



# Security & the IoT

GSMA industry position

August 2017

---

# GSMA industry position on security in the Internet of Things

The GSMA believes that security is vital to building and maintaining **consumer confidence** in mobile services and it will also be critical to the success of IoT services that have the potential to support and deliver increasingly sophisticated and security sensitive services.

While the IoT encompasses a hugely diverse range of different services, most IoT services present the same cybersecurity challenges: how to achieve the security properties of “availability”, “identity”, “integrity” and “privacy” in devices that are low complexity (low cost), have constrained power supplies (battery, solar), have long lifecycles (5+ years) and are physically more accessible to attackers.


In addressing these issues it is important that robust security measures are adopted by the whole IoT value chain for the lifetime of the service, since most IoT services are deployed using a collection of enabling entities and technologies each with their own set of attack vectors. As such, adopting a holistic security approach is the only way to mitigate security vulnerabilities in IoT devices, networks, applications and web services that comprise a typical IoT service.

Given the diverse range of types of IoT services, the unique security challenges of the IoT and need for a holistic approach towards security, the GSMA firmly believes that IoT security is best addressed via an industry-led approach:

- **Flexibility is critical**, as a ‘one size fits all’ approach to IoT security will prove ineffective given the diverse range of services that are likely to be developed. We urge that each service (in the context of its own local regulatory environment) develop its own security and privacy model based upon industry driven, standardised, security and risk assessment methodologies to achieve the necessary level of security for the particular service and its corresponding business model.
- GSMA does not propose the development of **new IoT security solutions** at this time, but suggests that cost effective, IoT services can be built to be ‘secure by design’ using currently available solutions, standards and best practice, such as those promoted within the [GSMA IoT Security Guidelines](#).
- Formal IoT security certification (or Trust Mark/Label schemes) should only be considered after comprehensive industry consultation, and if it is necessary, should wherever possible be developed on top of existing, vertical industry certification schemes.

Empowering customers to factor security into their purchasing decisions is critical to the success of IoT services. It is important that security is considered both within the internal supply chain of the IoT service provider when building a service and the final customer that purchases the service. To achieve this goal security must become both visible and measureable so that correct purchasing decisions can be made.

The GSMA has developed a IoT Security Assessment to enable IoT security to become visible and measureable within the supply chain. The GSMA IoT Security Assessment provides a flexible framework that accommodates the diversity of the IoT market, ensuring that companies to build secure IoT devices and solutions as laid out in the GSMA IoT Security Guidelines.



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, allowing the market to scale to its full potential.

A whitepaper explaining the benefits of using the IoT Security Assessment scheme can be downloaded here: <https://www.gsma.com/iot/wp-content/uploads/2017/04/3371-GSMA-Security-CS- WEB.pdf>



**GSMA HEAD OFFICE**

Floor 2

The Walbrook Building

25 Walbrook

London EC4N 8AF

United Kingdom

Tel: +44 (0)20 7356 0600

Fax: +44 (0)20 7356 0601