ARCADIAN-IoT

Zero-touch Network-based Authentication of IoT Devices to Cloud services

1GLOBAL
formerly TRUPHONE

João Casal (Head of R&D)

15/09/2023

AGENDA

ARCADIAN-IoT

1. Intro / Motivation
   - eSIM unique positioning for IoT cybersecurity
   - Cellular Programmable Networks – Acting in a security sweet spot
2. Zero-touch Network-based Authentication of IoT devices to Cloud services
3. Q&A

1. eSIM UNIQUE POSITIONING FOR IoT CYBERSECURITY

1. eSIM UNIQUE POSITIONING FOR IoT CYBERSECURITY

SIM – What is it?

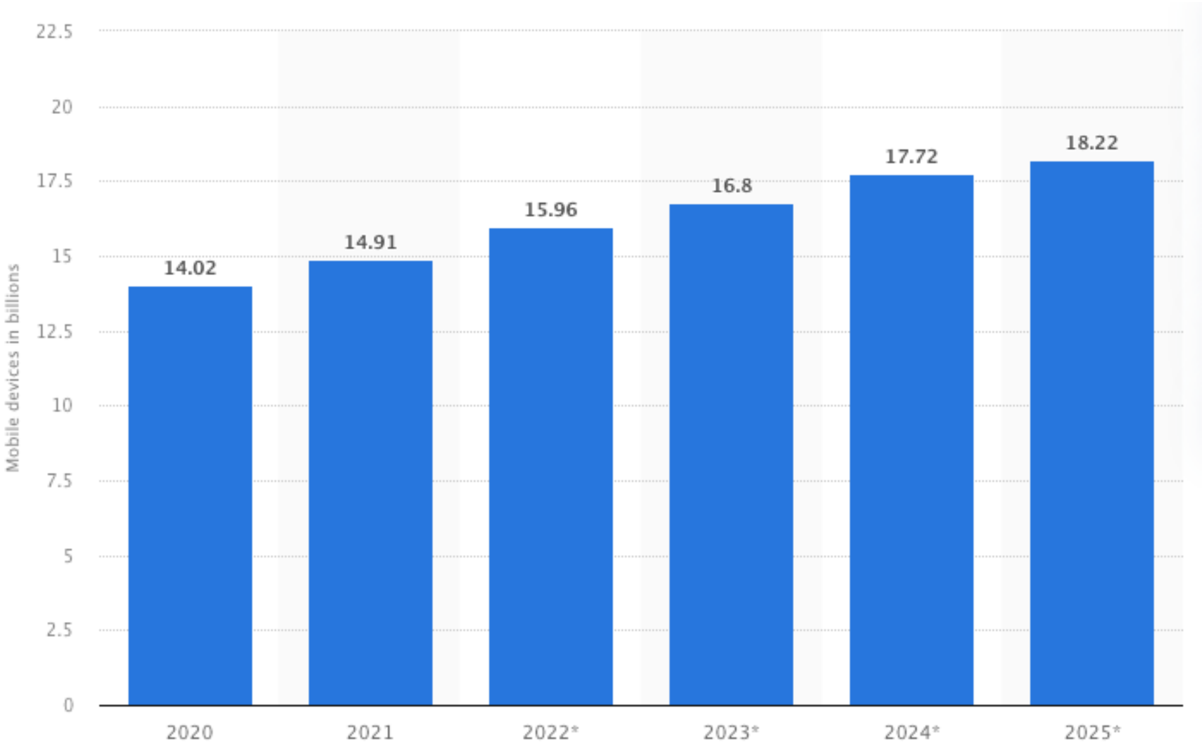
- **Subscriber Identity Module** – allows a cellular device to connect to a mobile operator
- **Hardware secure element** with **computing** and **storage** capabilities (from 8kb to 512kb)
- Stores phone number, contacts and text messages…
- … as well as **cryptographic material** and **unique identifiers** like authentication keys (Ki), at least one International Mobile Subscriber Identity (IMSI), mobile country codes (MCC)

now 1GLOBAL

1. eSIM UNIQUE POSITIONING FOR IoT CYBERSECURITY

SIM as a security enabler proven by billions' devices

All cellular devices have a dedicated hardware (UICC) with sensitive information and security functions



In future networks (5G, 6G,…) new SIM forms will be there with new security functions

Number of mobile devices worldwide 2020-2025
Published by Federica Laricchia @ statista , Mar 10, 2023

https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/

1. eSIM UNIQUE POSITIONING FOR IoT CYBERSECURITY

Is the SIM really secure or… it simply doesn't protect anything relevant for attackers? (network identifiers – authorization to access a network provider services)

If one attacker would compromise a SIM, he/she could:

Get mobile internet for free… or for selling it in the black market

(if SIM processes were easy to compromise mobile operators wouldn't be using for over 30 years now)

Impersonate a person in phone calls and SMSs

(if SIM processes were easy to compromise lawful interception – wiretrap a suspect person calls with court orders - would not be valid/relevant)

Get bank operations confirmation codes from the subscriber

(if SIM processes were easy to compromise banks would not rely on it for its operations)

Access public services, having access to information on personal incomes, household address, family member names, …

(if SIM processes were easy to compromise countries/states would not rely on it for the citizens identification in public services)

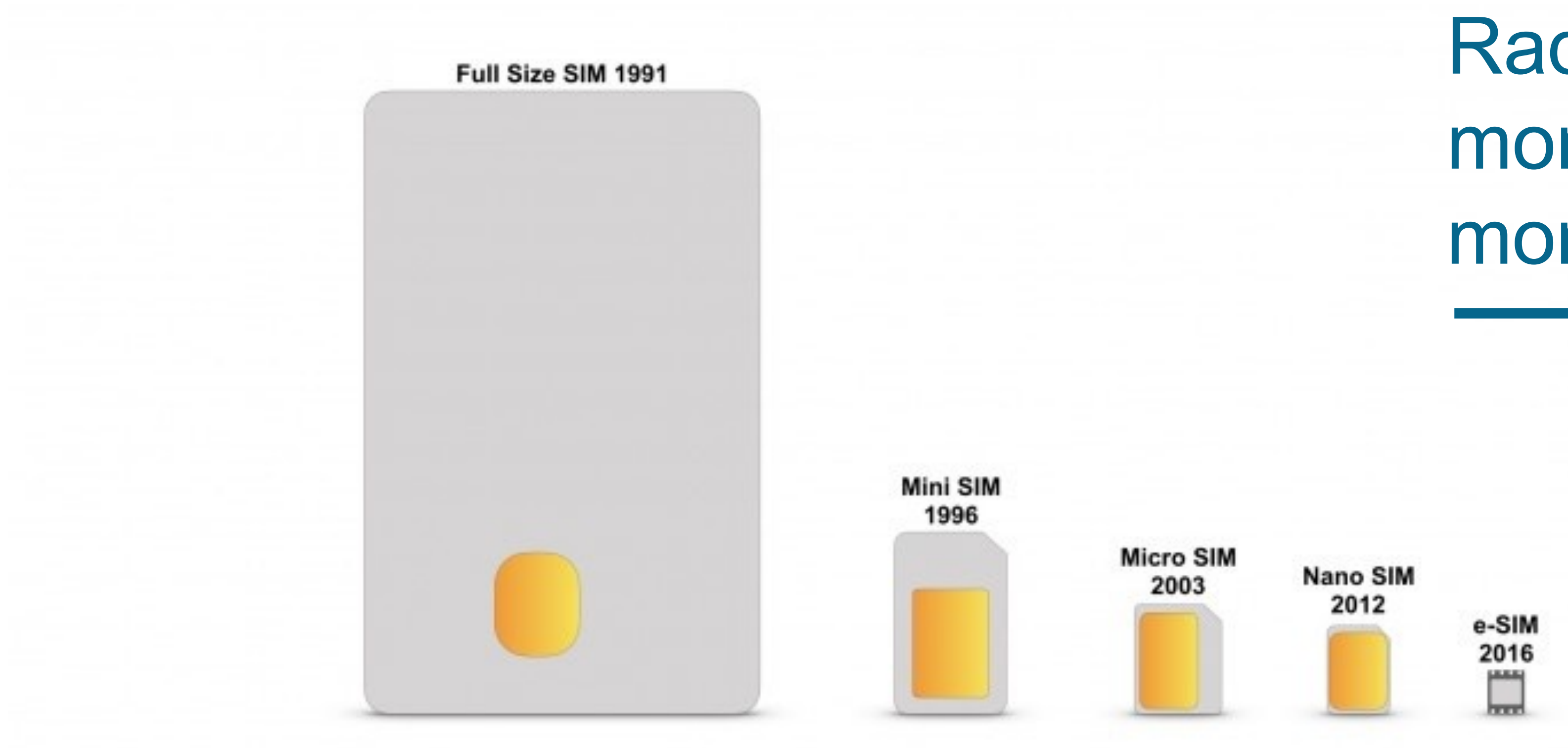
Can we accept that the SIM is hard to compromise?

↓

Some (GSMA) claim that it can be a Root of Trust

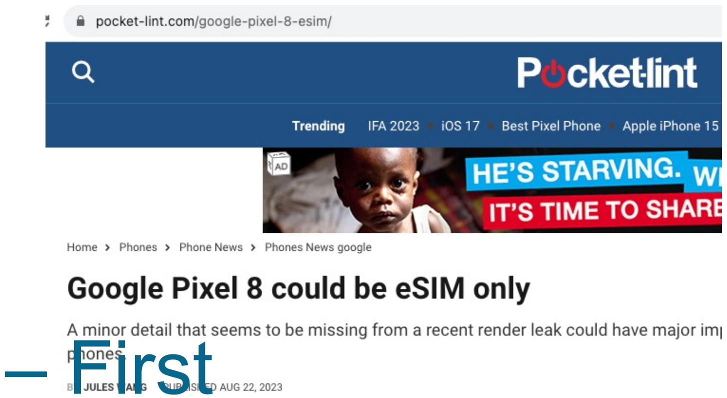
1. eSIM UNIQUE POSITIONING FOR IoT CYBERSECURITY

SIM family: identifying network customers since 1991



Lower size, less plastic

Radical innovation – more automation, more security



pocket-lint.com/google-pixel-8-esim/

Google Pixel 8 could be eSIM only

A minor detail that seems to be missing from a recent render leak could have major imp phones

BY JULES WANG PUBLISHED AUG 22, 2023

2022 – First eSIM-only iPhone (14)

Image from https://m.gsmarena.com/glossary.php3?term=sim

1. eSIM UNIQUE POSITIONING FOR IoT CYBERSECURITY

eSIM – Evolving towards more security

- If the SIM provides secure identity and stores authentication secrets**, being possible to remove it and use it in different devices is questionable** – PIN and PUK codes are used for security but, as passwords, are not the best approaches.

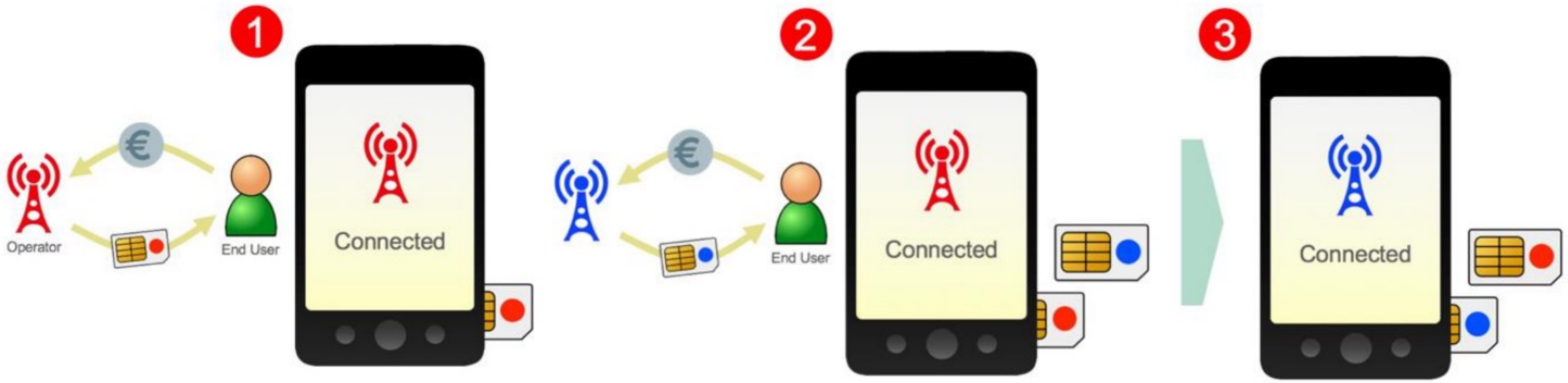
- Being soldered to the board the **eSIM ensures more security in the identity of subscribers** forcing a 1-1 relation between a device and a subscriber (the same happens with iSIM, integrated in the chipset)

1. eSIM UNIQUE POSITIONING FOR IoT CYBERSECURITY

ARCADIAN-IoT

eSIM today – From manual SIM insertion to Remote SIM Provisioning

The person interaction with the SIM



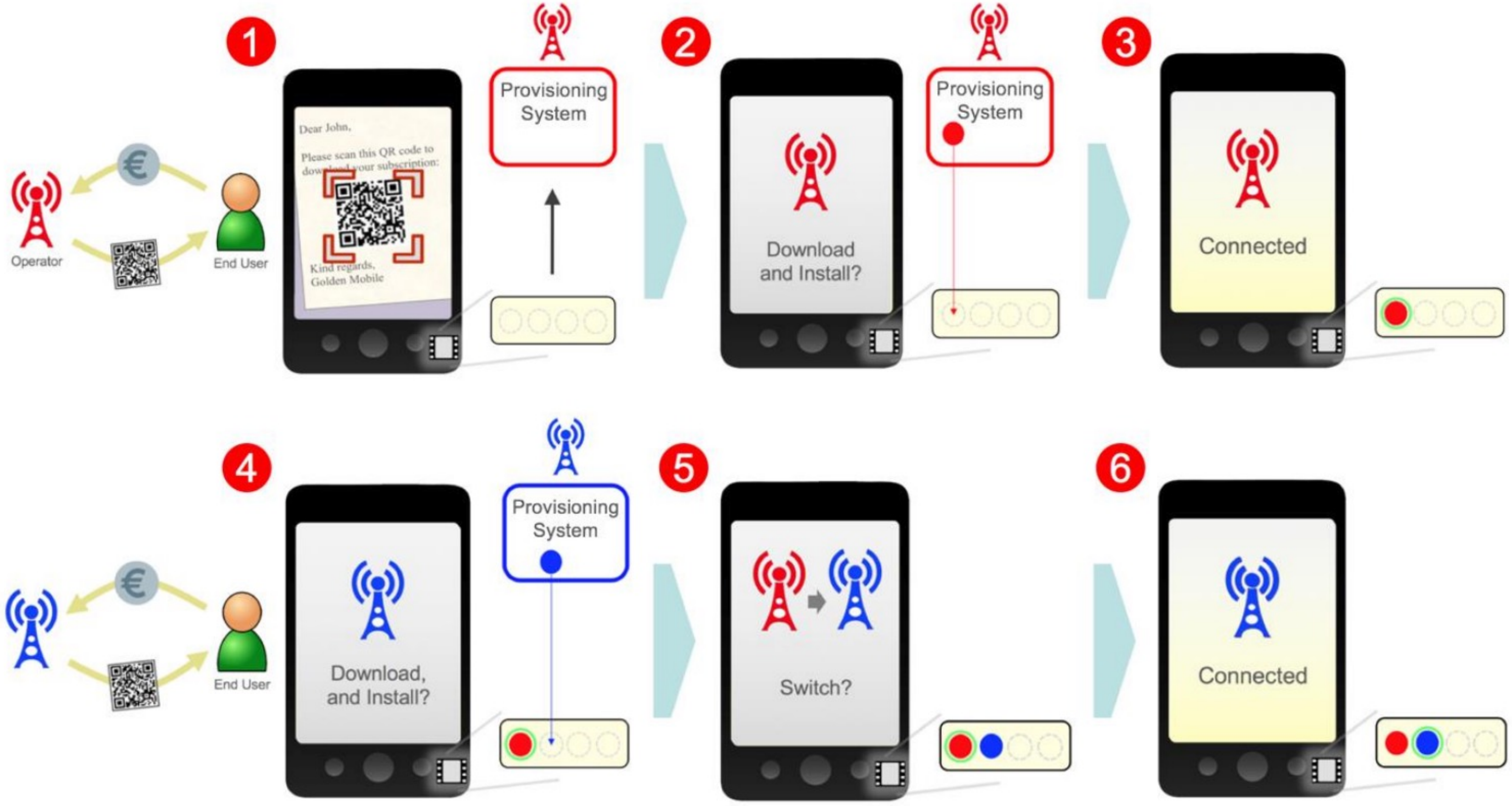
https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf

1. eSIM UNIQUE POSITIONING FOR IoT CYBERSECURITY

ARCADIAN-IoT

eSIM today – From manual SIM insertion to Remote SIM Provisioning

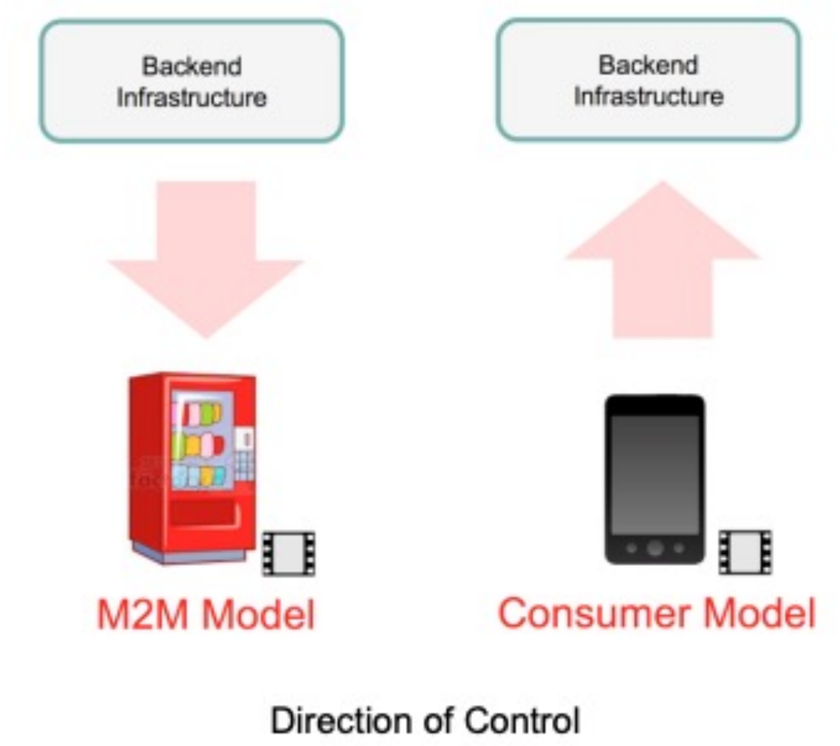
The person interaction with the eSIM



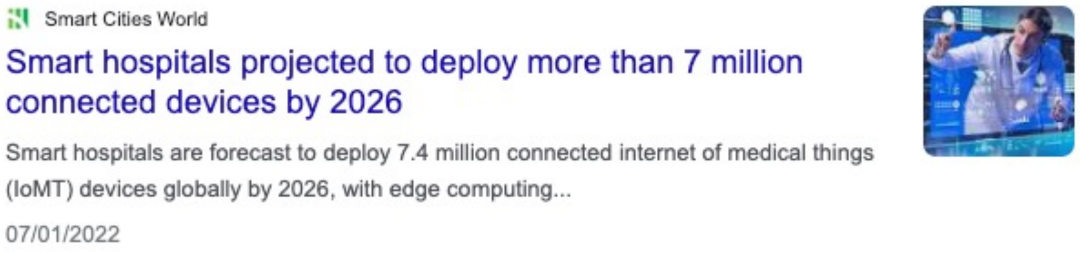
https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf

1. eSIM UNIQUE POSITIONING FOR IoT CYBERSECURITY

eSIM – Now think on IoT



https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf


Smart Cities World

Smart hospitals projected to deploy more than 7 million connected devices by 2026

Smart hospitals are forecast to deploy 7.4 million connected internet of medical things (IoMT) devices globally by 2026, with edge computing...

07/01/2022

Imagine these hospitals deployments with SIM…

… and with eSIM.

(complexity, costs, velocity, …)

Now imagine the deployment of a smart factory with hundreds of devices…

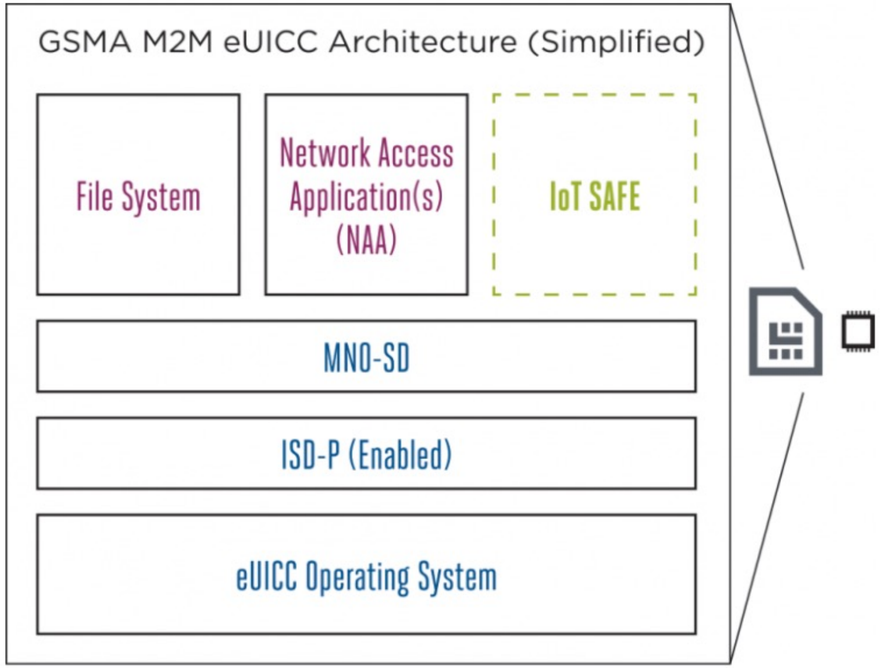
eSIM vs WiFI…

*(complexity, costs, velocity, **security**, …)*

1. eSIM UNIQUE POSITIONING FOR IoT CYBERSECURITY

ARCADIAN-IoT

GSMA IoT SAFE – Chip to Cloud Security


GSMA M2M eUICC Architecture (Simplified)
File System
Network Access Application(s) (NAA)
IoT SAFE
MNO-SD
ISD-P (Enabled)
eUICC Operating System

IoT SAFE SIM Architecture (Example)

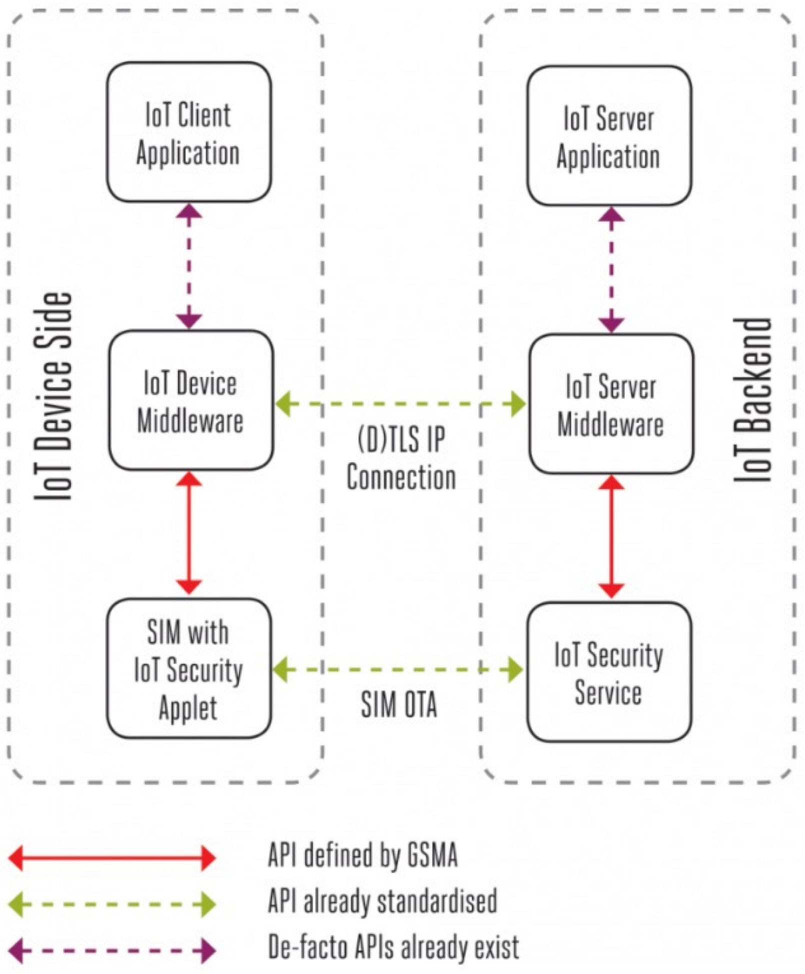
- Uses the SIM as a **mini 'crypto-safe**' inside the device to securely establish a (D)TLS session with a corresponding application cloud/server
- Compatible with **all SIM form factor**: SIM, eSIM, iSIM.
- Provides a **common API for the highly secure SIM** to be used as a hardware 'Root of Trust' by IoT devices
- Helps **solve challenge of provisioning millions** of IoT devices

https://www.gsma.com/iot/iot-safe/

1. eSIM UNIQUE POSITIONING FOR IoT CYBERSECURITY

ARCADIAN-IoT

GSMA IoT SAFE – Chip to Cloud Security



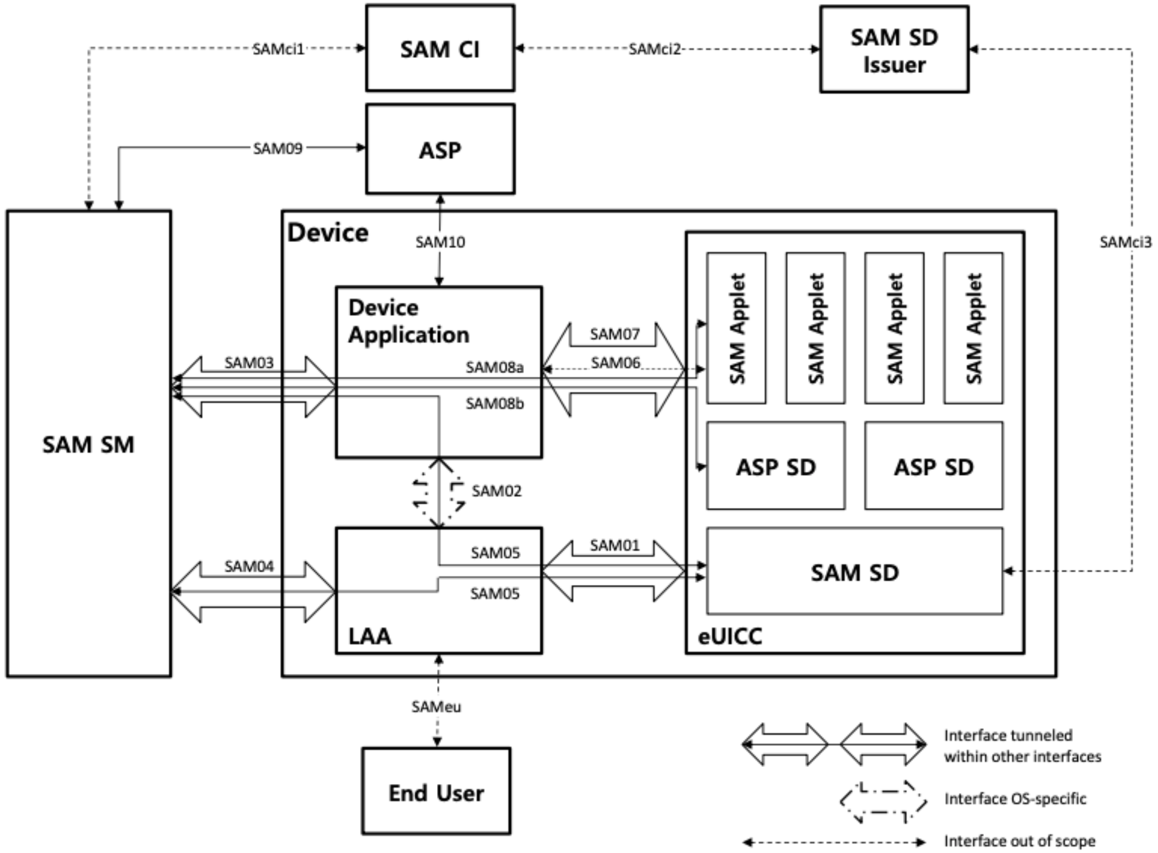
- IoT devices to securely perform **mutual (D)TLS authentication to a server** using either asymmetric or symmetric security schemes
- **IoT devices to compute shared secrets** and **keep long-term keys secret**
- Provisioning and credential lifecycle management from a remote IoT security service

1. eSIM UNIQUE POSITIONING FOR IoT CYBERSECURITY

GSMA SAM – Secured Applications for Mobile

- Cellular connected devices using secured applets within an eUICC paired with applications running on the device itself.

- Potential use cases:
  - Banking applications; Transport applications; Identity applications



https://www.gsma.com/newsroom/wp-content/uploads//SAM.01-v1.0.pdf

1. eSIM UNIQUE POSITIONING FOR IoT CYBERSECURITY

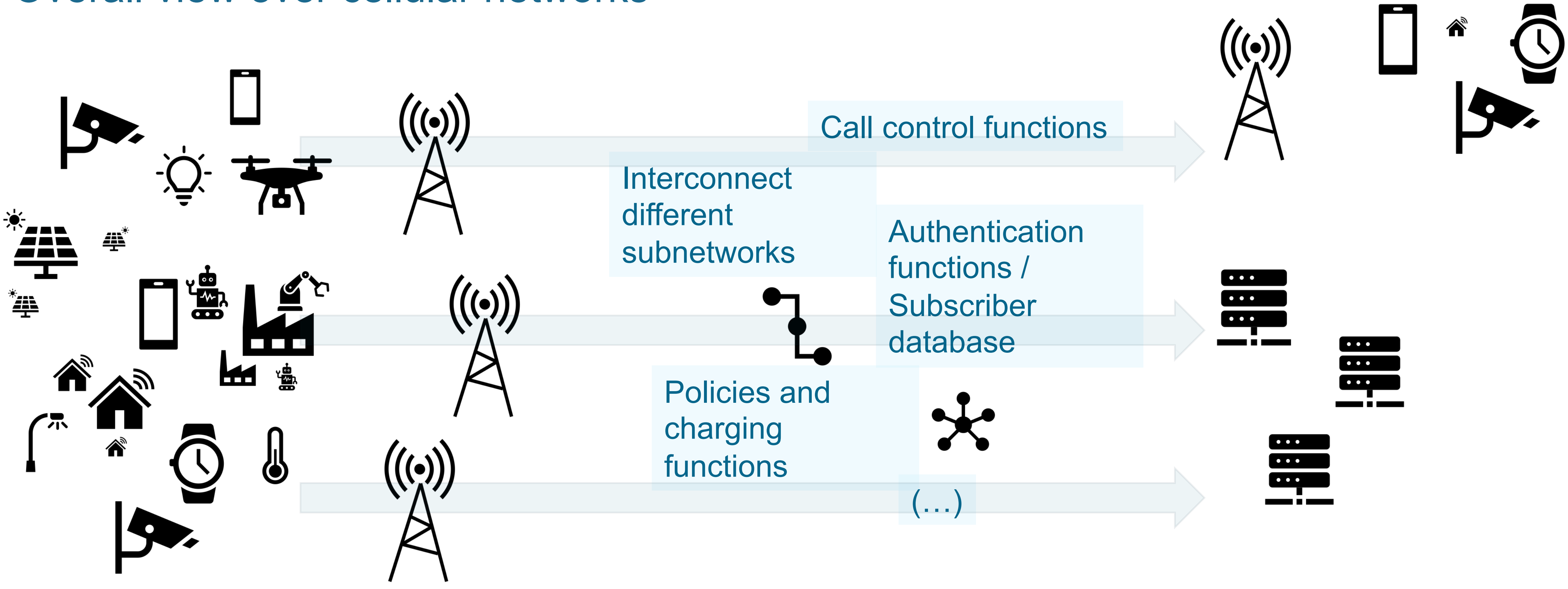
TLDR : Why eSIM has an unique positioning for IoT cybersecurity?

- **SIM is a proven secure element in use by +10 billion devices** for identity management, comms confidentiality and authentication – any innovation has a huge impact potential.
- **eSIM** builds on the proven hardware secure element features, adding **automation and security**
- Standardization is paving the way to bring **new security functions to the future SIMs** (GSMA IoT SAFE and SAM)

2. CELLULAR PROGRAMMABLE NETWORKS – ACTING IN A SECURITY SWEET SPOT

2. CELLULAR PROGRAMMABLE NETWORKS – ACTING IN A SECURITY SWEET SPOT

Overall view over cellular networks



Call control functions

Interconnect different subnetworks

Authentication functions / Subscriber database

Policies and charging functions

(…)

Devices

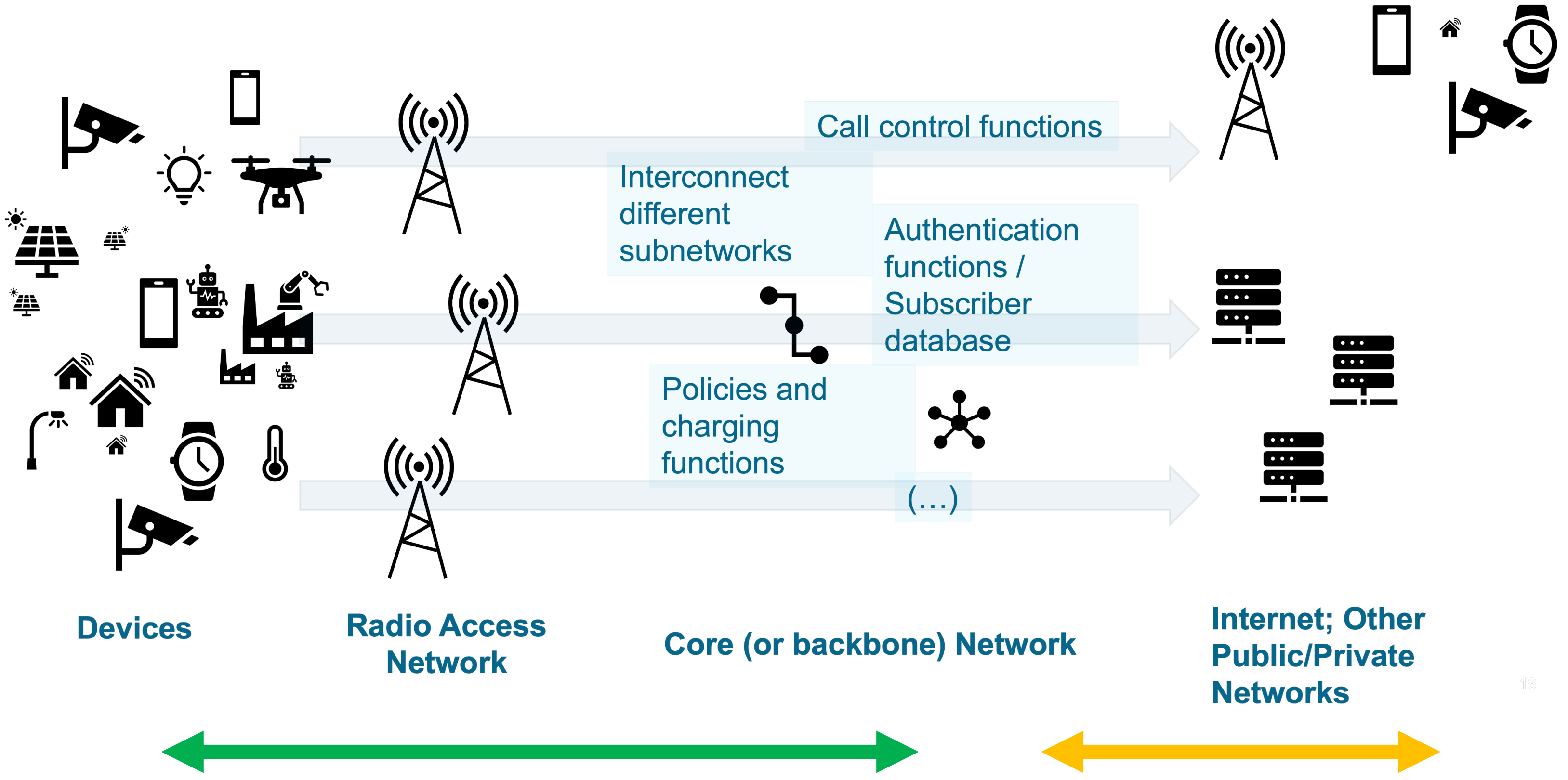
Radio Access Network

Core (or backbone) Network

Internet; Other Public/Private Networks

2. CELLULAR PROGRAMMABLE NETWORKS – ACTING IN A SECURITY SWEET SPOT

Security between devices/subscribers (SIMs) and the Core Network



Call control functions

Interconnect different subnetworks

Authentication functions / Subscriber database

Policies and charging functions

(…)

Devices

Radio Access Network

Core (or backbone) Network

Internet; Other Public/Private Networks

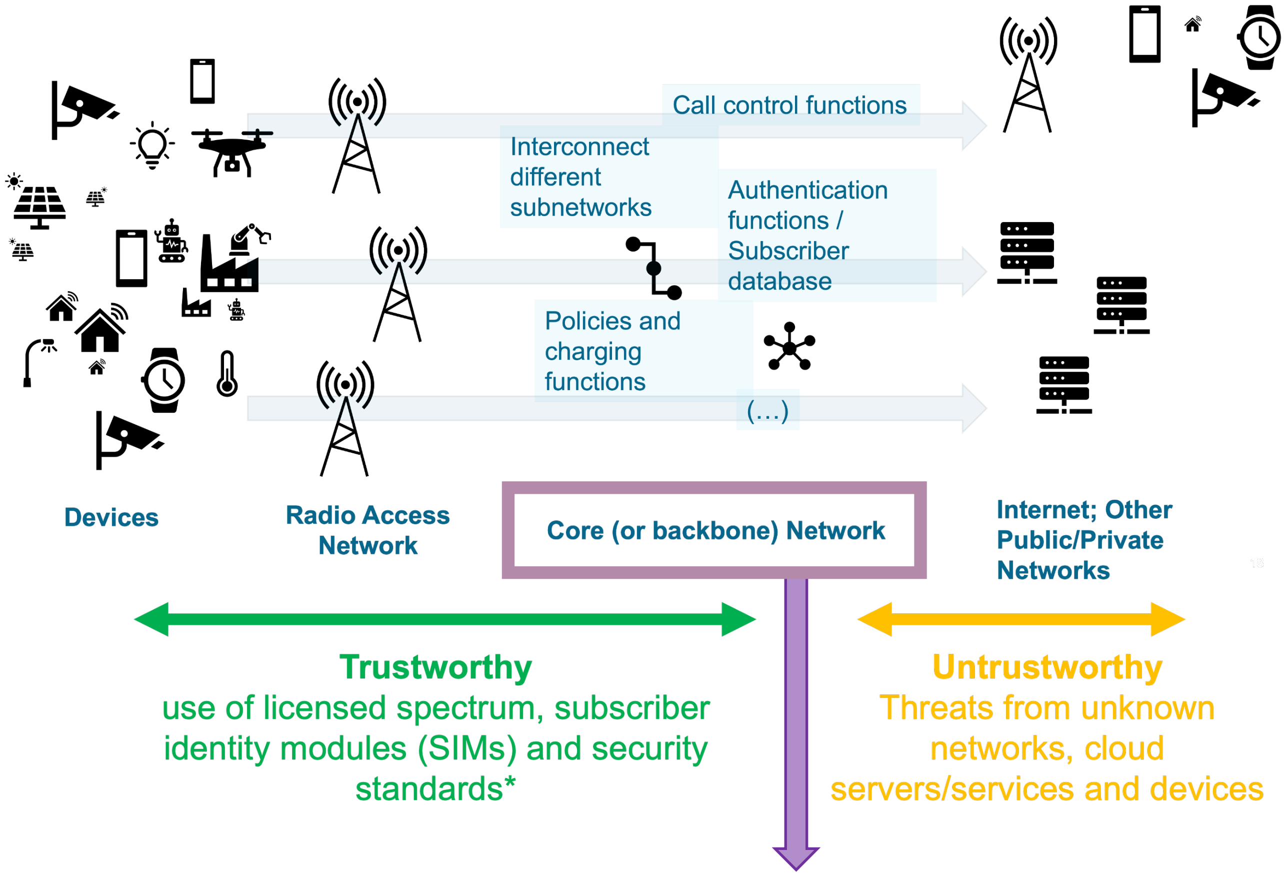
Trustworthy
use of licensed spectrum, subscriber identity modules (SIMs) and security standards*

Untrustworthy
Threats from unknown networks, cloud servers/services and devices

2. CELLULAR PROGRAMMABLE NETWORKS – ACTING IN A SECURITY SWEET SPOT

ARCADIAN-IoT

Core Network elements relevance for cybersecurity



Call control functions

Interconnect different subnetworks

Authentication functions / Subscriber database

Policies and charging functions

(…)

Devices

Radio Access Network

Core (or backbone) Network

Internet; Other Public/Private Networks

Trustworthy
use of licensed spectrum, subscriber identity modules (SIMs) and security standards*

Untrustworthy
Threats from unknown networks, cloud servers/services and devices

Cybersecurity Sweet Spot

In the intersection of the trustworthy and untrustworthy zone

2. CELLULAR PROGRAMMABLE NETWORKS – ACTING IN A SECURITY SWEET SPOT

High level intro to Programmable networks

- Computer networks are complex and difficult to manage.
- Many components (routers, switches, …) run proprietary/closed software, configured individually by network administrators.
- This approach slows down innovation, and increases complexity and costs on running a network.

- Paradigms like network function virtualization (NFV) and software defined networks (SDN) focus on virtualizing network components and controlling them (and the traffic) via software and standardized APIs.
- This fosters network automation, less complexity on the integration of new components and, ultimately, innovation

Feamster, Nick, Jennifer Rexford, and Ellen Zegura. "The road to SDN: an intellectual history of programmable networks." *ACM SIGCOMM Computer Communication Review* 44.2 (2014): 87-98.

2. CELLULAR PROGRAMMABLE NETWORKS – ACTING IN A SECURITY SWEET SPOT

TLDR: Why Programmable Networks are relevant for network-based cybersecurity

- **Automation and reduced human intervention**:
  - E.g. accelerated outage understanding / detection, self-protection and self-healing
- API-driven networks simplify and accelerate the **integration of new cybersecurity tools**
  - E.g. to understand a node level of vulnerability / compromise, relying on a trust reputation tool
- **Communication control,** acting in a security sweet spot - **most cyber-threats depend on the communication channels to achieve their goal** (DDoS, leakage of private data, unauthorized access to/control of devices, …)

3. ZERO-TOUCH NETWORK-BASED AUTHENTICATION OF IoT DEVICES TO CLOUD SERVICES

3. ZERO-TOUCH NETWORK-BASED AUTHENTICATION OF IoT DEVICES TO CLOUD SERVICES

Problem: IoT authentication in Cloud is still hard

Why:

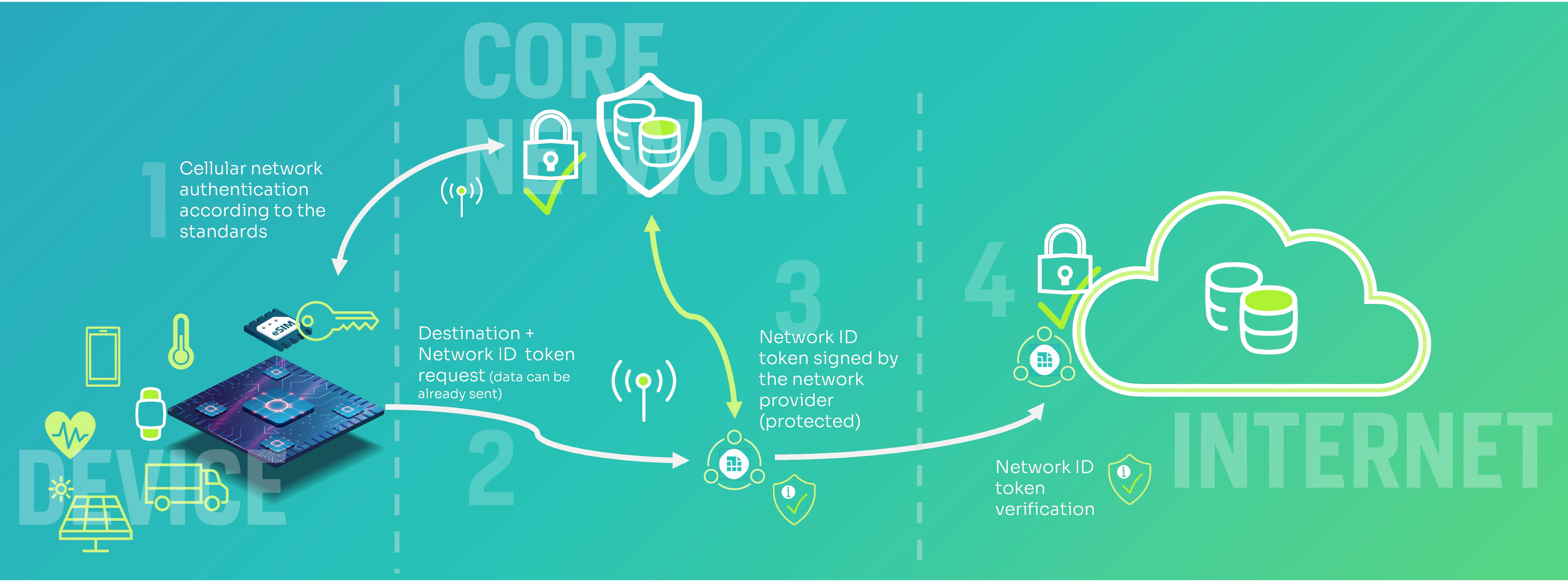
- Credential provisioning in manufacturing time is costly and hard to scale (e.g. connect a proprietary hardware to provide credentials to criptochips one by one)
- Hardcoded username / password (well-accepted as a weak practice) are still used

Solution:

Leverage cellular authentication standardized protocols and SIM credentials stored in a hardware secure element to authenticate IoT devices to Cloud services

3. ZERO-TOUCH NETWORK-BASED AUTHENTICATION OF IoT DEVICES TO CLOUD SERVICES

ARCADIAN-IoT



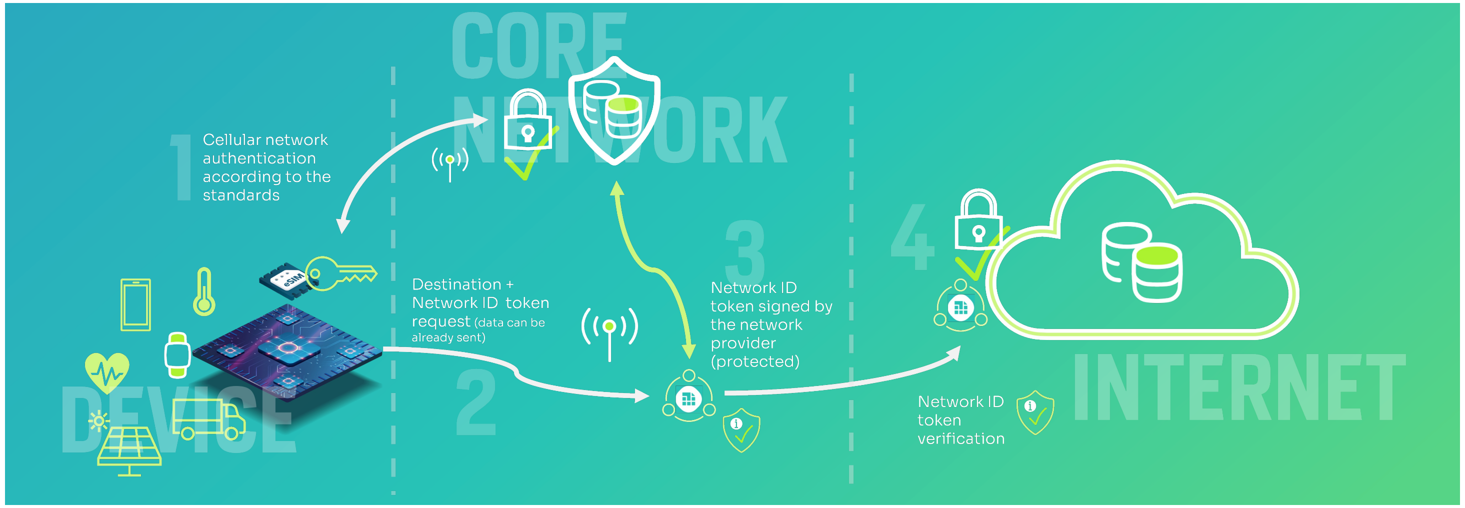
1 Cellular network authentication according to the standards

2 Destination + Network ID token request (data can be already sent)

3 Network ID token signed by the network provider (protected)

4 Network ID token verification

3. ZERO-TOUCH NETWORK-BASED AUTHENTICATION OF IoT DEVICES TO CLOUD SERVICES


CORE NETWORK
1
Cellular network authentication according to the standards
eSIM
DEVICE
Destination + Network ID token request (data can be already sent)
2
3
Network ID token signed by the network provider (protected)
4
Network ID token verification
INTERNET

Lightweight:

- no new cryptographic material – just the SIM secrets and processes)
- no added hardware (just the SIM, eSIM, iSIM… already needed for connectivity)

Secure:

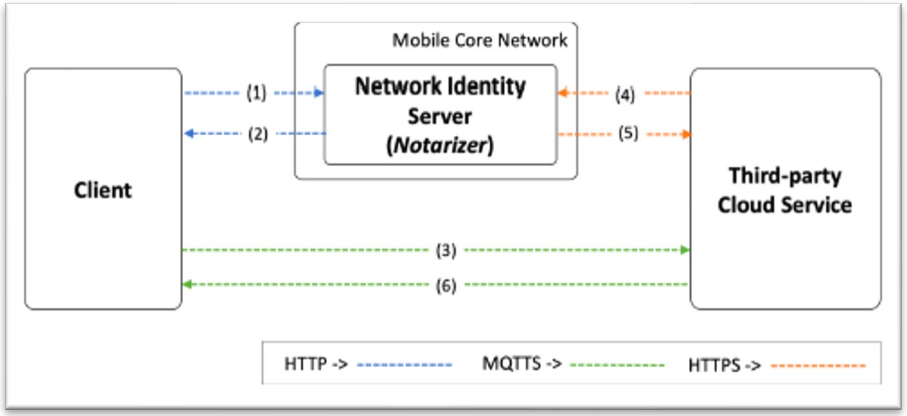
- Leverages proven security standards

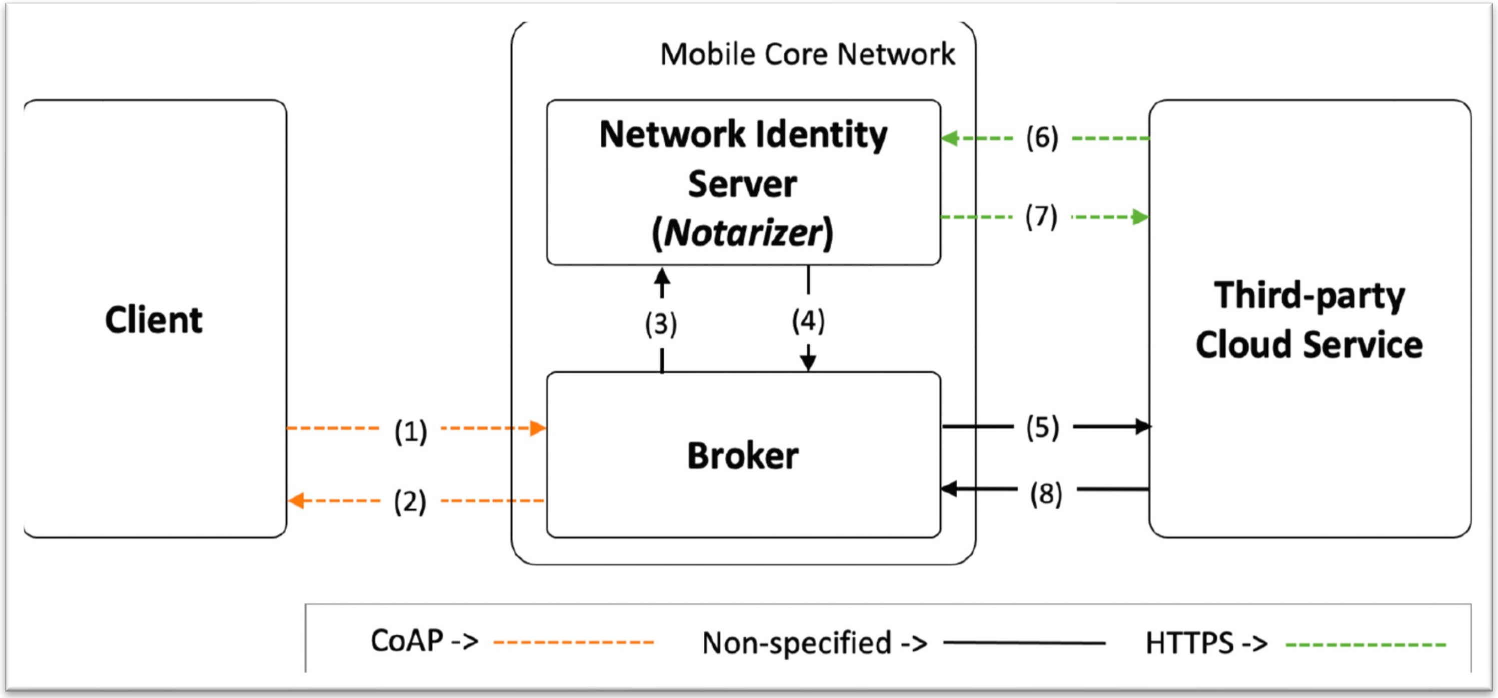
Scalable

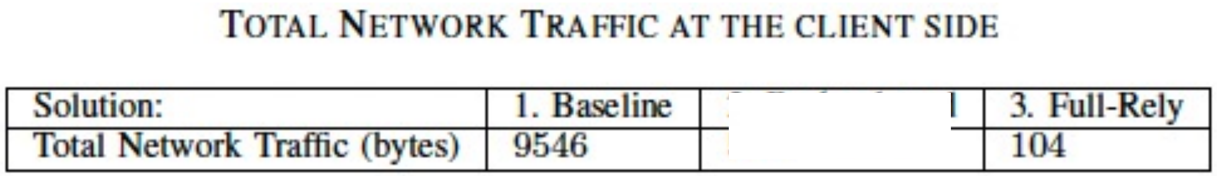
- No added provisioning effort on IoT device manufacture time (other than the SIM)

3. ZERO-TOUCH NETWORK-BASED AUTHENTICATION OF IoT DEVICES TO CLOUD SERVICES

Network-based authentication enabling security in **very constrained devices**







TOTAL NETWORK TRAFFIC AT THE CLIENT SIDE

Solution:	1. Baseline		3. Full-Rely
Total Network Traffic (bytes)	9546		104

* Paper accepted in TAISEN’23

TLDR: Why to use network-based authentication of IoT devices to Cloud services

- Overcomes common challenges related with:
  - passwords (weak or hardcoded passwords)
  - credential provisioning (scalability)
  - lack of physical hardeneing
- **SIM** technologies are already **critical and trusted in nowadays cybersecurity**
  - Trusted by telecom operators, governments, banks, … and people.
- The trust in the communication between devices and the core network allows to have a **very lightweight authentication proven as secure**

Q&A

João Casal (Head of R&D – joao.casal@1global.com)

Want to join my team in the sunny Lisbon working on innovative SIM, ProgNet and CyberSec tech? Talk with me! ☺