



## Future IoT Networks



## End-to-End Security Capability

In 2014, the GSMA worked on IoT security as part of the Connected Living Programme's Future IoT Networks project. In December 2014, the GSMA published the *End-to-End Security for IoT and M2M* position paper (CLP.04 End-to-End Security for M2M and IoT v1.0.doc), which introduced the requirements for security in IoT.

The position paper was followed by the publication of the *End-to-End Security for IoT and M2M* white paper (CLP.06 Whitepaper on End-to-End Security for IoT and M2M v1.0.doc) in February 2015, which provides an extended technical analysis of mobile network operators' (MNOs) security capabilities.

Both papers are available to the GSMA's Full, Rapporteur, and Associate Members via the GSMA's Infocentre.

### **The growing need for end-to-end security**

The emergence of the IoT, which spans both the public and private sectors, is attracting new players into the mobile ecosystem. As they develop specialist devices and solutions for particular industries and consumer segments, these players may be unaware of what threats they face. In some deployments, security and privacy are not always considered at the design stage and the resulting solutions may need to be modernised to address the end-to-end threat.

To ensure that end-to-end security is maintained, mobile operators need to apply their security expertise in this new market and share good practices.

End-to-end security can mean different things in different contexts. The aforementioned security papers published by the GSMA consider all aspects of security – the participants, the technology and the data exchanged.

In other contexts, end-to-end security may be considered simply as a cryptographic problem – i.e. that there is 'one security hop' (an end-to-end encrypted link) between the end device and the data end-point that it communicates with. Such end-to-end cryptographic security involves using a single set of credentials from data source to data destination, whatever the number of hops in the communication path. There are various means to achieve end-to-end cryptographic security, including the use of proprietary protocols and virtual private networks (VPNs), but it does not eliminate risk or security threats – it shifts them to the end-points. Set against the problem of credential management with the involvement of different parties, this may be an acceptable decision to make, but ultimately will require independent trusted parties for credential provisioning and authentication.

### **MNO value proposition for end-to-end security**

MNOs are well positioned to address a number of end-to-end security challenges within M2M and IoT implementations. In some cases, a MNO could act as a guardian of the data that transits its network. If it has access to both communication end-points, the operator could provide complete end-to-end cryptographic protection for the user via an IoT/M2M solution – using the capabilities of the network to provide virtual private networks (VPNs) and/or using the secure execution

environment of the SIM, or some other trusted execution environment on the device, to create session keys and store any long term keys. In the non-cellular environment, the UICC could be leveraged for application credentials and secure storage, even without a subscription.

MNOs can also add significant value by using the capabilities of their own infrastructure to provide resilience and additional security that other solutions cannot. For example, changes in information about the location of a device in relation to the mobile network could be used to detect the theft of a static device and alert the owner, even remotely disabling the stolen device for the owner, if necessary.

MNOs typically use SIM-based authentication and profile checking systems to determine which devices can use their networks and the services offered, including connections to the wider Internet and VPNs that are enabled via transport and access gateways. These systems enable MNOs to ensure the resilience and integrity of their networks and service offerings.

#### Next steps

Many of the technical recommendations, requirements and best practices that need to be implemented to create secure M2M and IoT devices and services already exist within the documentation that MNOs have created for mobile handsets, cloud services and management. Repurposing this work for the IoT market is a key next step.

The GSMA Connected Living Programme continues to work on IoT security. Please get in touch with the GSMA's Future IoT Networks team at [connectedliving@gsma.com](mailto:connectedliving@gsma.com)



[WWW.GSMA.COM/CONNECTEDLIVING](http://WWW.GSMA.COM/CONNECTEDLIVING)



[connectedliving@gsma.com](mailto:connectedliving@gsma.com)  
[www.gsma.com](http://www.gsma.com)

©GSMA February 2015