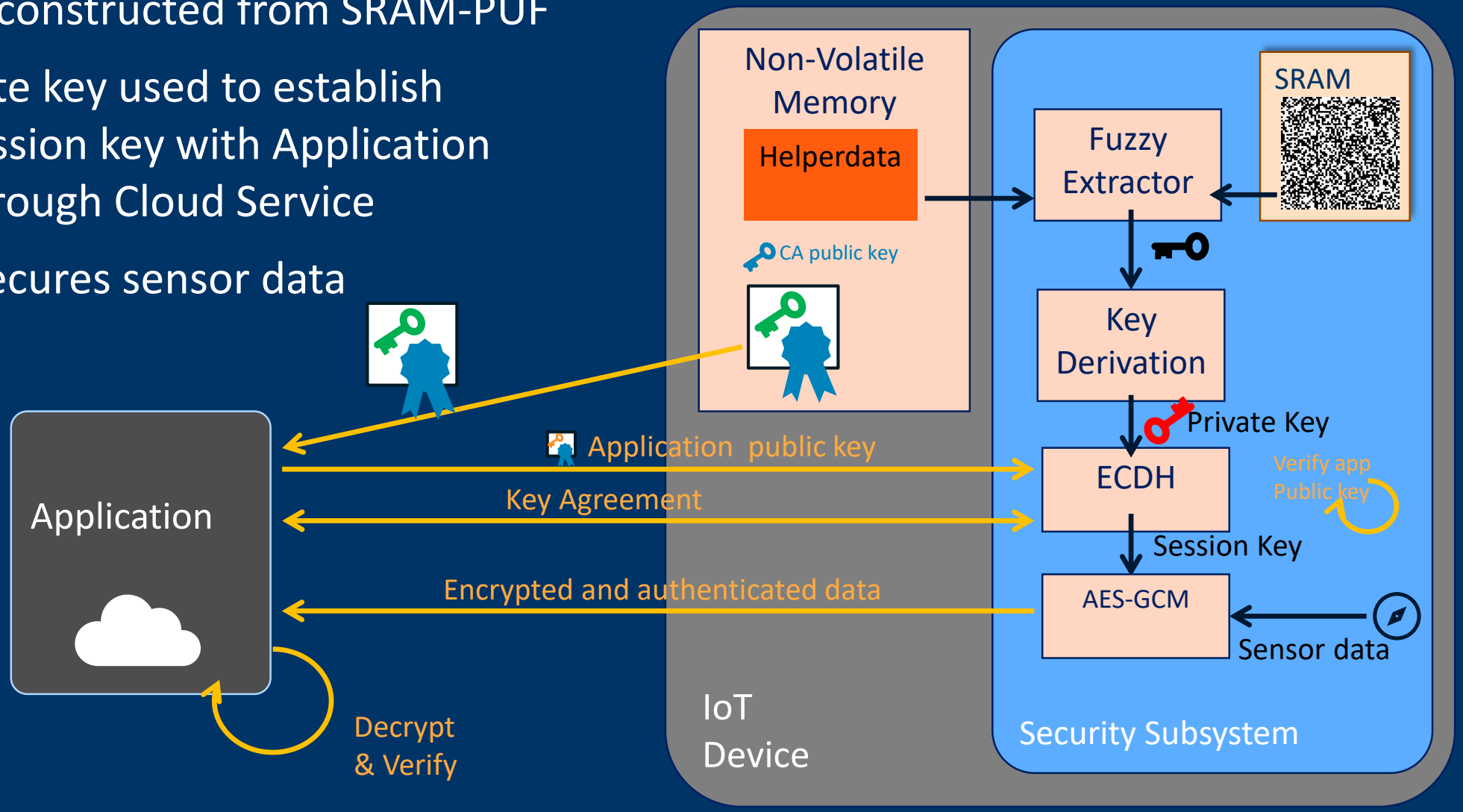


- End-to-end security is missing
  - Data can be intercepted, read and manipulated at the intermediate points
  - Recipient (doctor) cannot be assured that data is authentic
  - End-User privacy is not guaranteed

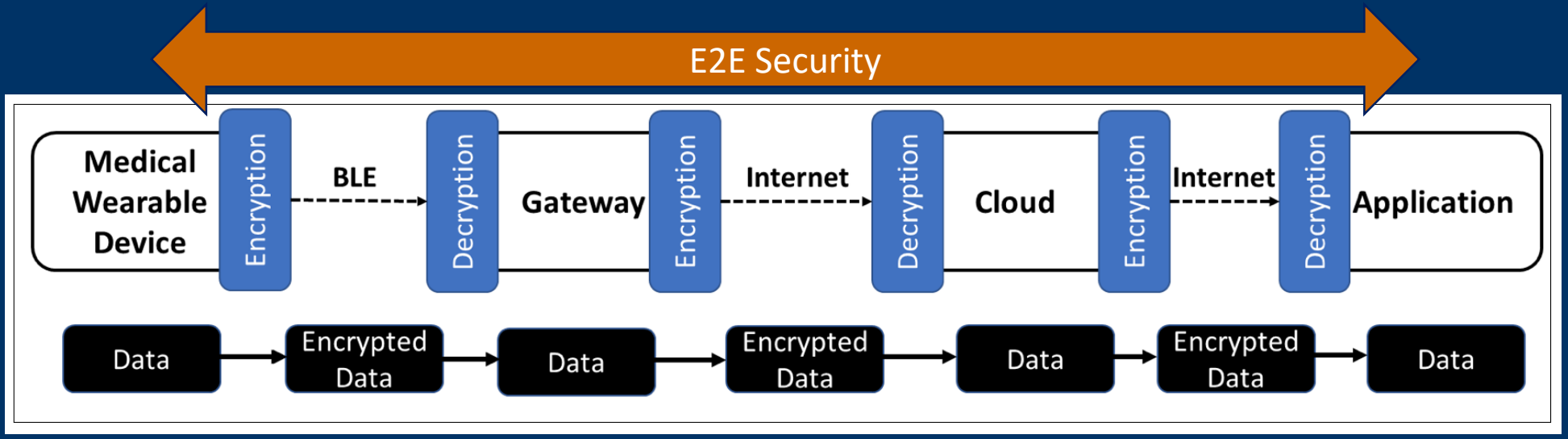
End-to-end secure channel is required!

End-to-End secure channel between Chip and Application

- Private key reconstructed from SRAM-PUF
- Derived private key used to establish symmetric session key with Application connected through Cloud Service
- Session key secures sensor data



Result: E2E Data Security



End-to-end security

- Data is passing through intermediate points encrypted
- Recipient (doctor) is assured that data is authentic
- End-User privacy is guaranteed

Extra steps to secure an existing device

Threat Analysis & Security Architecture

Leverage Chip Hardware

Secure Boot & Update

Disable Debugging

Conclusions

- The security of medical IoT devices need to be addressed on multiple levels: device security, secure authentication, communication and data security
- Starting point of such an architecture is a strong device security subsystem rooted in the hardware of the device
- Physical Unclonable Technology provides a flexible secure, cost-efficient way to bootstrap such a security subsystem and setup a strong digital device identity

Intrinsic ID's work in developing and deploying unique microchip fingerprint technology for new markets is supported by

INSTET

A project funded under European Commission Project Grant Agreement ID: 811509