SONY

White paper

LTE Cat-M1 for IoT wearables an introduction

Published: June 2020
Document no: v1

mSafety

Contributing Companies:

- Sony Mobile Communications
- Sony Network Communications Europe

With technology providers:

- Altair Semiconductors
- Sony Semiconductor Solutions
- Telenor Connexion
- Sony Research Centre Lund

Table of contents

Executive summary

LTE Cat-M1 provides cellular radio technology that is designed for use in cases requiring low-power IoT communication – such as in safety and eHealth wearables. This white paper puts forward the main reasons why LTE Cat-M1 is a good fit compared to standard 4G LTE communication (called Cat 1 or higher). It also explains common IoT communication protocols and outlines what you need to consider when deploying them in an LTE Cat-M1 network.

This white paper is published by:
Sony Network Communications Europe

Mobilvägen 4
223 62 Lund
Sweden

iot.sonynetworkcom.com

Introduction and scope

Most legacy standards for mobile communications – such as GSM, WCDMA and LTE – were designed for voice-centric or mobile broadband (MBB) devices that needed to communicate a relatively large amount of data. However, lately there has been rapid growth in the market for smaller cellular connected devices that require a long battery life. Using legacy standards in such cases would be inefficient since they only need to transmit a limited amount of data. This development has created a need for new, modified cellular connectivity protocols.

One example of such a protocol is the new version of LTE. It is called LTE-M, and the corresponding UE category is called LTE Cat-M1. Numerous optimisations have been introduced for LTE Cat-M1 technology, enabling it to evolve continuously along with 3GPP standardisation.

In this paper, we explain the main differences between LTE Cat-M1 and "4G LTE" which is found in most modern smart phones. We also elaborate on some of the key features which have been introduced at each 3GPP release.

At the end of this paper, we describe popular IoT communication protocols and outline how to ensure a secure, power-efficient IoT service running on LTE Cat-M1 networks.

Abbreviations

IoT	Internet of Things
LTE Cat-M1	Cellular technology 4G variant dedicated for IoT applications
LWM2M	Lightweight Machine to Machine
MQTT	Message Queue Telemetry Transport
MTC	Machine Type Communication
OASIS	Organization for the Advancement of Structured Information
PUR	Preconfigured Uplink Resource
RSSI	Received Signal Strength Indication
TLS	Transport Layer Security

Basic LTE technology

LTE technology, which is also known as fourth generation mobile communications, was developed as an evolution of 3G WCDMA. Its main goal was to further increase the capabilities and capacities of mobile networks so they could handle increased data rates and reduced latencies. Its development was driven by the increase in mobile broadband traffic and video streaming.

LTE allowed for more data to be transmitted at higher data rates than was possible with 3G. In the early stages of LTE deployment, the target peak data rates for downlink and uplink direction were 100 Mbps and 50 Mbps respectively. Now, the LTE peak data rates can be up to 3 Gbps and 1 Gbps, significantly improving the user experience.

But what about the need for evolution of mobile communications in the opposite direction i.e. optimization for lower, not higher data rates? Some devices, such as machinery or sensors, transmit data at pre-set time intervals (not continuously) and each block of data is relatively small. The development of these devices has triggered a separate standardisation activity – one specifically targeting the need for low power consumption and enabling the transmission of small amounts of data over a longer period of time.

The terms Machine-to-Machine (M2M) communication and Machine Type Communication (MTC) are used when referring to cases in which small amounts of data are transmitted fairly infrequently. To cater efficiently for this data traffic pattern, the industry began examining how to reach a device battery life of months and, in certain cases even years, employing a battery that was even smaller than that of a typical smartphone. In addition, they identified the need to offer better service coverage than was possible with LTE.

Figure 1: Evolution and bi-polarisation of radio access techniques

Between 2012 and the present day, a range of new radio access technologies have been introduced into the standard for LTE (see figure 1).

LTE-M is one of these, and its introduction led to the identification of a separate device category: category M1 (Cat-M1). Two other examples of technologies developed for similar machine-type communications within 3GPP standardisation are LTE Category 1, and Narrow-band IoT (NB-IoT).

In the following sections, we describe LTE-M technology in more detail. We summarise the technology concepts being introduced and their benefits in handheld devices with size and power constraints.

4G LTE standard technology

Legacy LTE technology was tailored for real-time communication such as voice and video transmission and mobile broadband communications. Today, these are typically supported in a smartphone device, and below we list some of the key aspects of the device/modem design.

- **Operating with large frequency bandwidth**
  An LTE standard device must support an operating frequency bandwidth of at least 20 MHz. This has continuously evolved over time, so devices can now typically support N times 20 MHz. This feature, known as 'carrier aggregation', allows for very high data rates.

- **Multiple antenna configuration**
  In order to increase capacity, a device can be operated with a multiple antenna configuration. Today, an LTE device can be designed to support 2-4 number of transmit antennas and 2-4 number of received antennas— increasing both the diversity and spatial multiplexing of data transmission.

- **High processing power**
  In this case, the device is designed to support a higher modulation scheme, such as 1024 QAM and a high capacity of transport block size and parallel data streaming.

- **Full duplex operation**
  This means the device can support simultaneous uplink and downlink operations.

The LTE standard initially gave rise to a category of low complexity devices known as LTE category 1. Its key properties were to support legacy LTE bandwidth of 20 MHz, one and two antenna configurations for uplink and downlink, full duplex operation, and transport block size of 10kbps and 5bps for downlink and uplink, respectively.

Although these properties enable a reduction in device complexity, in practice, the LTE category 1 can still support real-time communication and relatively low/medium quality mobile broadband. Consequently, it is still not optimised for machine type communication (MTC).

In the next section, we look at LTE Cat-M1, which is optimised for M2M or Machine-type communication.

LTE Cat-M1

LTE Cat-M1 was introduced in 3GPP global cellular standardization, release 13. Its main purpose was to reduce device complexity and power consumption while increasing coverage. LTE Cat-M1 devices support up-to 1 Mbps peak data rate for both uplink and downlink transmission. The network is also designed to support a huge number of LTE Cat-M1 devices.

Any 4G LTE infrastructure can easily be updated to support LTE Cat-M1 devices (via e.g. software updates). This eases deployment and increases the availability of 4G LTE supporting LTE Cat-M1 devices in the existing infrastructure. These objectives are essential aspects for IoT wearable use cases.

Low complexity device

Reducing complexity generally also means reducing costs. LTE Cat-M1 targets various IoT centric use-cases, such as smart meters, sensors and wearables. With smart meters such as power and water meters, devices are often deployed on a large scale. For this reason, the product cost needs to be relatively low. The same is true for wearables where the cost and size of communication modules need to be lower than those of legacy LTE devices. Below we outline the technical objectives for low complexity devices:

- **Operation with single antenna**
  Having a single antenna for transmitting and/or receiving limits the number of transmission chains to one, which can significantly reduce the cost of components.
- **Reduced bandwidth**
  LTE Cat-M1 is designed to operate with a maximum bandwidth of 1.4 MHz. This is lower than LTE cell bandwidth (10 MHz or 20 MHz) and it enables a simpler modem design as well as reducing power consumption.
- **Integrated device**
  Reducing the number of components makes it possible to have an integrated device, such as a single chip solution. This is relevant when e.g. LTE Cat-M1 is designed for low power transmission (20 dBm) with an integrated power amplifier.
- **Half duplex operation**
  Half duplex operation basically means sharing of the transmit-and-receive chain, further reducing the number of components.

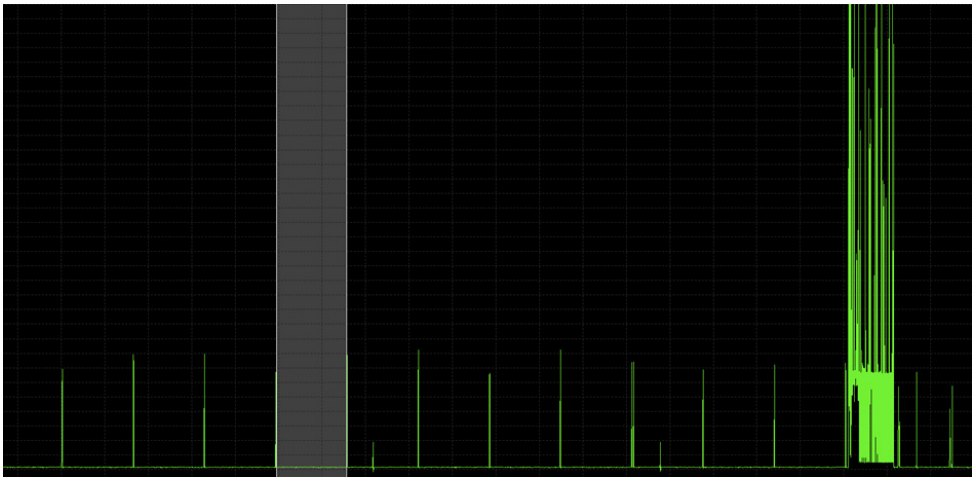
Low power consumption

One of the LTE Cat-M1's essential objectives is to achieve 10 years of battery life in use-cases such as smart meters. This is a significantly longer battery life than any smartphone can achieve (typically smartphone have just 1-2 days of battery life). Depending on the traffic model and usage, wearable devices can have a battery life of around 7+ days. Below are some of the new features that enable low power consumption:

- **Enhanced DRX (eDRX)**
  When a legacy LTE device is in idle mode, the sleep cycle plays a key role in determining battery life. Legacy LTE technology supports up to 10.24 sec of sleep time during discontinuous reception (DRX operation). By contrast, an LTE device would typically be configured with a DRX cycle (paging window) of 1.28 sec, during which time the device can be contacted by the network – enabling a voice call setup delay that is within tolerable limits. For example, when a phone user gets a call, the network can reach an LTE device within around 1 sec. LTE Cat-M1 is designed for IoT devices that do not necessarily need real-time communications and can support up to 40 minutes of enhanced DRX operation. This is a significant increase in sleep cycle time, and it reduces power consumption for LTE Cat-M1 devices, when configured by the network.

- **Power save mode (PSM)**
  An LTE Cat-M1 device can activate PSM by indicating to the network that it is going to enter a dormant state. In this case, the device will almost completely switch off its communication module. Please note that the device becomes unreachable in power save mode, so it should only be used in cases where this does not pose a risk. Another way that PSM reduces power consumption is through the dormant state of the modem. Once the device is back in connected mode, it needs to go through the initial steps to gain access (i.e. synchronization, cell identification, and so on.)

Below, we illustrate a typical power profile for a case using eDRX at 40s (time between the paging instead of every 1.28sec), which gives a much lower standby current while still being connected to the network. It also reduces the number of times the network can ask the device to carry out a new cell search and report. The high current peak on the left shows when the device is sending data to the network, including some retransmission peaks.



Coverage enhancements

LTE Cat-M1 is designed to support 20 dB enhancements in coverage (improved link budget) compared to legacy LTE. Basically, an LTE Cat-M1 device can receive and process data even when the signal is 100 times lower than the signal for a legacy LTE device. The key feature that supports coverage enhancement is repetitive transmissions. Rather than a single transmission (as in legacy LTE devices) LTE Cat-M1 devices can support up to 2000 times repetitive transmissions. The receiver processes and accumulates the repetitive transmission in order to retrieve the transmitted information.

In the white paper "Use of LTE Cat-M1 technology in wearable for improved safety in near-shore activities", you can find out about our field trials for connectivity range in a real-life environment.

Support for mass deployment

Considering that LTE Cat-M1 devices or general IoT devices can be deployed en masse, the network is designed to support efficient signalling and reduced overheads in both downlink and uplink transmission.

Figure 2 summarises LTE Cat-M1 features. For a performance evaluation of LTE Cat-M1, see the white paper "Coverage Analysis of LTE M – Category M1 – Version 1.0 January 2017" [1].

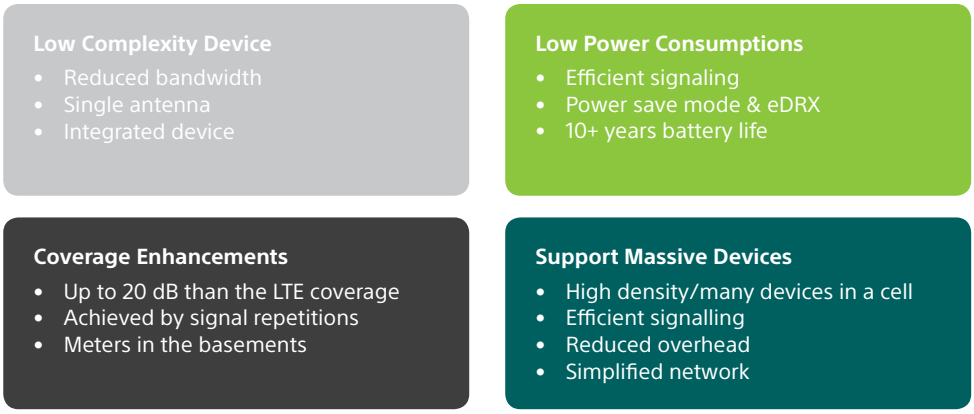


Figure 2: LTE Cat-M1 key features

Evolution of LTE Cat-M1

One of the major advantages of introducing a technology by global standardisation (e.g. 3GPP) is that it enables continuous evolution and the introduction of new features. LTE Cat-M1 has evolved continuously and new features have been added in each 3GPP release, ever since its first introduction in release 13. Figure 3 shows features added at each release.

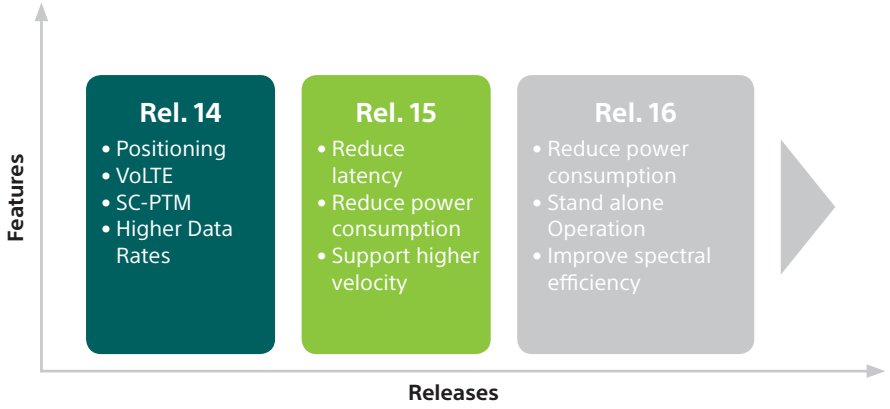


Figure 3: Evolution of LTE Cat-M1 key features

3GPP release 14

- The introduction of device localisation using LTE radio signal. Thanks to a positioning feature introduced in LTE Cat-M1, it became possible to locate the device without additional or dedicated positioning equipment, such as GPS.
- It became possible to enable voice over LTE in LTE Cat-M1 devices.
- The addition of SC-PTM facilitated the transmission of the broadcast message in the most efficient manner, such as software updates.
- Since many IoT use cases predominantly require uplink transmission, the peak data rate was increased to up to 3 Mbps.

3GPP Release 15

- Latency was reduced by optimising the initial access process. This included the introduction of a re-synchronisation signal and more efficient transmission of system information.
- Power consumption was reduced by the introduction of a wake-up signal (WUS) operation.
- An early data transmission (EDT) mechanism contributed to further reductions in both latency and power consumption.
- Release 15 is also known as the point at which 5G was introduced. LTE Cat-M1 was identified as one of technologies that can fulfil 5G requirements. Hence, it is compliant and can co-exist in a 5G network. Our report on LTE Cat-M1 and 5G requirements can be found in [3].

3GPP Release 16

- Power consumption was further reduced by the grouping of wake-up signal (WUS) mechanisms and by preconfigured uplink resource (PUR) transmission.
- It also became possible for a network to operate stand-alone LTE Cat-M1 cell with high efficiency.

IoT communication protocols

The introduction of IoT services with hardware created a demand for efficient IoT communication protocols. Devices typically have limitations with regard to power consumption and processing capacity so it must be possible to run the protocols on narrow band communication links.

Given concerns about data security and privacy, services must also be secure. In the following sections, we describe two popular IoT protocols (MQTT & LWM2M) and outline what is needed to secure an IoT service.

MQTT Protocol

MQTT was initially developed by engineers at IBM 1999 to monitor oil pipelines using satellite communication links. Since then, the protocol has evolved and MQTT is now a well-established open standard managed by OASIS [4]. MQTT is now a popular protocol for IoT devices, largely because it is light weight and bandwidth/power efficient. For example, the minimum overhead imposed by MQTT can be as low as 2 bytes.

The key component in MQTT-based solutions is the message broker which routes messages to the correct destination. MQTT clients that connect to the message broker can be IoT devices, but they can also be cloud servers providing IoT services (i.e. an application server).

When an MQTT client connects to a message broker, the client can start to publish and subscribe to messages. This creates a solution whereby the publisher of messages does not need to know which clients have subscribed to messages. This set-up is called a publish–subscribe message pattern, and it enables new services to be added just by subscribing to messages. Figure 4 below shows a system in which IoT devices publish information to a message broker, and IoT Services subscribe to the published data from the devices.

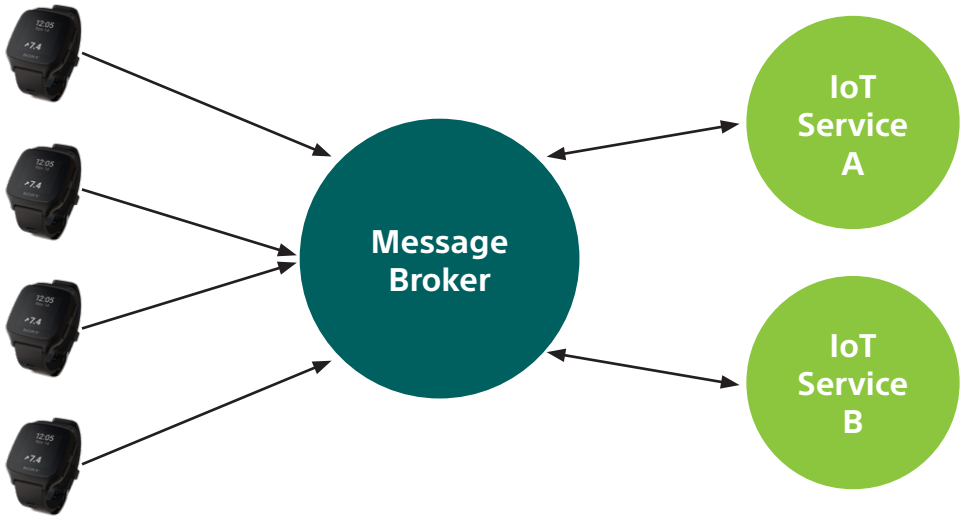


Figure 4: Illustration of MQTT message broker with MQTT clients

Messages to the message broker are always pubished according to a message topic with a requested Quality of Service (QoS). Each topic can also have sub-topics.

The structured use of topic and sub-topic names makes it possible to create a system in which services to subscribe to a subset of messages have a degree of flexibility. For example, a temperature sensor could publish all measurements on a topic: */{id of the device}/temp*. For an IoT service gathering temperature sensor data the IoT service should subscribe to the topic */+/temp*, where '+' is a wild card meaning that the IoT service will get all messages reported to the sub topic */temp* independently of device ID.

The MQTT protocol operates above the TLS and TCP/IP protocol stacks, as illustrated in figure 5 below. TLS provides the transport security and TCP provides the transport protocol. The stack leverages widely-deployed, proven technologies.

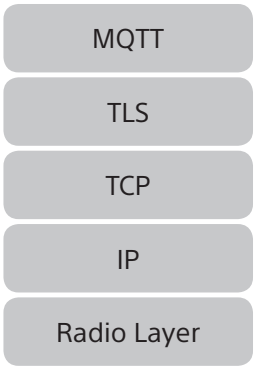


Figure 5: MQTT protocol stack

When deploying a system based on the MQTT protocol there are several practical aspects that need to be considered, depending on use case requirements.

The MQTT protocol is designed to be lightweight and bandwidth/power efficient. However, in order to make efficient use of radio resources and ensure a secure, power-efficient solution, you need a deep understanding of the interaction across the entire protocol stack. In many cases it is the radio that consumes the most power in an IoT device.

Even though MQTT is a lightweight protocol, it can be costly to run the underlying TLS protocol in terms of computational resources and the number of bytes sent over the air.

The TLS session establishment always starts with TLS full handshake to establish a common security context between the protocol end points. A full TLS handshake requires approximately 3-5 KB of data and involves CPU intensive public/private key cryptography when, for example, certificates are used to authenticate MQTT clients and brokers. The overhead can be reduced by using an abbreviated TLS handshake that allows an old security context to be resumed over connection cycles.

In many cases, it is possible to have long-lived sessions that reduce the TLS handshake overhead even more than an abbreviated handshake. In this case, the handshake is only needed when re-negotiating a new security context.

Long-lived sessions are indeed possible with the new low power features described in section LTE Cat-M1. Even if the device goes to low power mode, the device can keep its IP-address, and a long-lived session can take place – provided the same security context is applicable in low power mode.

If long-lived connections are used and there are Network Address Translators (NAT) in the request/response chain, the configuration of TCP connection timers and port allocations must take this into account. In practice, devices often need to send keep-alive messages to prevent the connection being timed out, or to keep the port in the NAT.

Another aspect of the MQTT protocol, is that the TLS protocol provides transport security between the MQTT client and MQTT message broker. In other words, it does not provide end to end security between two MQTT clients. Rather, it is a hop-by-hop security solution. The most common way of adressing this is to locate the message broker in a trusted environment with strictly controlled access. Whether or not this is sufficient depends on the security requirements of the service provided. When security equirements are stricter, the MQTT protocol must be complemented with a further layer of security in the application.

End-to-end security

As stated above, TLS does not provide end-to-end (E2E) security between two MQTT clients because it's a hop-by-hop solution. To provide E2E security, an additional application layer security protocol would be needed. This solution would have to guarantee secrecy, even if the communication is intercepted.

An implementation of E2E encryption could be based on the Noise protocol framework that specifies a set of handshake patterns for building a secure protocol. Noise protocols support mutual and optional authentication, identity hiding, forward secrecy, zero round-trip encryption, and other advanced features. Implementations use Ephemeral/Static Diffie-Hellman key exchange, X25519, in which the sender creates a keypair every time a key is exchanged. However, the receiver keypair is static. The two parties agree on a shared secret exchanging only public information, and the shared secret is then used to encrypt the payload application data.

IoT Security

There are numerous dimensions to IoT Security including communication security, identity management, resilience and privacy. In this section, we describe the steps involved in provisioning and onboarding a device to an IoT service.

As stated in previous sections, TLS and DTLS are common protocols used for securing the communication link between an IoT device and an IoT service. However, since IoT devices often do not involve humans, security cannot rely on an end user entering credentials. In fact, in many cases the IoT device might not even have a screen or keyboard where credentials *can* be entered.

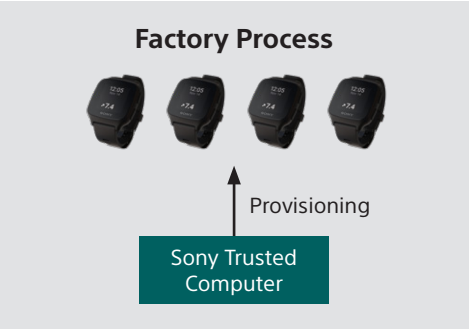


Figure 6: Provisioning in the factory

For IoT devices, security is often managed by adding a key-pair to the device, either during production or before the device is onboarded to an IoT service. The key-pair consists of a public and a private key, both of which are generated with an algorithm using input from high-quality entropy sources. The public key is embedded into a client certificate and signed by a certificate authority.

The client certificate and private key are then added to the device along with other settings that are known during the production. Meanwhile, the private key is stored in a secure key storage in order to prevent unauthorised access. At this point, the device is also provisioned with information on the certificate authorities and servers that are trusted by the device. This is carried out in a trusted environment to prevent malicious keys and certificates being added during production. When complete, the IoT device and IoT Service can be mutually authenticated.

Since it is not always feasible to provision the device with all parameters during production, an address to a trusted server is usually added, allowing for further provisioning after production.

Summary

- In this whitepaper we described the LTE Cat-M1 standard – an evolution intended for low-power, high-latency and low-data rate IOT devices, in contrast to the other LTE track (for 5G) which is focused on high bandwidth, low-latency applications that consume much more power.
- A typical wearable device with this cellular technology will have approximately 7+ days of battery time, when using all the low-power features the standard defines, and when the wearable is designed for limited battery size.
- For IoT device management, we presented the basic principles of the MQTT protocol and outlined how it is used for managing devices. Finally, we presented the TLS/DTLS protocol that is used to ensure security in this type of device, and which is a very important part of any deployment.

References

[1] – White paper – Coverage analysis of LTE M – Category M1 – version 1.0 January 2017
https://altair-semi.com/products/alt1250/coverage-analysis-of-lte-cat-m1-white-paper/

[2] – GSMA IOT deployment map -
https://www.gsma.com/iot/deployment-map/#deployments

[3] - White paper – Evaluation of LTE-M towards 5G IoT requirements
https://www.gsma.com/iot/resources/evaluation-of-lte-m-towards-5g-iot-requirements/

[4] - OASIS MQTT version 3.1.1MQTT specification
http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html

Trademark and acknowlegement

Visit iot.sonynetworkcom.com for more information.

Contact

Sony Network Communications Europe BV
Mobilvägen 4
223 62 Lund
Sweden

E-mail: msafety@sony.com

Website: iot.sonynetworkcom.com/msafety