IDEMIA

The cellular networks to power IoT

Because of the rapid development of the Internet of Things (IoT), increasing numbers of connected objects are putting huge pressure on cellular networks. These objects also have to consume as little energy as possible, as they are often off the power grid. Cellular networks therefore have to evolve towards Low Power Networks, with the help of a new generation of SIM cards that can reduce power consumption while ensuring durable security.

The Internet of Things is everywhere

+25 BILLION connected objects by 2025

1 What technologies are used to connect IoT?

NETWORKS OF TODAY AND TOMORROW

The networks currently used by mobile operators (2G, 3G & 4G) offer the capacity to connect large numbers of everyday objects. Their next generation, **5G, will play an important part in answering IoT-related demand (e.g. for connected vehicles or remote healthcare).**

In response to the growth of the IoT, and to address devices with reduced bandwidth requirements, new mobile network technologies have emerged. **Low-Power Wide Area (LPWA) networks are designed to improve coverage while saving energy** ("Low Power"). They can connect objects in remote locations ("Wide Area").

There are two types of LPWA networks:

1 **The first type operates on "Licensed Spectrum" frequency ranges.** These government-regulated radio frequencies are already leased to Mobile Network Operators for their 2G, 3G and 4G networks, meaning that operators can easily roll out LPWA networks on the same frequencies. The main LPWA networks in this spectrum are **Long Term Evolution-Machine** (LTE-M) and **Narrow Band-Internet of Things** (NB-IoT).

2 **The second type operates on unlicensed, «Free Spectrum» radio frequencies.** Companies operating in these frequencies can only roll out LPWA networks.

Reduced bandwidths for small bits of data

LTE-M and NB-IoT technologies use a narrower spectrum than 2G, 3G and 4G networks. As the devices only need to transmit small amounts of data, they require less bandwidth and therefore less energy to function. As a result, **LTE-M and NB-IoT allow devices to reduce their power consumption while increasing their network coverage** (up to 10 km for LTE-M and up to 15 km for NB-IoT).

LESS ENERGY TO FUNCTION

NB-IoT	200kHz
LTE-M	1,4MHz
3G	5MHz
4G	up to 20MHz

2 What is a low power network SIM card?

New form factors for low cost devices

To reduce the Bill Of Material (BOM), **the SIM card has to shrink, in terms of memory but also footprint.** The mobile operator SIM profile has to be reduced to a few tens of kBytes and the SIM card needs to adapt to device requirements, including all traditional form factors as well as evolutions of the soldered form factor.

- 2FF
- 3FF
- 4FF
- MFF2, DFN, CSP

Endurance in extreme environments

+105°C

-40°C

Low power SIM cards have to be able to operate from -40°C to +105°C.

Low power SIM cards need to function durably, even in harsh environmental conditions. They have to support at least 1,000,000 write cycles at 25°C and offer **15-year data retention even in extreme temperatures.**

Enabling devices to consume less power and last longer

Connected objects such as off-grid pieces of equipment sometimes need to be able to transmit data for a decade. New functionalities have been introduced in Low Power network SIM cards to reduce power consumption: poll interval negotiation, for instance, allows the interval between times when the device interrogates the SIM card to be extended.

WITHOUT POLL INTERVAL NEGOTIATION

WITH POLL INTERVAL NEGOTIATION

TIME

More energy-efficient communication

Thanks to poll interval negotiation, the SIM card and device manage their communication more efficiently, reducing power consumption in the process.

Without coverage, a connected device is just a device

Connected objects can be located in remote areas or behind thick walls, yet it's crucial for mobile operators and objects makers to ensure they have good coverage. As these types of IoT devices are not running on Android nor iOS, putting an application in them is challenging. The most interoperable solution is therefore to have a dedicated agent in the SIM card that monitors network events and sends data to a server.

An agent in the SIM to monitor coverage and get location information

3 What about security?

Although IoT technologies will become more established in the coming years, the security of the data is still a work in progress. The security and protection of data is a priority concern for players in this sector.

3 SECURITY CHALLENGES

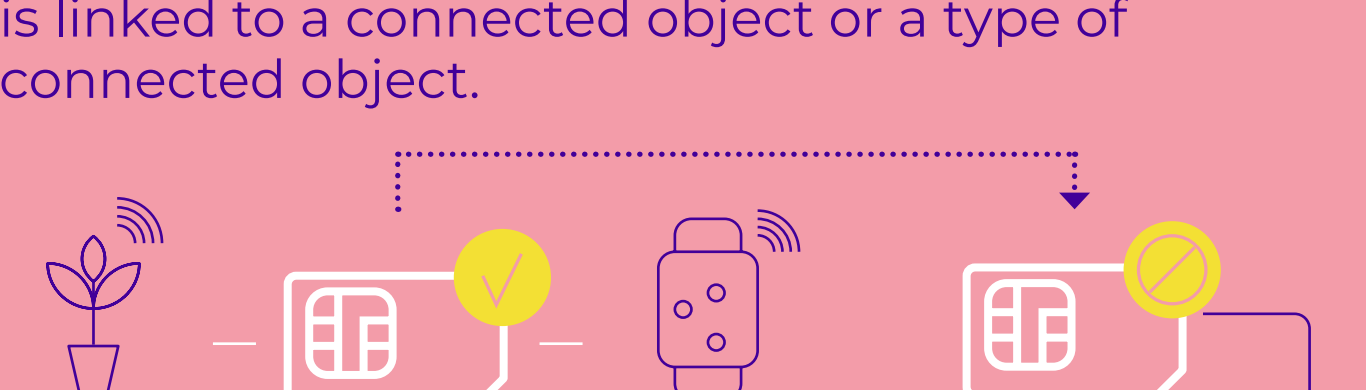
IDENTIFICATION AND AUTHENTICATION
The identity of the objects transmitting data must be verifiable.

INTEGRITY
The data must not be modifiable during transmission.

CONFIDENTIALITY
The data must be able to be transmitted without being hacked or viewed by a malicious third-party.

Avoiding fraud and vandalism

A SIM card can be used in any type of connected object. In order to avoid someone taking it out to put it in a smartphone for a personal call, the functionality previously known as IMEI locking and now called USAT pairing has been standardized. Thanks to this, the SIM is linked to a connected object or a type of connected object.



Pairing for security

The SIM cannot be used in any type of device other than it was intended for.

Ensuring security, now and for years to come

To enable durable security through the years, the SIM has to be ready for future security evolutions. One of these evolutions is the TUAK algorithm that will replace Milenage, providing a longer key length for increased security. It can be embedded in the SIM now and activated over-the-air later, when the network is ready to switch to it.

Durable security: a future-proof warranty

For a safer connected world, IDEMIA is actively working with MNOs and other IoT network operators to secure Low Power Wide Area Networks in both licensed and non-licensed spectrums.

Join us on

www.idemia.com