




# IoT Security, Drones: Creating a Connected and Secure Future

Wednesday, 28 February 2018 | 12:00 - 14:00  
**at Mobile World Congress 2018**

A large, stylized network diagram in red lines and dots forms a globe-like shape in the background. It features several circular nodes, each containing a red icon: a signal tower, a molecular structure, a padlock, a classical building, a city skyline, a car, and a drone. These nodes are interconnected by a web of red lines.

# GSMA INTERNET OF THINGS PROGRAMME



**SECURING THE  
CONNECTED FUTURE**

**IAN SMITH**  
IoT Security Lead, GSMA

# 25 BILLION CONNECTED DEVICES BY 2025

## IN SELECTED VERTICAL SECTORS

Smart Cities: **0.9bn**

Connected Industry: **12.5bn**

Connected Vehicles: **1.2bn**

Consumer Electronics: **3.4bn**

Smart Home: **5.4bn**

## PER REGION

North America:  
**5.8bn**

Europe:  
**5.6bn**

Middle East/Africa:  
**1.4bn**

Latin America:  
**1.3bn**

Asia-Pacific:  
**10.9bn**

# GSMA IoT Security Guidelines and Assessment



# New Security Challenges Require New Best Practices

## 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.

# A New Approach to IoT Security Evaluations

- ➔ The diversity of the IoT ecosystem and the quick pace of technological development are creating obstacles for using traditional methods of security evaluation for the IoT
- ➔ Light-touch benchmarking tools and general approaches are better suited to
  - ➔ Accommodate the complexity of the IoT ecosystem
  - ➔ Factor in a diversity of stakeholders and components of the IoT device or service





# GSMA IoT Security Assessment



## IoT Security Assessment

Without security, the Internet of Things will cease to exist. *Security by Design* – embedding security from the beginning – can minimize the risk of destroyed reputations and costly remediation. IoT companies will need to take action now to shield their solutions from cyberattacks and safeguard customer data, if they are to protect their reputation as a provider of secure devices and services.

The GSMA IoT Security Assessment provides a flexible framework that addresses the diversity of the IoT market, enabling companies to build secure IoT devices and solutions as laid out in the *GSMA IoT Security Guidelines*, a comprehensive set of best practices promoting the secure end-to-end design, development and deployment of IoT solutions.

Building on the extensive expertise of the mobile industry, gained from decades of providing secure, trusted and reliable products and services, the GSMA IoT Security Assessment scheme ensures *Security by Design* and enables companies to identify and mitigate any potential security gaps in their services, allowing the market to scale to its full potential.

[DOWNLOAD ASSESSMENT](#)

GSMA IoT Security Assessment

### 3 GSMA IoT Security Assessment Checklist

All sections of this checklist must be completed.

GSMA Assigned Reference Number:  Enter Number Here

Note: Reference Number assigned by GSMA is part of the GSMA IoT Security Assessment process. For full details of the process click on this link: [www.gsma.com/iot/iot-security-assessment/](http://www.gsma.com/iot/iot-security-assessment/)

#### 3.1 Organisation Information

Company Name:	Trading As:
Contact Name:	Title:
Telephone Number:	Email Address:
Address:	Country:
Website URL:	
Type of Organisation:	IoT Service Provider:
	IoT Service Platform Vendor:
	IoT Endpoint Vendor:
	Service Ecosystem Component Vendor:
	Endpoint Component Vendor:
	Other:

#### 3.2 IoT Service Information

##### 3.2.1 Overall Service Information

Service Name:	Version:
Product website:	
Date of Submission:	

##### 3.2.2 Service Ecosystem Information

Service Platform Name:	HW Version:	SW Version:
------------------------	-------------	-------------

##### 3.2.3 Endpoint Ecosystem Information

Endpoint Name:	HW Version:	SW Version:
----------------	-------------	-------------

##### 3.2.4 Communication Network Information

Communications Network Provider(s):	Technology:
-------------------------------------	-------------

GSMA IoT Security Assessment Checklist

### 3.1 IoT Security Assessment Checklist

3.1.1 Security and Privacy Organisational Level Checklist  
The following recommendations are taken from CLP10 (1).

Company Recommendations

Recommendation	CLP10, 3	Response	Notes			
Question	3.1.1 What method is your Risk Assessment Model based upon?	Yes	Part	No	N/A	
Control	3.1.1.1 Our Risk Assessment Model is based upon a standard method (e.g. ISO 27005 (4)).					
Question	3.1.2 Have a Risk Assessment been completed?					
Control	3.1.2.1 We have identified the assets (digital or physical) that need to be protected.					
	3.1.2.2 We have identified the risk factors that affect our personnel.					
	3.1.2.3 We have identified third agents.					
	3.1.2.4 We have completed a vulnerability assessment.					
	3.1.2.5 We have evaluated the security, privacy and safety impacts of our product upon being commercialised for our organisation, our partners and our clients.					
	3.1.2.6 Our organisation's chosen risk model assesses the probability of our assets being compromised.					
Question	3.1.3 Do you have processes to address existing future risks and vulnerabilities?					
Control	3.1.3.1 We have implemented a process to identify, detect, mitigate and contain existing future risks and vulnerabilities.					
	3.1.3.2 We have a process in place for incident response.					
	3.1.3.3 We have implemented a process to manage security incidents from our suppliers (e.g. hardware and software providers) and/or provide security updates to our partners.					
	3.1.3.4 We have implemented a process to share vulnerability or incident information with affected stakeholders as mandated by regulations.					

#### 3.2 Privacy Considerations

Recommendation	CLP10, 6	Response	Notes			
Question	3.2.1 Have your organisation have a privacy compliance process?	Yes	Part	No	N/A	
Control	3.2.1.1 We have implemented a privacy compliance process within our product/service development lifecycle.					
	3.2.1.2 We have performed a privacy impact assessment.					
Question	3.2.2 Do you have processes to identify the sources of personal data?					
Control	3.2.2.1 We have identified which entities are collecting, storing, sharing and using personal data.					
	3.2.2.2 We have identified level and location source of personal data.					
	3.2.2.3 We have identified when and why personal data is being collected.					

# GSMA IoT Security Assessment

- ➔ The growth of non-cellular IoT devices poses an authentication challenge
- ➔ SIM card-based technology can be used to improve authentication within IoT services
- ➔ Methods for SIM-card based authentication include, e.g.:
  - ➔ Verify the integrity of firmware updates
  - ➔ Connect and authenticate to a trusted WLAN
  - ➔ Offload IoT traffic to a WLAN using Passpoint™







- ➔ Download the GSMA IoT Security Guidelines

[gsma.com/iotsecurity](https://gsma.com/iotsecurity)

- ➔ Complete the GSMA IoT Security Assessment

[gsma.com/iotsa](https://gsma.com/iotsa)

- ➔ Talk to the GSMA Internet of Things Team

Ian Smith, IoT Security Lead: [ismith@gsma.com](mailto:ismith@gsma.com)

- ➔ More resources at

[gsma.com/iot](https://gsma.com/iot)