Managing Identities and Security through the IoT lens

Challenging IoT Security & Privacy Workshop

22nd October 2018

About the GSMA

The GSMA was founded in **1987**

12 offices worldwide

UNITING **750+** MOBILE OPERATORS

WITH **350+** MOBILE COMPANIES

In the broader mobile ecosystem

The GSMA represents the interests of mobile operators worldwide

The world's leading mobile industry events, Mobile World Congress, Mobile World Congress Shanghai, and Mobile World Congress Americas, together attract

192,000+

people from across the globe each year

8.8+ billion mobile connections worldwide

américa móvil · at&t · axiata advancing asia · bharti · 中国移动 China Mobile · China unicom中国联通 · T · · · · اتصالات etisalat

KDDI · kt · MTN · NTT docomo · orange · ooredoo · SK telecom · TATA

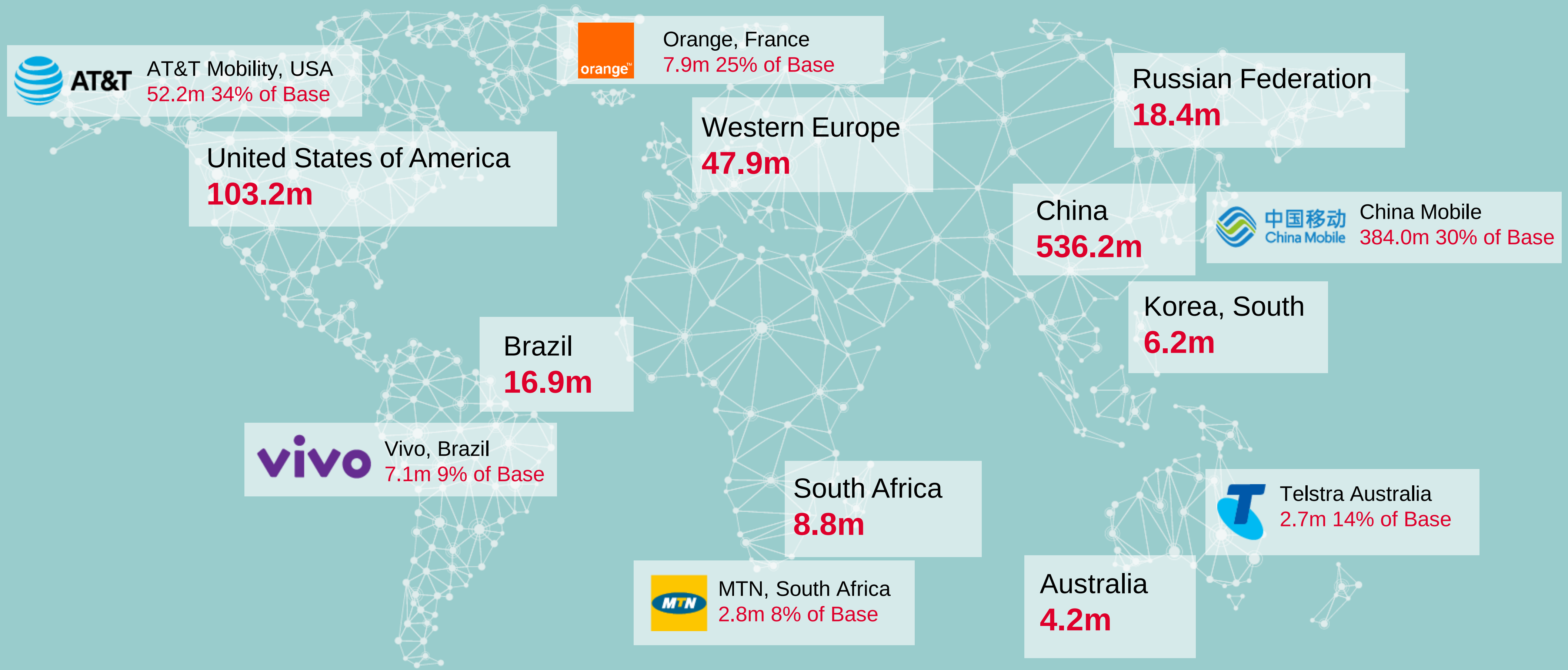
TELECOM ITALIA · Telefonica · telenor · Telstra · TÜRK TELEKOM · verizon · VimpelCom · vodafone

Connecting Everyone and Everything to a Better Future

The IoT is already happening

Q2 2018 CELLULAR IoT DATA

511 operators **195** countries **920** million connections



AT&T Mobility, USA
52.2m 34% of Base

United States of America
103.2m

Orange, France
7.9m 25% of Base

Western Europe
47.9m

Russian Federation
18.4m

China
536.2m

China Mobile
384.0m 30% of Base

Korea, South
6.2m

Brazil
16.9m

Vivo, Brazil
7.1m 9% of Base

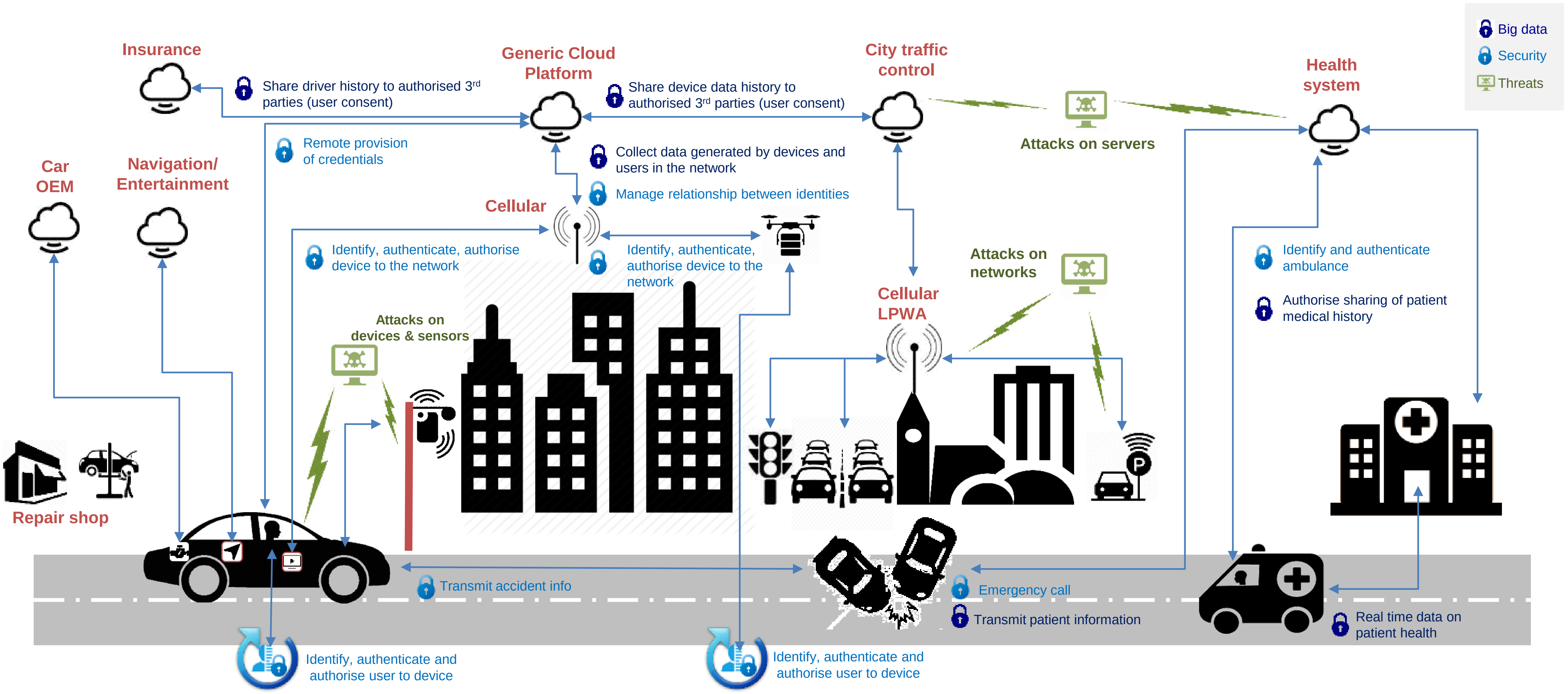
South Africa
8.8m

MTN, South Africa
2.8m 8% of Base

Telstra Australia
2.7m 14% of Base

Australia
4.2m

A Diverse and Complex IoT Market – the Smart City as an Example



🔒 Big data
🔒 Security
🖥 Threats

Insurance

Share driver history to authorised 3rd parties (user consent)

Generic Cloud Platform

Share device data history to authorised 3rd parties (user consent)

City traffic control

Health system

Attacks on servers

Remote provision of credentials

Collect data generated by devices and users in the network

Manage relationship between identities

Car OEM

Navigation/ Entertainment

Cellular

Identify, authenticate, authorise device to the network

Identify, authenticate, authorise device to the network

Identify and authenticate ambulance

Authorise sharing of patient medical history

Attacks on networks

Cellular LPWA

Attacks on devices & sensors

Repair shop

Transmit accident info

Emergency call

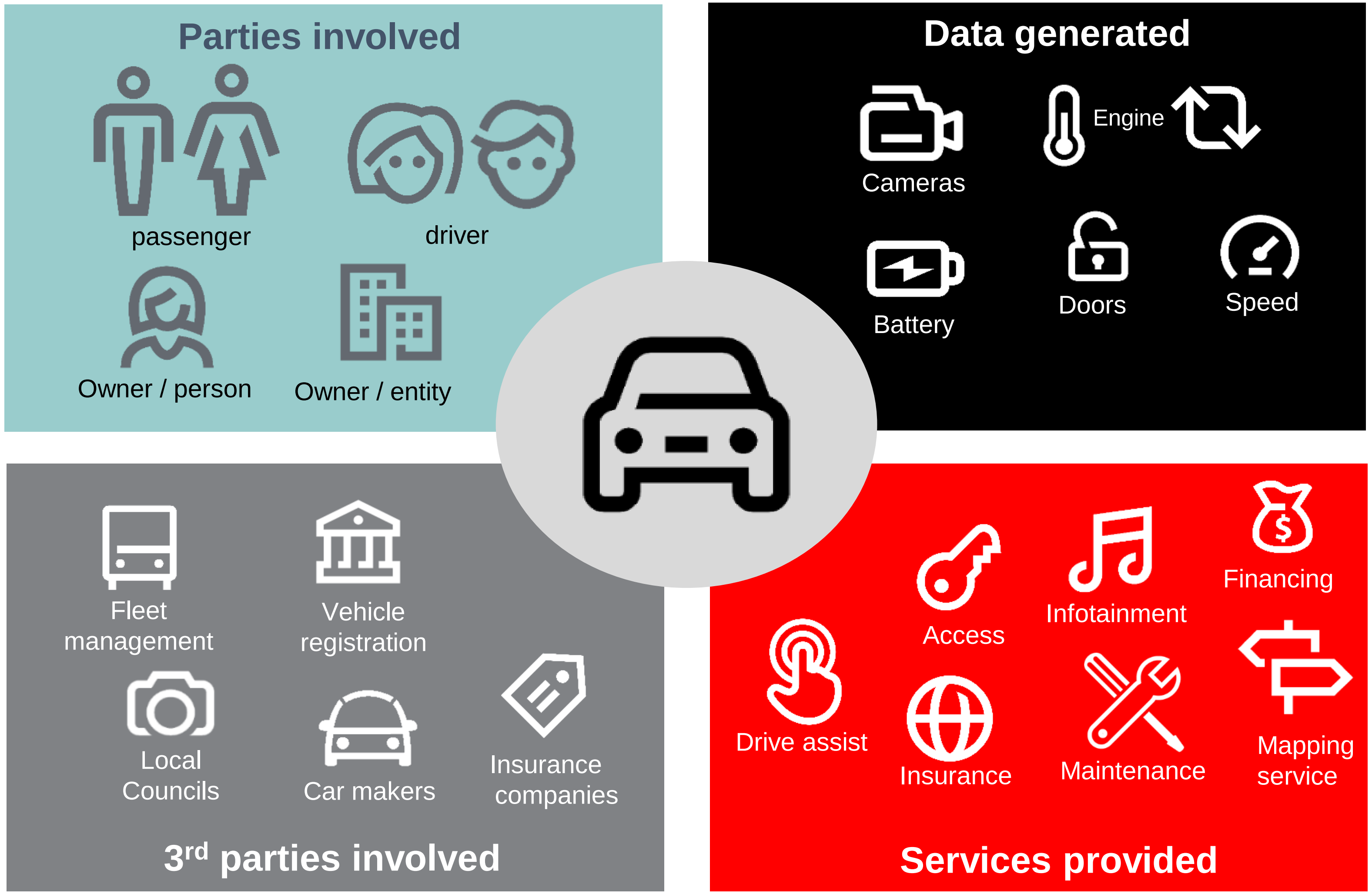
Transmit patient information

Real time data on patient health

Identify, authenticate and authorise user to device

Identify, authenticate and authorise user to device

Complex nature of our digital lives



Leveraging the SIM to Secure IoT Services

Mobile network operators use SIM Cards to authenticate devices accessing their networks and services. SIM cards can also support additional security capabilities that can be harnessed by Internet of Things (IoT) applications.

The case study shows how mobile operators in the Americas, Asia and Europe are developing and deploying SIM-based IoT security services to support their IoT customers.

Four mini-case studies in one document:

Telefónica aws	Secure provisioning and storage of a PKI certificate on a SIM card in a smart meter.
Taiwan Mobile Able Device	SIM-based solution to update the passcodes on smart meters once they have been deployed in the field.
China unicom中国联通 Tencent 腾讯	Use of SIM cards to authenticate smart watches and other IoT devices.
AT&T	Use of SIM to securely provision an IoT device’s identity and credentials for secure authentication to cloud platforms.

GSMA

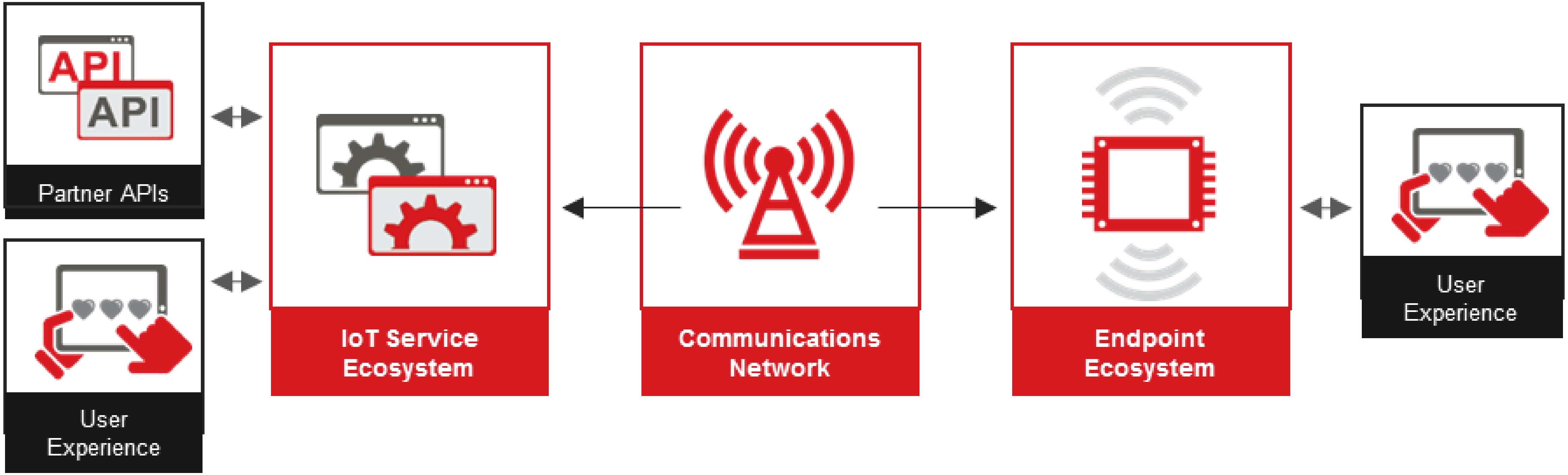
Case Study

LEVERAGING THE SIM TO SECURE IoT SERVICES

gsma.com/IoTSecurity

www.gsma.com/iot/case-study-sim-secure-iot-services/

Most IoT Services are Based Upon a **Generic IoT Architecture**



Partner APIs

User Experience

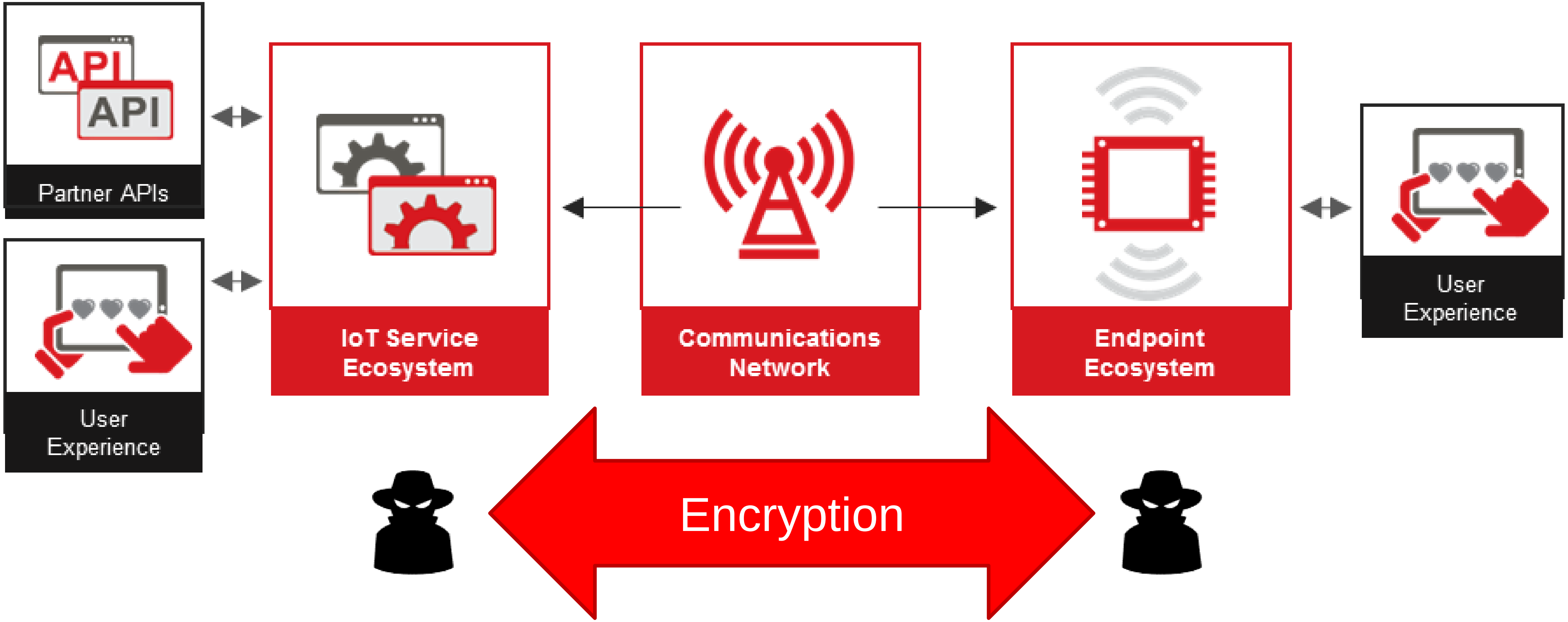
IoT Service Ecosystem

Communications Network

Endpoint Ecosystem

User Experience

Encryption Pushes Attacker’s to the Front and Back End



GSMA IoT Security Guidelines and Assessment

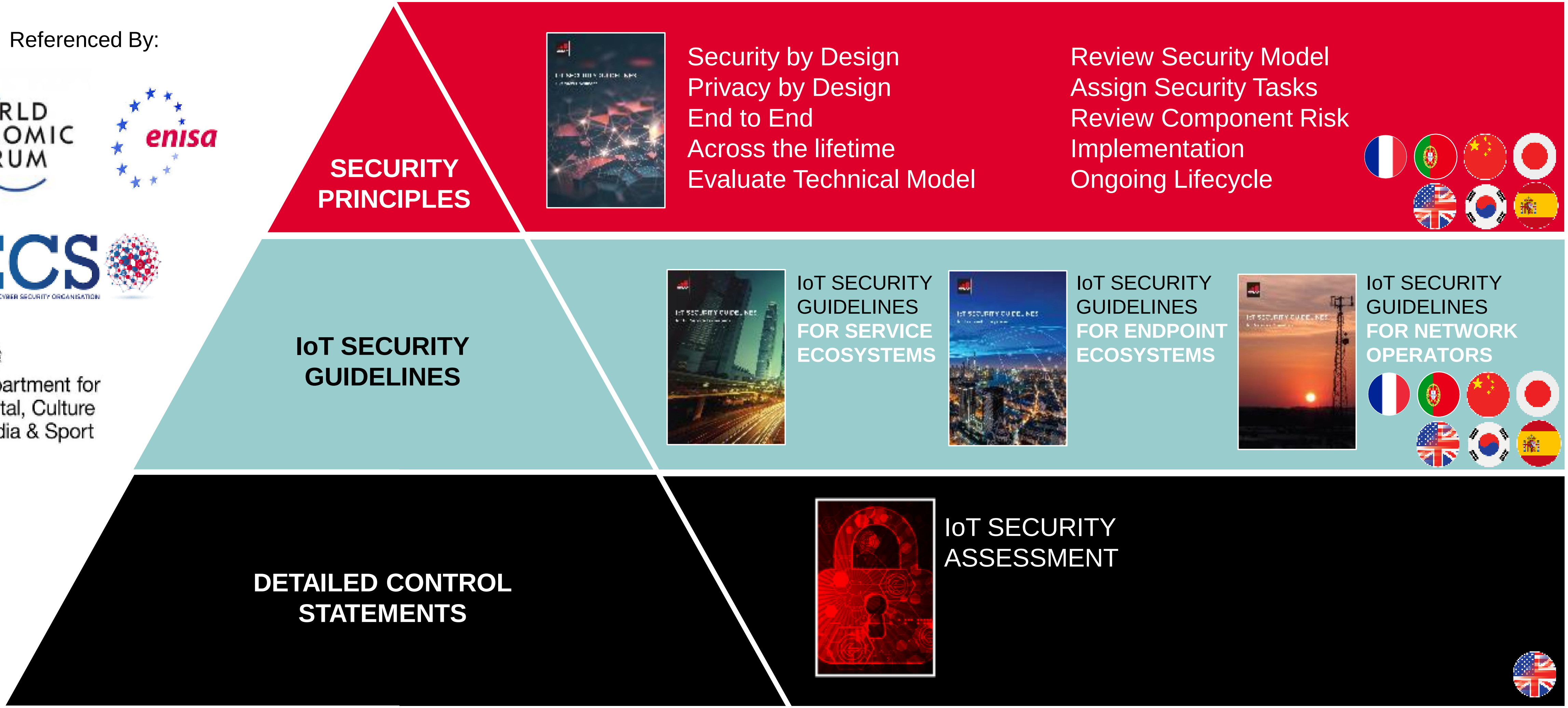
Referenced By:

WORLD ECONOMIC FORUM

enisa

ECS
EUROPEAN CYBER SECURITY ORGANISATION

Department for
Digital, Culture
Media & Sport



SECURITY PRINCIPLES

Security by Design
Privacy by Design
End to End
Across the lifetime
Evaluate Technical Model

Review Security Model
Assign Security Tasks
Review Component Risk
Implementation
Ongoing Lifecycle

IoT SECURITY GUIDELINES

IoT SECURITY GUIDELINES **FOR SERVICE ECOSYSTEMS**

IoT SECURITY GUIDELINES **FOR ENDPOINT ECOSYSTEMS**

IoT SECURITY GUIDELINES **FOR NETWORK OPERATORS**

DETAILED CONTROL STATEMENTS

IoT SECURITY ASSESSMENT

gsma.com/iotsecurity

What Does “Secure by Design” Actually Mean?

It is How to Ensure:

AVAILABILITY

Ensuring constant connectivity between Endpoints and their respective services

IDENTITY

Authenticating Endpoints, services, and the customer or end-user operating the Endpoint

PRIVACY

Reducing the potential for harm to individual end-users.

INTEGRITY

Ensuring that system integrity can be verified, tracked, and monitored.

In Services and Devices that are:

LOW COMPLEXITY

- Low processing capability.
- Small amounts of memory.
- Constrained operating system.

LOW POWER

- No permanent power supply
- Possibly permanent, but limited power supply.

LONG LIFECYCLES

- Requires cryptographic design that lasts a lifetime.
- Manage security vulnerabilities which can’t be patched within the endpoint.

PHYSICALLY ACCESSIBLE

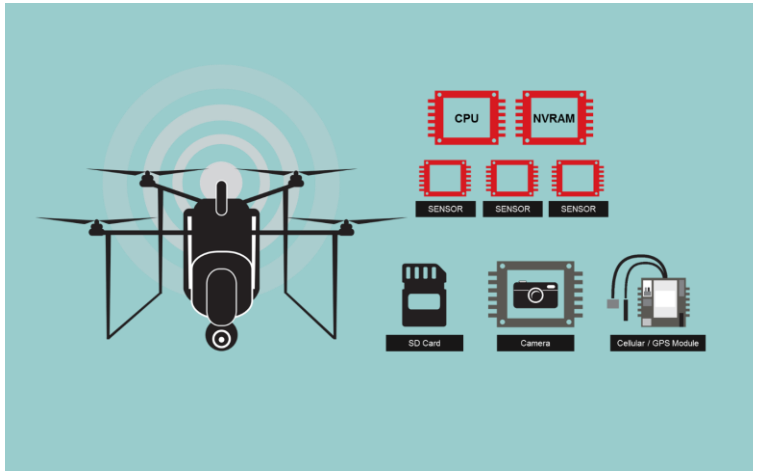
- Access to local interfaces inside the IoT endpoint.
- Hardware components and interfaces potential target of attackers.

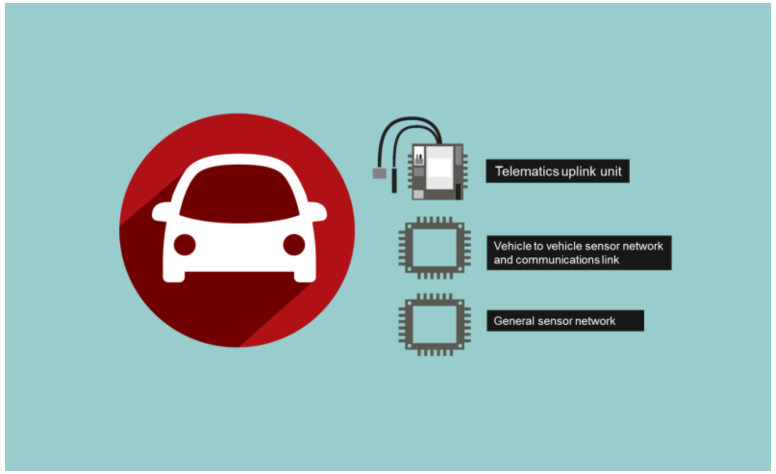
Key Considerations for IoT Applications and Services

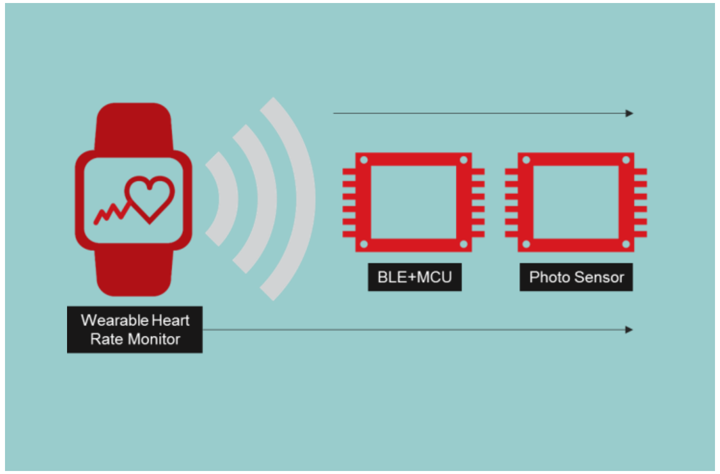
- How do I Combat Cloning?
- How do I Secure the Endpoint Identity?
- How do I Reduce the Probability of Endpoint Impersonation?
- How do I Disallow Tampering of Firmware and Software?
- How do I Reduce the Possibility of Remote Code Execution?
- How do I handle Side-Channel Attacks?
- How do I Implement Secure Remote Management?
- How do I Detect Compromised Endpoints?
- How do I Ensure my Privacy of Data?
- How do I Ensure User Safety While Enforcing Privacy and Security?

Worked Examples

- The guidelines contain three worked examples to demonstrate how to use the guidelines
- Shows how generic guidelines can be applied to a multitude of different IoT services because most IoT services are build from the same components
- The worked examples cover both the front-end ‘devices’ and back-end ‘service platforms’

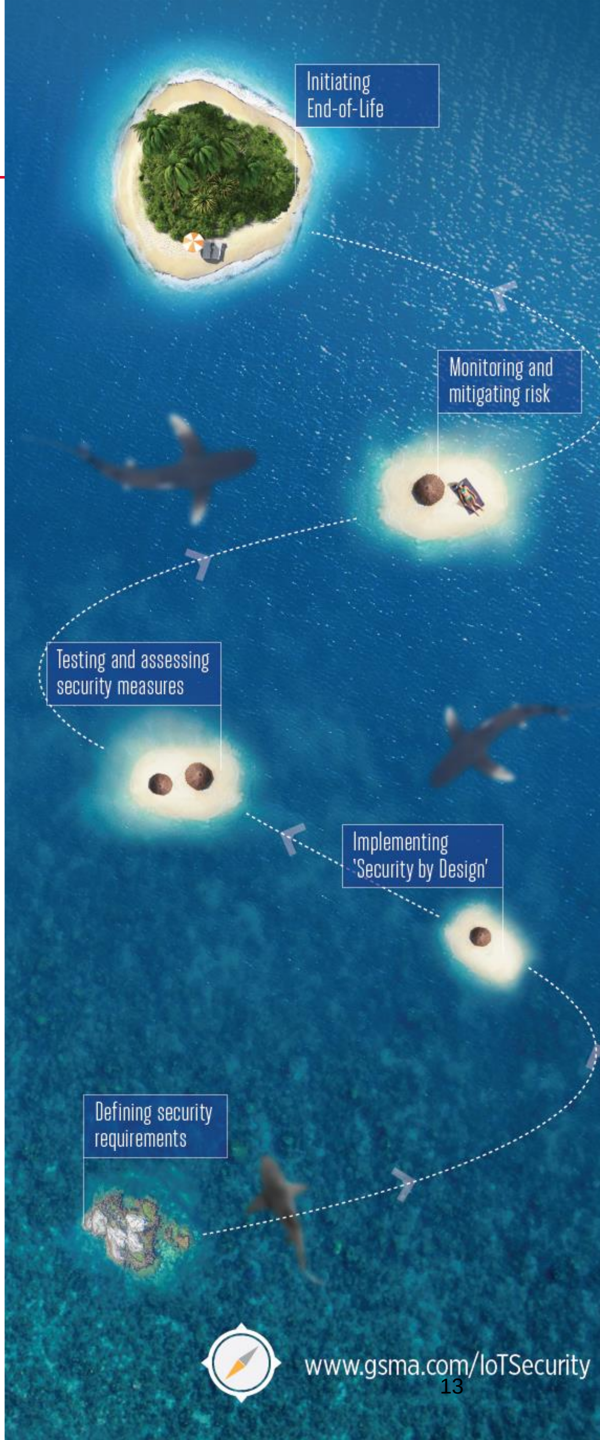






GSMA IoT Security Assessment – The Next Step

- Covers security controls for the whole ecosystem ensuring end-to-end security
- Establishes concise framework with consistent terminology
- Provides a structured approach to IoT security information
- Allows IoT service providers, platform vendors and device suppliers to discover if their security measures align with the best practice outlined in the GSMA IoT Security Guidelines
- Helps companies to address weaknesses in their products and services
- Enables companies to highlight the security measures they have taken to protect their products and services from cybersecurity risk



Initiating End-of-Life
Monitoring and mitigating risk
Testing and assessing security measures
Implementing 'Security by Design'
Defining security requirements
www.gsma.com/IoTSecurity

Download the GSMA IoT Security Guidelines

www.gsma.com/iotsecurity

Complete the GSMA IoT Security Assessment

www.gsma.com/iotsa

Talk to the GSMA Internet of Things Team

Mona Mustapha: mmustapha@gsma.com

More resources at

www.gsma.com/iot

Case Study

LEVERAGING THE SIM TO SECURE IoT SERVICES

Download the Case Study

www.gsma.com/iot/case-study-sim-secure-iot-services/