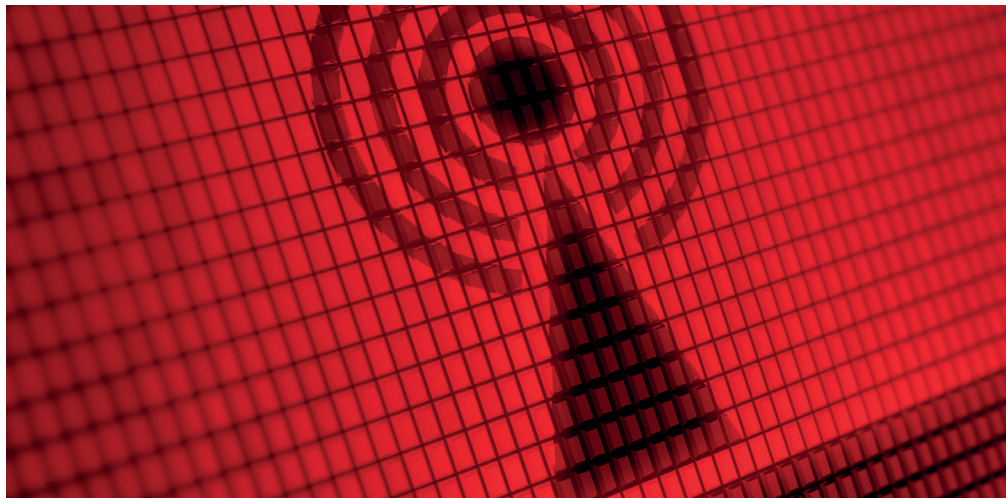




Future IoT Networks



Non-GSM Authentication Capability

During 2014, the GSMA worked on enabling authentication on non-GSM networks as part of the Connected Living Programme's Future IoT Networks project. In February 2015, the GSMA published the Non-GSM Authentication white paper (CLP.07 Whitepaper on Non-GSM Device Authentication v1.0.doc), which provided an extended technical analysis of mobile network operators' (MNOs) authentication capabilities for devices without SIM cards.

This paper is available to the GSMA's Full Members on the Infocentre.

Growing demand for authentication of devices without a SIM

Non-GSM devices (connected devices without SIMs) include sensors, actuators and other resource-constrained devices with limited memory, intelligence and user interfaces; most require management via alternative means, such as fixed or wireless network gateways. In the next five years, the number of non-GSM devices is set to grow exponentially. Machina Research predicts that, by 2020, as many as 13 billion devices will be connected via a range of fixed and wireless technologies, such as Wi-Fi, Bluetooth, ZigBee and Z-Wave.

MNO value proposition for non-GSM device authentication

Authentication of non-GSM devices takes places using a variety of mechanisms to exchange credentials that establish and confirm the claimed or asserted identity of an entity. Authentication of these edge devices is an essential service for MNOs to offer in the IoT environment. This capability could also be provided as part of an overall IoT security service.

Most IoT deployments today use walled-garden models, developed in-house by the enterprise, for authenticating non-GSM devices. However, as new deployment models are introduced into the market, such as plug-and-play smart devices for homes and healthcare, new authentication mechanisms might be required. Moreover, most authentication solutions today are vertical- or service-specific. A platform approach could generate economies of scale for authentication-as-a-service.

If every IoT service provider deploys a proprietary authentication solution, the existing market fragmentation will be exacerbated, increasing the costs of solution maintenance and device replacement, and potentially increasing security risks. As more small players start using IoT solutions, they will need support to implement secure mechanisms, particularly authentication, fuelling demand for the services of trust providers, and managers of consent and authorisation.



MNOs can help M2M/IoT service providers address the following challenges related to authenticating non-GSM devices:

- **Services or applications built in silos can be vulnerable if they aren't underpinned by adequate authentication, authorisation and data exchange implemented by the service/application provider.**
- **As well as focusing on the dedicated service logic, the service provider also needs to consider the security of the authentication, which may delay time-to-market for its product/service and lead to unpredictable behaviour of its devices/ applications on the network.**
- **For both authentication at application/service provider level and walled-garden solutions, customer choices are very limited, potentially resulting in lock-in.**

MNOs can leverage their existing authentication capabilities and provide a higher level of assurance and uniform and transparent authentication mechanisms to service providers that can help overcome these issues.

Importantly, MNOs can offer harmonised standards-based solutions, such as the Mobile Connect solution developed by the GSMA Personal Data Programme. MNOs have many assets required for the secure management of non-GSM devices: They are already providing gateways and routers to businesses and consumers and have all the necessary tools to introduce end-to-end security elements in the core and at the edge of the network. Thus, MNOs can offer both device and network management tools, such as diagnostics, software and firmware management in the gateways for managing sensors.



Next steps

The GSMA Personal Data and Connected Living Programmes continue to develop M2M and IoT non-GSM authentication use cases.

For further information, please get in touch with the GSMA's Future IoT Networks team at **connectedliving@gsma.com**

WWW.GSMA.COM/CONNECTEDLIVING



connectedliving@gsma.com
www.gsma.com

©GSMA February 2015