



IoT SAFE

Robust and Effective IoT Security at Scale



GSMA

Ian Smith
IoT Security Lead



Regulatory Push for IoT Security – Applying Pressure to Developers





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
Worked Examples

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

Referenced By:





GSMA IoT Security Guidelines

Over 200

pages of advice and best practice to secure devices, service platforms and networks

85 detailed recommendations

12 principal attack models

IoT Security Assessment checklist

3 'worked' examples – wearables, personal drone, automotive

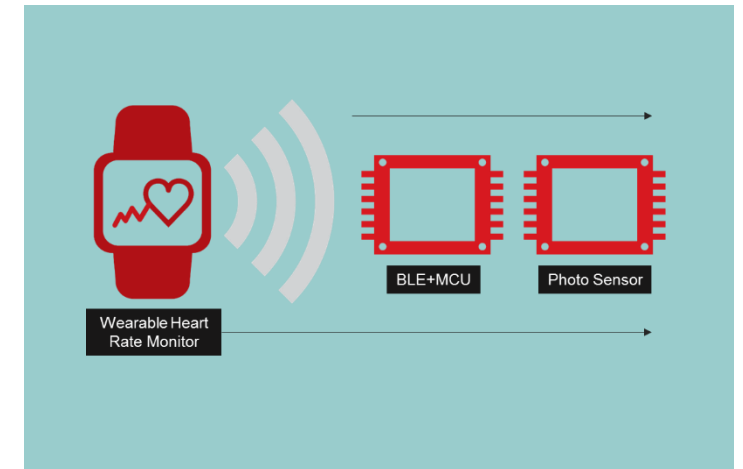
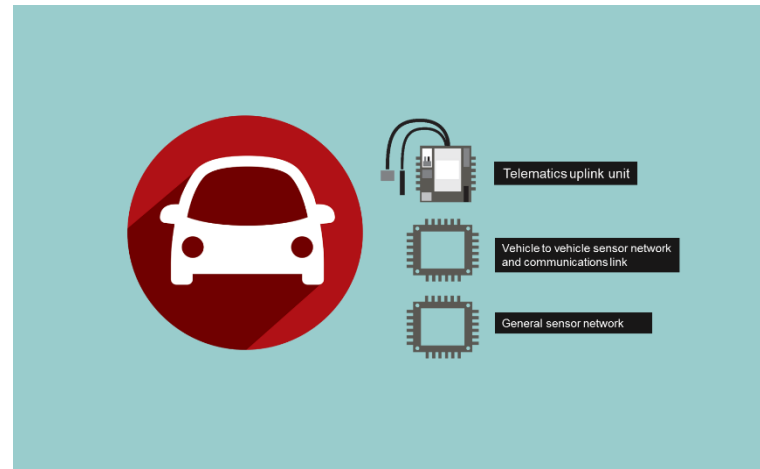
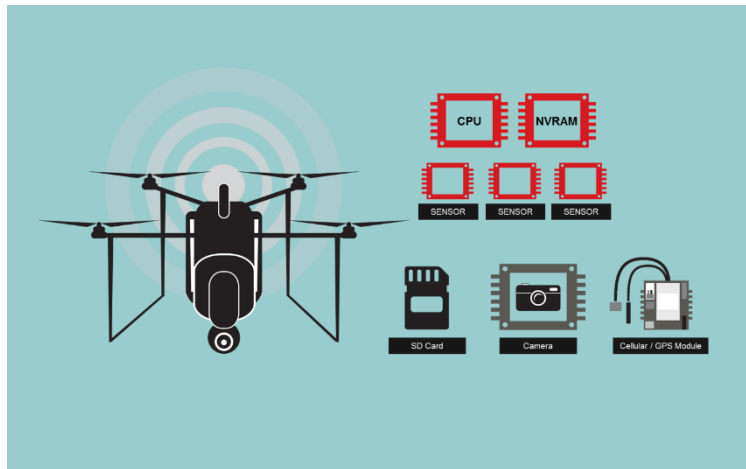
Risk and privacy impact assessments

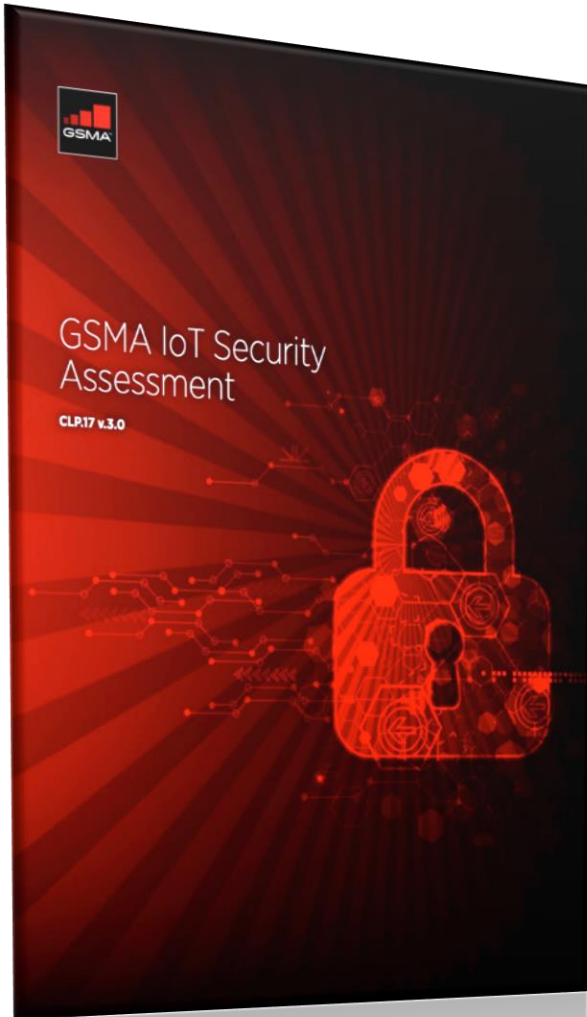
Supported by:



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 built from the same components
- The worked examples cover both the front-end 'devices' and back-end 'service platforms'





How To Assess Your Solution or Your Suppliers:

- Organisational Procedures
- Service Platform Security
- Communications Security
- Device Security



GSMA IoT Security Assessment as a Service

Don't have the resources/knowledge to complete an GSMA IoT Security assessment?

→ Then use the services of a security expert, some examples being:



www.7layers.com



www.firmalyzer.com



www.iot.achelos.com



www.ilabs.ai



www.appluslaboratories.com



www.orange.es



www.brightsight.com



www.redalertlabs.com



www.dekra-product-safety.com



www.testandverification.com



www.elevenpaths.com



www.vfgsecurity.com



GSMA IoT SAFE

IoT SAFE = **IoT** **SIM** **A**pplet **F**or Secure **E**nd-to-End Communication

- Just launched by GSMA in November 2019
- Enables a common way for the SIM to be used as a hardware “Root of Trust” for IoT Services
- Defines common APIs to new security services provided by SIM (including eSIM) to secure IP data communications using mutual authentication

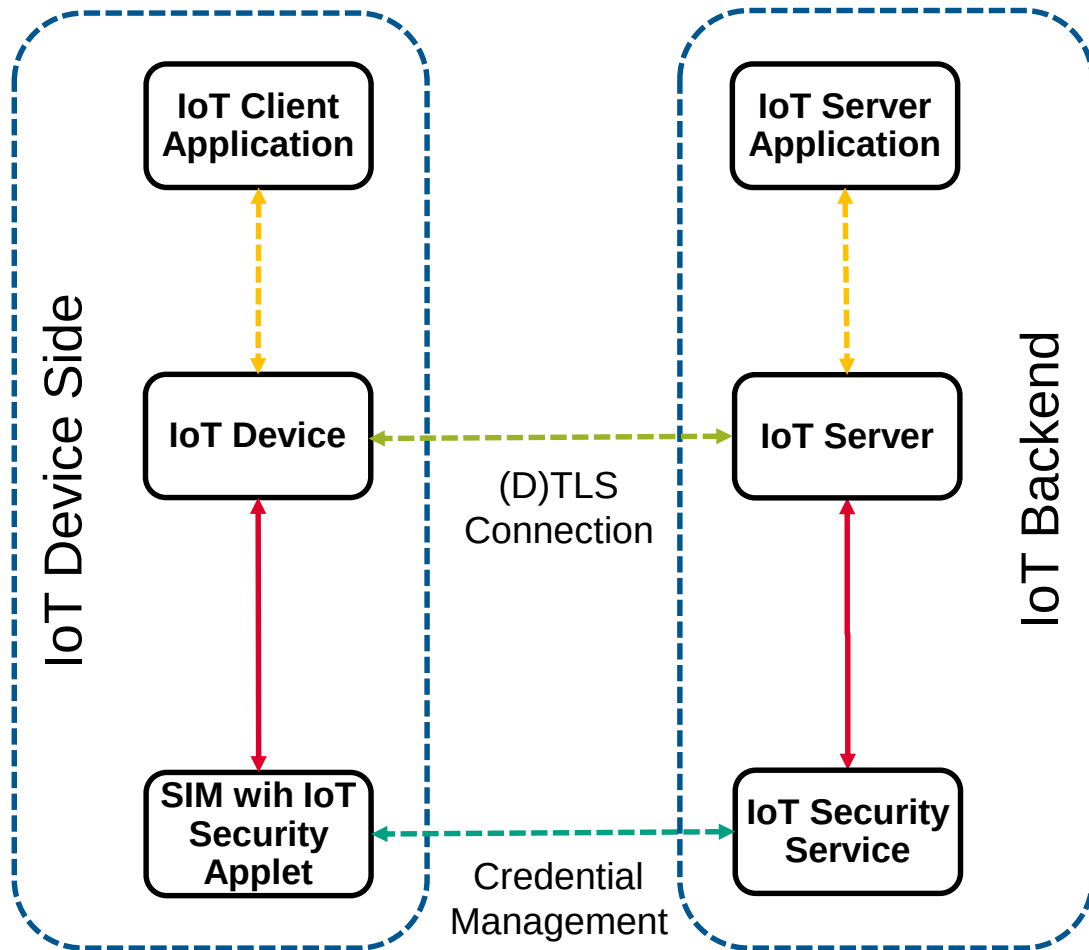


IoT **SAFE**

IoT **SIM** **A**pplet **F**or Secure **E**nd-to-End
Communication



IoT SAFE – Service Architecture



- ↔ Interface in Scope
- - - Out of Scope (Already Standardised)
- - - Out of Scope (Defacto APIs Already Exist)

In this solution we use IoT Security Applets to:

- Enable the IoT device to securely perform mutual (D)TLS authentication to a server using asymmetric and symmetric security schemes
- Enable the IoT device to compute shared secrets and keep long term keys secret
- Enable credential life cycle management from an IoT Security Service

IoT Security Applet uses APIs defined by JavaCard, GlobalPlatform and ETSI 102 241.

IoT SAFE – Applet Feature Sets

		IoT Security Applet 1	IoT Security Applet 2
TLS Version		TLS 1.2 and 1.3	TLS 1.2 and 1.3
Cryptography	RSA	Yes* (2048bit)	No
	ECC	NIST P256	No
	ECDHE	Yes	No
	ECDSA	Yes	No
	PSK	Yes* (512bits)	Yes (512bits)
SHA-256		Yes	Yes
HMAC		Yes	Yes
HKDF		Yes	Yes
OBKG		pRNG RFC5246	pRNG RFC5246



IoT SAFE



GSMA IoT SECURITY

Download the GSMA IoT SAFE Specification

www.gsma.com/iot/iot-safe

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

Ian Smith, IoT Security Lead: ismith@gsma.com

