Mobile IoT

Mobile IoT = **TRUSTED IoT**

3GPP LOW POWER WIDE AREA TECHNOLOGIES

GSMA WHITE PAPER

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

The growing usage of connected devices, machines and vehicles is making organisations more effective and enriching the lives of individuals. To support the development of this Internet of Things (IoT), the mobile industry has developed and standardised a new class of low power wide area (LPWA) technologies that help network operators to tailor the cost, coverage and power consumption of connectivity for specific IoT applications.

Three low power wide area network (WAN) solutions operating in licensed spectrum bands – Extended Coverage GSM for Internet of Things (EC-GSM-IoT), Long Term Evolution Machine Type Communications Category M1 (LTE MTC Cat M1, also referred to as LTE-M) and Narrowband IoT (NB-IoT) – have emerged to address the diverse requirements of the IoT market. Mobile network operators (MNOs) will implement these technologies, which have been standardised by 3rd Generation Partnership Project (3GPP) in its Release 13, through the modification of their cellular networks, bringing to the market a wide range of benefits.

The main advantage of 3GPP-standardised LPWA solutions, compared to proprietary technologies, is that they have the support of a huge ecosystem with more than 400 individual members. 3GPP stipulates that standardised technologies deliver a minimum level of performance, regardless of the vendor. Standardisation also ensures interoperability across vendors and mobile operators. Moreover, standardisation by 3GPP helps technologies to reach scale due to the number of companies that implement these standards.

The standardised LPWA technologies possess several characteristics that make them particularly attractive:

- Low power consumption (to the range of nanoamp) that enables devices to operate for 10 years on a single charge
- Low device unit cost
- Improved outdoor and indoor penetration coverage compared with existing wide area technologies
- Secure connectivity and strong authentication
- Optimised data transfer (supports small, intermittent blocks of data)
- Simplified network topology and deployment
- Integrated into a unified/horizontal Internet of Things (IoT)/ Machine-to-Machine (M2M) platform, where operators have this in place
- Network scalability for capacity upgrade

Using low power solutions in licensed spectrum, MNOs can provide proven, secure and reliable end-to-end IoT platforms that allow their customers to scale and manage their business requirements without adverse risk to capacity, security of data and quality of service in an independently regulated environment. MNOs can also offer unrivalled global network coverage, and technical and business support to react to customers' changing needs. Last, but not least, MNOs can offer a full range of connectivity options through their IoT platforms, including device management, application enablement and data analytics.

In August 2015, the GSMA launched the Mobile IoT Initiative (MIoT). Backed by many of the world's leading mobile operators, device makers, security solution providers, chipset, module and infrastructure companies, the MIoT Initiative is facilitating demonstrations, proofs of concept and trials of the three complementary LPWA licensed spectrum technologies.

Following trials and pre-commercial pilots during 2016, commercial launches will take place world-wide in 2017.

To support the development of efficient, trusted and reliable IoT services that can scale as the market grows, the GSMA's Mobile IoT Initiative is seeking to accelerate the commercial availability of LPWA solutions in licensed spectrum.

Businesses that work with mobile operators to pilot these technologies early will gain insights into their potential that could give them a competitive edge over rivals.

2 INTRODUCTION

2.1 OVERVIEW

Mobile network operators are implementing new capabilities to support emerging Internet of Things (IoT) and machine-to-machine (M2M) services. New low power wide area technologies have evolved to enable MNOs to play a central role in the growing IoT market. In the context of this paper, low power refers to the ability of an IoT device to function for many years on a single battery charge, while at the same time it is able to communicate from locations where shadowing and path loss would limit the usefulness of more traditional cellular technologies.

The GSMA Mobile IoT Initiative participants, consisting of 35 operators and 22 vendors, identified and analysed 24 IoT use cases across seven application categories, which require wide area coverage, strong propagation (for example, to locations deep indoors), low cost or no access to the mains power.

This report presents the results of the analysis of the IoT use cases, and summarises the technical characteristics and deployment considerations of three low power wide area technologies standardised and published in 3GPP Release 13. The 3GPP family of LPWA technologies includes Enhanced Coverage – GSM–IoT (EC-GSM-IoT), LTE

Machine Type Communication Category M1 (LTE MTC Cat M1) and Narrowband – IoT (NB-IoT). This family of technologies is able to address the majority of IoT applications with a wide range of data throughput rates, costs and power options. This report considers the following aspects of the three LPWA technologies:

- Overview of each technology's technical aspects;
- The low power requirements of IoT applications;
- The relationship between the power consumption, battery performance and traffic load.

The details of the LPWA technologies described in this report reflect the knowledge of the GSMA Mobile IoT Initiative participants as of the end of July 2016.

2.2 SCOPE

Within the scope of this paper:

- **Analysis of licenced spectrum-based LPWA technologies.**
- **Analysis of key low power applications and services.**
- **Analysis of the relationship between power consumption and traffic load of IoT devices and applications, and between power consumption and coverage of LPWA networks.**

Short-range radio solutions are outside of the scope of this paper.

Note: All references made in this paper to LTE MTC Cat 1 are based on 3GPP Release 8 specifications; all references made to LTE MTC Cat 0 are based on 3GPP Release 12 specifications; all references made to LTE MTC Cat M1, EC-GSM-IoT and NB-IoT are based on 3GPP Release 13 specifications.

3 EMERGING MARKET FOR LOW POWER SERVICES AND APPLICATIONS

3.1 GROWING DEMAND FOR LOW POWER WIDE AREA SERVICES

LPWA networks will play an important role in connecting a range of Internet of Things devices that are low power consumption, long range, low cost and secured. The LPWA connections are likely to serve a diverse range of vertical industries and cover a range of applications and deployment scenarios for which existing mobile network technology may not be best placed to provide connectivity.

Analysys Mason, in its study for the GSMA published in April 2015 [1], identified seven categories of LPWA applications: agriculture and environment; consumer; industrial; logistics; smart building; smart city and utilities. The GSMA Low Power Use Case (LPUC) project group developed further segmentation, identifying and analysing 24 use cases across these seven categories. These are presented in Figure 1:

Figure 1: Key Low Power Applications

UTILITIES

- Gas and water metering, including smart meter consumption tracking and pipeline monitoring
- Mocrogeneration (monitoring status of generation equipment (solar, wind, thermal) with sensors
- Smart Grid (energy infrastructure monitoring)

LOGISTICS

- Asset tracking (e.g. industrial assets, containers, vehicles; location and status update)

INDUSTRIAL

- Industrial: tank process/safety monitoring, (petrochemical and waste storage monitoring, hazardous fluids tank monitoring, High RF interference environments)
- Industrial: machinery control (equipment status, factory control, process and safety monitoring)
- Industrial: propane tank monitoring (monitoring and reporting fill level of propane tanks for rural and suburban, residential and light industry customers)
- Vending machines - general (item filling level report, device diagnosis report, raising alarm on burglary attempt)
- Vending machines - privacy / data verification (e.g. age) for cashless payments

SMART CITY

- Parking sensors (to monitor and report availability of parking spaces)
- Waste management (monitoring status of waste containers to optimise the collection of waste)
- Smart lighting (remove management of street lights, e.g. remotely turning lights on or off or adjusting the strength of the light)

AGRICULTURE & ENVIRONMENT

- Agricultural applications - live stock tracking (fishing, cattle and wild animal tracking and monitoring)
- Agricultural - stationary tracking and monitoring of soil, temperature, weather conditions
- Environmental monitoring - near real-time (e.g. fire hydrant network monitoring, manhole cover status reporting, alerts for chemical emission levels)
- Environmental monitoring - data collection (Pollution, noise, rain, wind, river flow speed, health hazard, bore hole, etc)

CONSUMER & MEDICAL

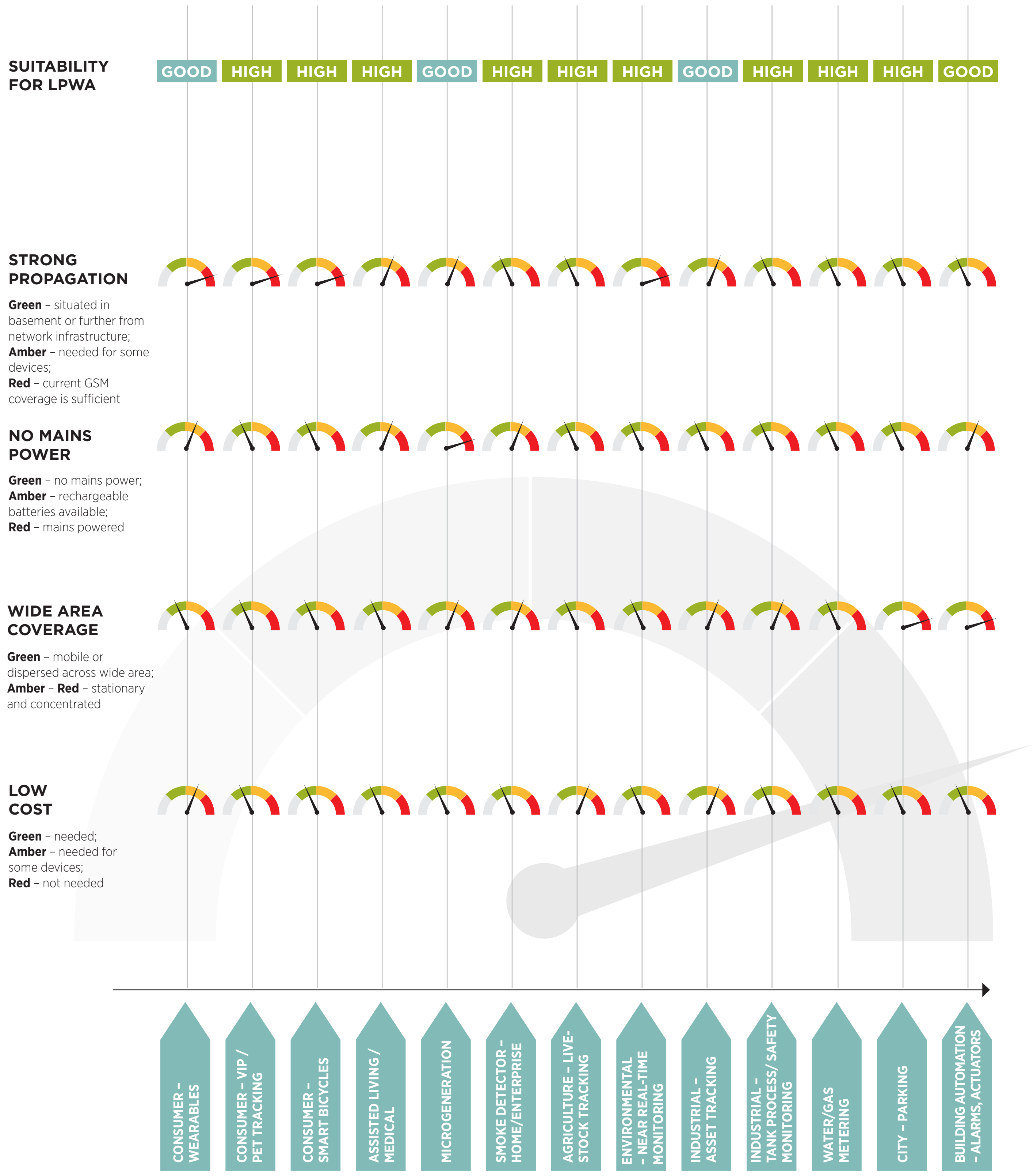
- Wearables (e.g. fashionable low-end leisure devices such as smart watches
- VIP/Pet tracking (e.g. reporting location of persons or pets, paging when queried)
- White goods/appliances (e.g. refrigerators, washing machines)
  Smart bicycles (tracking location)
- Assisted Living / Clinical remote monitoring (e.g. temperature sensors, alert buttons)

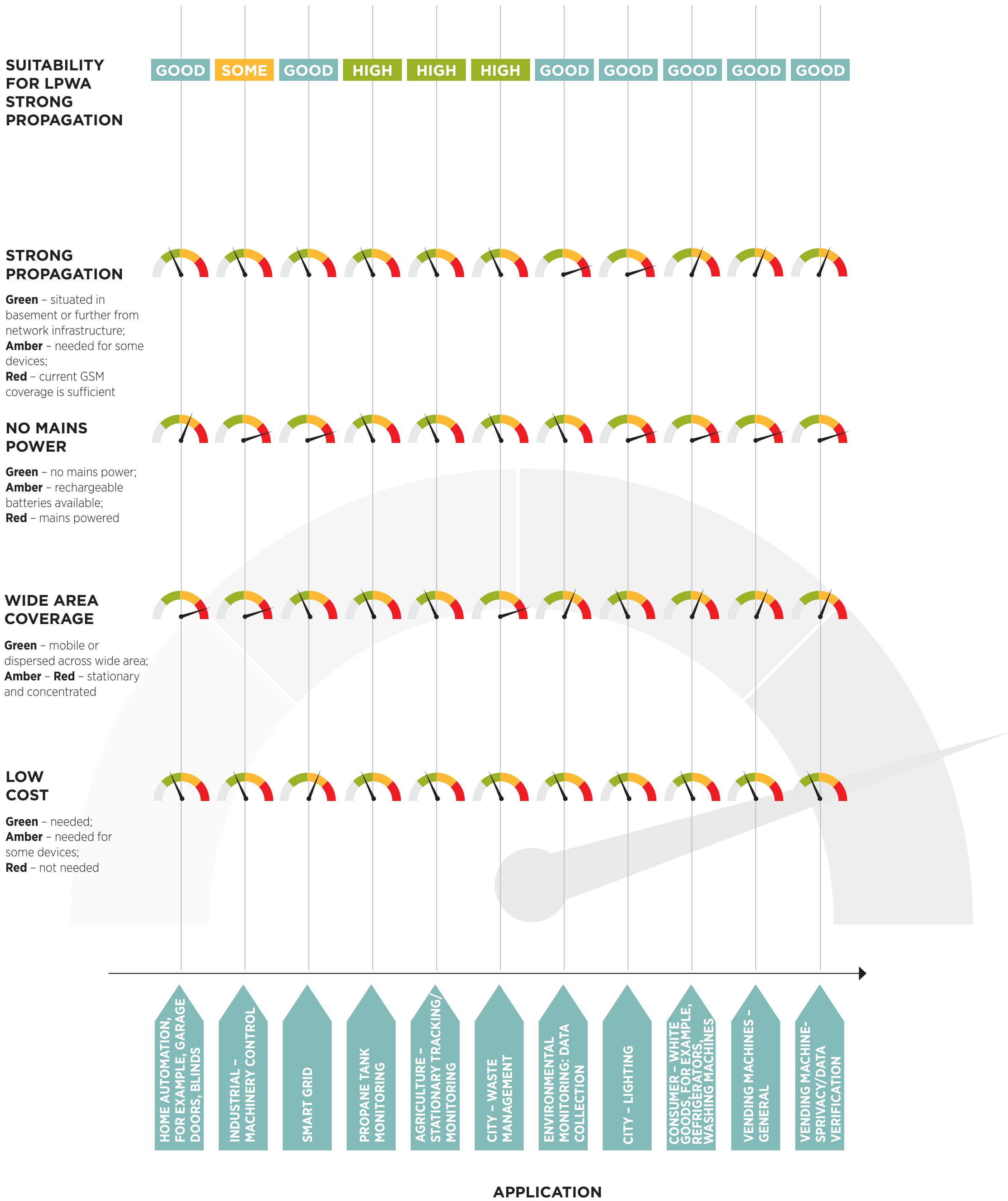
SMART BUILDINGS

- Smoke detectors (regular auto-test, battery check, real-time alerts to the relevant parties in case of fire)
- Alarm systems, atuators
- Home automation (e.g. values for temperature, humidity, control of garage doors, blinds)

All of these applications possess at least two of the following characteristics: a need for wide area coverage, strong propagation (for example, a location deep indoors), low cost and no access to the mains power, as illustrated in Table 1.

Table 1: Application Suitability to LPWA



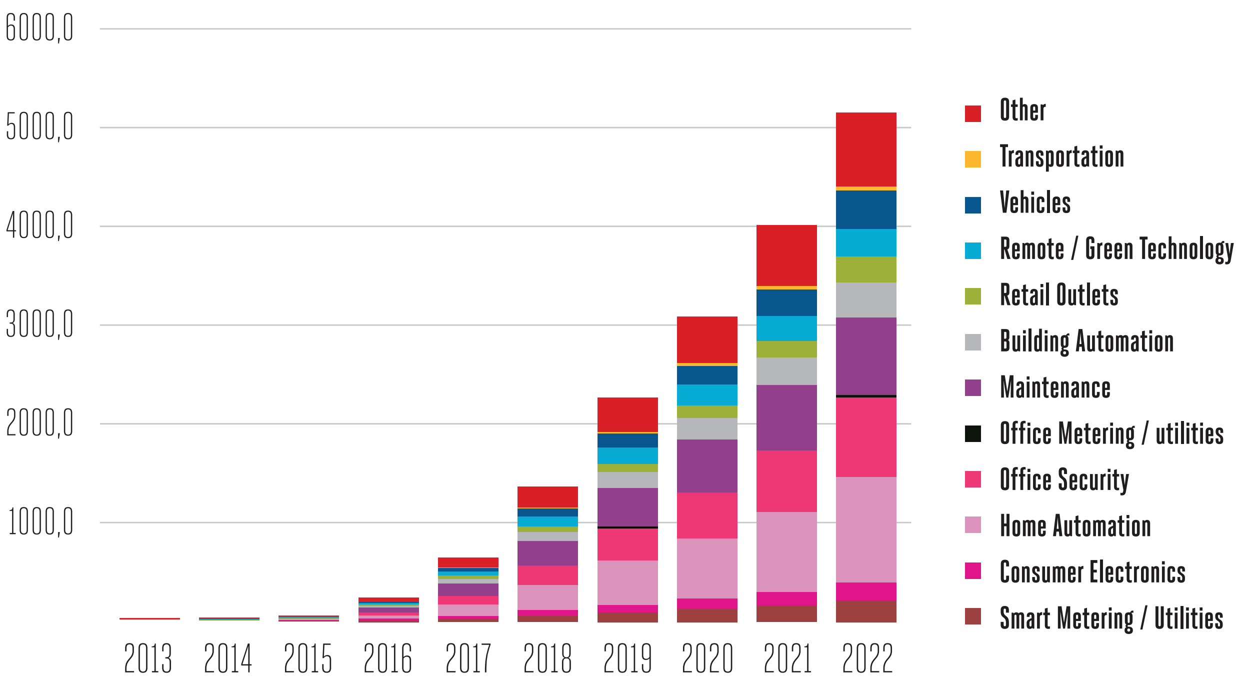

SUITABILITY FOR LPWA STRONG PROPAGATION
GOOD
SOME
GOOD
HIGH
HIGH
HIGH
GOOD
GOOD
GOOD
GOOD
GOOD
STRONG PROPAGATION
Green – situated in basement or further from network infrastructure;
Amber – needed for some devices;
Red – current GSM coverage is sufficient
NO MAINS POWER
Green – no mains power;
Amber – rechargeable batteries available;
Red – mains powered
WIDE AREA COVERAGE
Green – mobile or dispersed across wide area;
Amber - Red – stationary and concentrated
LOW COST
Green – needed;
Amber – needed for some devices;
Red – not needed
HOME AUTOMATION, FOR EXAMPLE, GARAGE DOORS, BLINDS
INDUSTRIAL – MACHINERY CONTROL
SMART GRID
PROPANE TANK MONITORING
AGRICULTURE – STATIONARY TRACKING/ MONITORING
CITY – WASTE MANAGEMENT
ENVIRONMENTAL MONITORING: DATA COLLECTION
CITY – LIGHTING
CONSUMER – WHITE GOODS, FOR EXAMPLE, REFRIGERATORS, WASHING MACHINES
VENDING MACHINES – GENERAL
VENDING MACHINE- SPRIVACY/DATA VERIFICATION
APPLICATION

3.2 LOW POWER APPLICATION ADDRESSABLE MARKET

Analysts anticipate the number of LPWA connections is likely to grow gradually over the next two years before surging in 2018 as standardised LPWA technologies gain economies of scale and are proven in the marketplace.

Strategy Analytics, for example, forecasts there will be well over one billion LPWA connections worldwide by the end of 2018 and more than two billion by the end of 2019 (see Figure 2). It predicts this figure will rise to more than five billion by the end of 2022. These forecasts include all the LPWA technologies that Strategy Analytics expects to be available in the market: the 3GPP standards-based LPWA solutions in licensed spectrum, including EC-GSM-IoT, LTE MTC Cat M1 and NB-IoT, as well as unlicensed spectrum solutions. Short-range radio technologies used in the access portion of IoT connectivity are excluded from these forecasts.

Figure 2: Global LPWA Connections Share, by Application (millions)

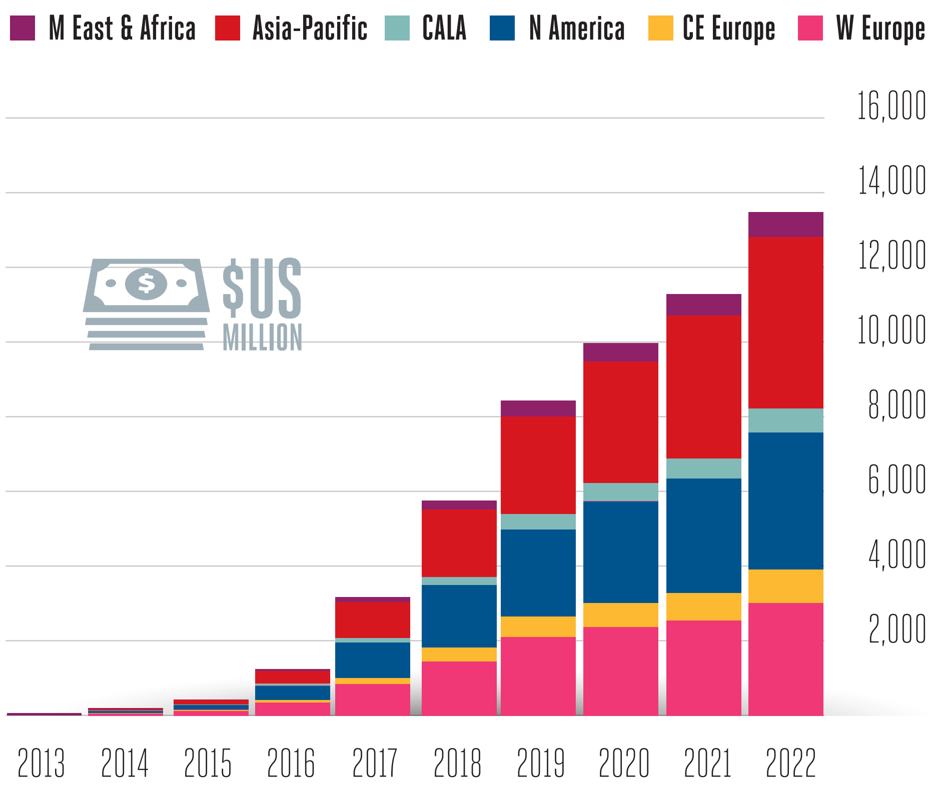


Source: Strategy Analytics

LPWA connectivity is likely to be widely used in both developed markets and emerging markets. In the latter, it could have a particularly significant impact on agricultural productivity and the efficiency of energy and water networks. Uptake is also likely to be strong in those countries building new smart cities or retrofitting IoT applications to existing urban areas.

By 2022, Strategy Analytics anticipates that Asia-Pacific will be the largest LPWA market, worth $4.6 billion, followed by North America and Western Europe (see Figure 3). Globally, Strategy Analytics forecasts LPWA revenue will reach $13.9 billion in 2022.

Figure 3: Global LPWA Annual Revenue, 2013-2022 (US$ million)



Source: Strategy Analytics, February 2016

3.3 LOW POWER APPLICATION PROFILES

To further analyse the LPWA applications outlined in section 3.1, the GSMA collected a range of requirements for each use case, including battery life, coverage, total expected daily load, latency and mobility.

Based on similarities in these requirements, 24 use cases were grouped into four families as described below, in order to simplify their analysis.

Application Family Type 1 includes applications and use cases that involve tracking persons or objects, such as children or pets; assisted living and remote health monitoring; wearables; and bicycle tracking.

The key requirements for this application family are as follows:

- Most messages for application family Type 1 are event-triggered, for example, when a tracked object is lost, several messages per hour will be sent to determine its location. In the uplink, as many as 8 messages per hour at 50 bytes per message could be sent.
- All applications of this type require bi-directional communication. Downlink is required for four categories of communication:

    1. Acknowledgment of the message delivery, for example, for people and high value asset tracking;
    2. Actuator control, for example, for geofencing and paging;
    3. For security key exchange;
    4. For any application firmware updates and patches.

- For wearables and for human tracking, high mobility is required.
- For wearables, assisted living, and for human tracking, voice support is often required.
- The security requirements for these applications are high, as personal data is involved.

Application Family Type 2 includes industrial asset tracking, microgeneration, agricultural livestock and environmental near real time monitoring, for example, for fire hydrants, industrial tank processes or during a fire in woods. Some devices covered in this category are nomadic – for example, industrial assets and agricultural livestock that need to be tracked on the move.

- The majority of messages for family type 2 are event-triggered. For example, when a value read from a monitored device exceeds a pre-determined threshold, as many as 100 messages per day could be transmitted.
- Bi-directional communication is a requirement for all use cases in this family. Downlink connectivity is needed to support various needs:

  1. Message acknowledgement is required for a range of use cases, such as microgeneration and near real-time environmental monitoring (e.g. fire hydrant monitoring, industrial tank process and safety monitoring);
  2. Security key exchange is needed for the same use cases as above;
  3. Actuator control might be needed for the environmental use cases, to modify the parameter configuration of reporting intervals;
  4. Firmware updates might be needed for most use cases, with patches rather than full images.

Application Family Type 3 includes two types of use cases. **Type 3a** use cases require deep indoor coverage, for example, smart water and gas metering, smart parking, smart building, home automation, smart grid and industrial machinery control.

For Type 3b use cases the primary requirement is extended outdoors/rural coverage, for example, smart cities, waste management, agricultural stationary asset monitoring, propane tank monitoring (residential and business) and environmental sensor data collection.

All devices in this category are stationary.

- The majority of messages for family types 3a and 3b are transmitted at regular intervals, in the range of one to four messages per hour.
- Bi-directional communication is required for the following:

  1. An acknowledgement of messages or alerts;
  2. Although actuator control is not a requirement for normal operation, it might enable some value added adjunct applications, for some devices, such as propane tanks.
  3. For firmware updates or patches.
  4. For configuration purposes.

Application Family Type 4 includes very diverse use cases, such as smart city lighting, home white goods and vending machines, grouped according to the fact that all of them are powered and therefore require only a limited battery life for back up purposes. All devices in this category are stationary.

- The transmission of messages in Family type 4 follows a variety of patterns. As few as three to five messages per day are read at regular intervals for such use cases as white goods or smart streetlights; as many as 100 messages per day can be event-triggered for a vending machine verification use case.
- Bi-directional communication is a requirement for all use cases in this family. Downlink connectivity is needed to support different needs:

1. Message acknowledgement for all use cases;
2. Actuator control: regular control to turn the lights on or off, or reduce (dim) power. Actuation might also be required for some white goods.
3. Firmware upgrades and patches are required for all use cases; time sync and configuration updates are required for some use cases, such as street lighting.

Family	TYPE 1	TYPE 2	TYPE 3, A AND B	TYPE 4
Type of application	Use cases that involve tracking persons or objects, for example, VIP/ pet tracking; assisted living and remote health monitoring; wearables; and bicycle tracking.	Industrial asset tracking, microgeneration, agricultural livestock and environmental near real time monitoring, for example, of fire hydrants, industrial tank processes or during fire in woods.	Type 3a – use cases that primarily require deep indoor coverage, for example, smart water and gas metering, smart parking, smart building, home automation, smart grid and industrial machinery control. Type 3b – use cases that primarily require extended outdoors/rural coverage, for example, smart cities waste management, agricultural stationary asset monitoring, propane tank monitoring (residential and business) and environmental sensor data collection.	Use cases that are mains powered, for example, smart city lighting, home white goods and vending machines.
Family properties	- Shorter to medium battery life - Medium coverage - Low to high mobility - Low to mid latency - Higher bandwidth - Voice is sometimes	- Medium battery life - Medium coverage - Stationary or nomadic - Mid to low latency	3a and 3b - Very long battery life - High coverage - Stationary - Medium to high latency	- Mains powered (requires backup) - Low/mid coverage - Stationary

Further comparison of requirements for each application group are presented in **Table 2:**

	TYPE 1	TYPE 2	TYPE 3, a AND b	TYPE 4
Family properties	➔ Shorter to medium battery life ➔ Medium coverage ➔ Low to high mobility ➔ Low to mid latency ➔ Higher bandwidth ➔ Voice is sometimes	➔ Medium battery life ➔ Medium coverage ➔ Stationary or nomadic ➔ Mid to low latency	3a and 3b ➔ Very long battery life ➔ High coverage ➔ Stationary ➔ Medium to high latency	➔ Mains powered (requires backup) ➔ Low/mid coverage ➔ Stationary
Battery life	5 years of battery might be required, although in many cases, the battery could be recharged, or replaced	5 - 10 years of battery life	10 - 15 years of battery life	All devices in this category will be mains powered. Battery will be required for back up.
Coverage	Most devices will need to be tracked while located outdoors. And some indoors coverage might also be needed.	Mostly outdoors	The most challenging coverage requirement, including deep rural and deep indoors (+20dB)	Both outdoors and indoors
Downlink require-ments	Acknowledgment Actuator control Security key exchange ➔ Firmware upgrade and patches	Acknowledgment Actuator control Security key exchange ➔ Firmware upgrade and patches	Acknowledgment Actuator control Configuration ➔ Firmware upgrade and patches	Acknowledgment Actuator control Security key exchange ➔ Firmware upgrade and patches
Mobility	High to low mobility, mostly nomadic	Nomadic (assets or live stock) and stationary	Stationary	Stationary
SLA	Medium to high	Medium to high; a response might be needed as quickly as possible in case of emergency events.	Medium to high	Varies: low for white goods, medium to high for the rest
Latency	Estimated at about 30 seconds, which is a human interaction tolerated latency. However, a lower latency of 2-5 seconds might be required in case of VIP tracking.	Under 10 seconds in most cases.	10 seconds for control use cases; 60 seconds for data collection.	Under 30 seconds for most use cases. But for vending machine privacy/data verification use case, under 1 second latency is needed.

Table 2: LPWA Application Family Communications Requirements

The detailed calculations for each application's daily data load and coverage requirements are presented in Annex A.

3.4 LPWA APPLICATIONS SECURITY REQUIREMENTS

A distinctive requirement across most LPWA use cases is a long battery life, which imposes restrictions on the amount of uplink and downlink data that can be sent to and from the device, plus the amount of processing power that is available to support network and application layer cryptographic security functions. Moreover, some LPWA devices deployed in remote physically inaccessible locations for more than 10 years will need to implement long-term security features; it may also be desirable to deploy security patches remotely.

There is a wide spectrum of security considerations that apply to LPWA services, such as:

- In LPWA devices, the energy overhead due to security must be minimised. This energy overhead arises both from the computing power required to perform cryptographic computation and from the need to transmit additional security-related data. One way to minimise this energy overhead would be to avoid stacking multiple, independent security layers.
- Many LPWA devices are located in remote locations, and are easily accessible to a partisan attacker. IoT application and communication providers must make these devices physically and electronically tamper-proof, and enable remote monitoring that checks for any signs of tampering.
- For critical infrastructure, critical functions or confidential personal data, there may be a need for stricter security requirements. Regulators set some of these requirements; for example, utilities industries tend to be heavily-regulated. MNOs need to assess if LPWA technologies are suitable for such use cases.
- In some LPWA use cases, involving data transmission through different independent platforms, it may be necessary to relocate credential management and access control in a separate entity.
- Due to power, bandwidth, processing power and memory constraints within LPWA devices, it may not be possible to implement common internet security protocols (such as transport layer security) and it may be impossible to implement multiple layers of security. The application layer is very likely to be dependent upon strong and efficient security features implemented in the LPWA transport layer to provide secure device registration and access to secure communication channels. If transport security cannot be realised or results in a high level of superimposition of security protocols, it might be better to consider application level security with data encryption/signature at the edge device and decryption at the customer back-end.
- IPv6 compatibility of the IoT end nodes should be observed. As well as avoiding the address exhaustion problem in IPv4, IPv6 allows direct interaction between end points and with platforms, simplifying the deployment of protocols in routers, avoiding intermediary steps introduced by NAT. Moreover, IPv6 allows for the establishment of VPNs in a natural way (native IPSec in IPv6) whenever an IoT end device is used in a mobile scenario (two IPv6 enabled devices can immediately connect via a VPN without intermediate elements).

Regardless of the type of LPWA application, there is a minimum set of security-related requirements for all, such as:

- Secure provisioning of device identity, network authentication credentials and communication cryptographic keys.
- Physical protection of device identity, network authentication credentials and communication cryptographic keys.
- Strong mutual authentication of the device and network.
- Strong (and efficient) cryptography to provide secure communication channels.

3.5 BENEFITS OF STANDARD BASED LOW POWER SERVICES BY MNOS

Today most existing IoT applications are supported via short-range wireless and mobile WAN technologies. However, these technologies are not well suited for some applications due to power consumptions levels, the associated costs or the complexity of the infrastructure. Therefore, a new breed of both proprietary LPWA solutions operating in unlicensed spectrum and 3GPP-standardised LPWA network solutions operating in licensed spectrum has emerged to fill the gap. Compared to proprietary solutions, standardised LPWA solutions bring a wide range of benefits. The most important is the support of a huge ecosystem made up of more than 400 individual members. Standards body 3GPP stipulates that the standard technologies meet a minimum level of performance, regardless of vendor. Standards also ensure interoperability across vendors and mobile operators. Furthermore, 3GPP standards benefit from economies of scale due to the large number of companies that implement these standards.

The LPWA technologies being standardised by 3GPP possess several characteristics that make them particularly attractive for market devices and applications requiring low mobility and low levels of data transfer:

- Low power consumption (to the range of nanoamp) that enable devices to last for 10 years on a single charge
- Optimised data transfer (supports small, intermittent blocks of data)
- Low device unit cost
- Simplified network topology and deployment
- Improved outdoor and indoor penetration coverage compared with existing wide area technologies
- Secured connectivity and strong authentication
- Integrated into a unified/horizontal IoT/M2M platform, where operators have this in place.
- Network scalability for capacity upgrade.

Using low power solutions operating in licensed spectrum, MNOs can offer proven, secure and reliable end-to-end IoT platforms that allow customers to scale and manage their business requirements without adverse risk to capacity, security of data and quality of service in an independently regulated environment. MNOs also offer unrivalled global network coverage, and technical and business support in response to customers' changing needs. Moreover, MNOs can offer a full range of connectivity options through their IoT platforms, including device management, application enablement and data analytics.

4 EMERGING LOW POWER TECHNOLOGIES

This section analyses the LPWA technologies standardised by 3GPP up to Release 13, with particular focus on the enhancements introduced in Release 13 for better support of M2M/IoT services.

In order to optimise the support of IoT by cellular networks, and compete with proprietary non-3GPP technologies in the lower data-rate end of the IoT / M2M market, 3GPP has specified three LPWA technologies: EC-GSM-IoT, LTE MTC Cat M1 and NB-IoT.

The common high-level objectives for all three technologies were to:

- Decrease user equipment (UE) complexity and thus cost
- Decrease power consumption
- Increase coverage (about 15-20dB improvement)

In addition, 3GPP defined more specific objectives for EC-GSM-IoT and NB-IoT to meet the following objectives [2]:

- Provide a data rate of at least 160 bps at 20 dB coverage extension beyond GPRS.
- Scale to support a massive number of MTC mobile stations (more than 50k per cell).
- Support a ten-year battery life with battery capacity of five watt-hours.
- Lower network complexity.
- Avoid negative impacts to legacy GSM/WCDMA/LTE system(s) and adhere to regulatory spectrum requirements.
- Minimise impacts on the GPRS/EDGE base station hardware. Identify core network architecture, security framework and radio access network-core network interface (e.g. S1 or Gb), and associated protocol stacks.
- Restrict use to a simple QoS model.
- There is no requirement for inter-RAT mobility, as it would increase the complexity and, therefore, the cost of the device.

4.1 RADIO ACCESS NETWORK ASPECTS

The three 3GPP LPWA technologies have been designed to support IoT services and to connect devices that are potentially constrained by their battery technologies. Each solution constrains the maximum user equipment (UE) transmission power to limit the consumption of power. This section provides an overview of the technical characteristics for each of the three technologies, with references to the relevant 3GPP documents.

LTE MACHINE TYPE COMMUNICATION (CAT 1, CAT 0, CAT M1) 4.1.1

From 3GPP Release 8, several categories of User Equipment (UE) are available. The category with the lowest performance is called Cat-1. This category is a full LTE category, which means that it offers two RF receiver chains; it is full duplex and supports Frequency Division Multiplexing (FDD) and Time Division Multiplexing (TDD). It supports 5Mbps on the uplink and 10Mbps on the downlink. This category is fully commercial and is already used in many existing M2M/IoT deployments.

In 3GPP Release 12, a Cat-0 UE was specified with the main object to reduce device complexity to be comparable to a GSM/GPRS mobile station (user device). It supports simplifications, such as allowing the device to operate with only one Rx chain (device category Cat-0), allowing half-duplex operation, and reducing the peak rate for uplink and downlink to 1Mbps. This category is expected to be in very limited commercial availability.

In 3GPP Release 13, a Cat-M1 UE was specified with three main objectives: reduce complexity further from Cat-0 UE, increase coverage by at least 15 dB, and improve battery life, while allowing reuse of the LTE installed base.
The main cost reduction for Cat-M1 from Cat-0 was to reduce bandwidth to six physical resource blocks (PRBs) (1.08MHz) and is referred to as a bandwidth-limited (BL) UE in the 3GPP specifications. Due to this bandwidth limitation, a new control channel and frequency hopping mechanism were specified. However, given most of the legacy LTE-broadcasted signalling for synchronisation and system information is sent in six PRBs, these channels did not need to be redesigned or re-broadcasted just for Cat-M1 UEs, thus significantly reducing signalling overhead. In addition, a new 20 dBm power amplifier (PA) option has been specified and, with this new PA class and all the other complexity reductions, integration into a single silicon die is practical, further reducing costs.

Cat-M1 allows an extended battery life of more than 10 years for a wide range of machine type communication use cases mainly through the use of power saving mode (PSM) and extended idle-mode Discontinuous Reception (eDRX), and connected mode eDRX, Cellular IoT (CIoT) control plane and user plane Evolved Packet System (EPS) optimisations for small data transmission. These features are explained in more detail in section 4.2.

Even with the reduced complexity, Cat-M1 UEs still provide many similar features to legacy LTE UEs, such as connected mode mobility and seamless hand-offs, efficient scheduling of frequency packets through semi persistent scheduling (SPS), and low latency packet while in connected mode. All these features open the possibility for a CAT-M1 UE to integrate voice in IoT applications in coverage mode A.

EXTENDED COVERAGE GSM IOT (EC-GSM-IOT) 4.1.2

Extended coverage GSM IoT (EC-GSM-IoT) is a 3GPP Release 13 feature based on eGPRS and designed as a high capacity, long range, low energy and low complexity cellular system for IoT communications [15].

The optimisations made in EC-GSM-IoT are backwards-compatible to previous releases to allow the technology to be introduced into existing GSM networks as a software upgrade on the radio network and also on the core network, as per section 4.2, enabling extensive coverage from day one, facilitating time to market. At the same time, this backwards-compatibility includes resource sharing between EC-GSM-IoT and legacy packet-switched services to allow for a gradual introduction of the technology in the network without the need to reserve dedicated resources for IoT. EC-GSM-IoT has been designed to offer coverage for M2M devices in locations with challenging radio coverage conditions.

On the device side, EC-GSM-IoT can either be implemented on existing EGPRS platforms or on stripped-down versions of existing platforms in order to realise the reduced complexity of EC-GSM-IoT. The optimisations can be summarised as:

- adapting the physical layer to support extended coverage,
- streamlining the protocol layer to minimise device complexity,
- improving upper layers to facilitate superior battery life, and
- the introduction of a security framework comparable with 4G standards.

NARROWBAND IOT (NB-IOT) 4.1.3

Narrowband IoT (NB-IoT) is a 3GPP Release 13 feature that reuses various principles and building blocks of the LTE physical layer and higher protocol layers to enable rapid standardisation and product development. NB-IoT has been designed to offer extended coverage compared to the traditional GSM networks. NB-IoT can improve UL capacity for users in bad coverage areas through single tone transmissions. New physical layer signals and channels, such as synchronisation signals and physical random access channel, are designed to meet the demanding requirement of extended coverage and ultra low device complexity. Higher protocols, signalling, and physical-layer processing requirements are greatly simplified in order to reduce UE power consumption and complexity. All references for NB-IoT UE in this document are for Category NB1 (CAT-NB1).

A battery life of more than 10 years can be supported for a wide range of machine type communication use cases. In addition to features of the physical layer design, such as low peak to average power ratio (PAPR) transmission technology, UE power consumption is optimised by using a PSM feature and eDRX. The complexity of NB-IoT devices can be even lower than that of GSM devices due to the changes to the synchronisation signal design and simplified physical layer procedures (e.g., single-process HARQ and relaxed timing relationships), simplifying the received signal processing, which supports the objective of a very low cost device. By using a numerology compatible with LTE numerology, NB-IoT can coexist with LTE. In addition, NB-IoT in standalone operation can coexist with 2G/3G/4G, according to 3GPP evaluations.

4.2 NON RADIO ACCESS NETWORK ASPECTS

This section provides an overview of the functions designed to support IoT services and also for devices that are potentially constrained by their battery technologies.

For simplicity, this paper will focus on a limited set of functional characteristics, as follows:

- Power saving mode (PSM)
- Extended idle-mode DRX cycle (eDRX)
- Enhancement for cellular IoT applications

The settings for all these functions need to be discussed and negotiated between service providers and mobile operators, in order to achieve the best performance.

POWER SAVING MODE (PSM) 4.2.1

This capability is focused on reducing the power consumption of a UE and it is defined for both LTE and GSM technologies and enables devices to enter a new deep sleep mode. PSM is intended for UEs designed for infrequent data transmission and that can accept a corresponding latency in the mobile terminating communication.

With this approach, the UE decides how often and for how long it needs to be active in order to transmit and receive data. Details are described in 3GPP TS 23.682-4.5.4 [26] , 3GPP TS 23.060-5.3.20 [27] and 3GPP TS 24.301-5.3.11 [10]. PSM mode is similar to power-off, but the UE remains registered with the network. This means that when the UE becomes active again there is no need to re-attach or re-establish PDN connections. While the UE is in PSM mode it is not reachable for mobile terminating services, but the network is aware of this and avoids paging the UE in vain. However, it is available for mobile terminating services during the time that the UE is in connected mode and for a period of active time after the connected mode is established.

The UE requests the PSM simply by including a timer (T3324) with the desired value in the attach, tracking area update (TAU) or routing area update. The T3324 will be the time the UE listens to the paging channel after having transitioned from connected to idle mode. When the timer expires, the UE enters PSM. The UE can also include a second timer, which is an extended T3412 in order to remain in PSM for longer than the T3412 broadcast by the network. The network accepts PSM by providing the actual value of the T3324 (and T3412) to be used in the attach/TAU/RAU accept procedure. The maximum duration, including T3412, is about 413 days.

A service may request the use of SMS to trigger an application on the UE to initiate communication with the Service Capability Server/Application Server (SCS/AS). If the UE is not available, the request will be delivered when the UE becomes reachable.

EXTENDED IDLE-MODE DISCONTINUOUS RECEPTION 4.2.2

The extended idle-mode discontinuous reception (eDRX) is another mechanism that reduces power consumption by extending the sleeping cycle in idle mode. It allows the device to turn part of its circuitry off during the extended DRX period to save power. During the extended DRX, the device is not listening for paging or downlink control channels, so the network should not try to contact the device.

The main difference with PSM is that this capability is useful for mobile terminating data, with a delayed reach-ability compared to current DRX. To achieve the same degree of mobile terminating services reachability with

PSM, a UE should exit PSM and issue periodic TAU/RAU with the same frequency as the extended idle mode DRX cycle, thus causing additional signalling for the network and power consumption in the UE. The UE can request the use of extended idle-mode DRX cycle (eDRX) during an attach, tracking area updating (TAU) or routing area updating (RAU) procedure by including the eDRX parameters IE. Details are described in 3GPP TS 23.682 - 4.5.13 [26], 3GPP TS 23.060 – 8.1.2a [27] and 3GPP TS 23.401 – 5.3.12 [28].

The network accepts the request to use the eDRX by providing the extended DRX parameters IE when accepting the attach or the tracking/routing area updating procedure. The SGSN/MME may reject or accept the UE request to allow eDRX. When the network accepts the extended idle mode DRX, based on operator policies, the UE may receive different values of the extended idle mode DRX parameters. Then the UE will use the received values for extended idle mode DRX. Otherwise, if the UE did not receive any values, it means that the request to support eDRX was rejected by the network, probably due to the fact that the network is not supporting the capability. In case the request is rejected, the UE should apply its regular discontinuous reception, as defined in 3GPP TS 23.401 - 5.13 [28]. 3GPP specification TS 36.304 [29] allows the following values for the extended idle mode DRX cycles length (TeDRX):

EDRX CYCLE LENGTH (SECONDS)		
LTE/eMTC	NB-IoT	EC-GSM-IoT
~ 5.12	20.48	1.88
~ 10.24	40.96	3.76
20.48	81.92 (~1 min)	7,53
40.96	163.84 (~ 3 min)	12.24
81.92 (~1 min)	327.68 (~ 5 min)	24.48
163.84 (~ 3 min)	655.36 (~ 11 min)	48.96
327.68 (~ 5 min)	1310.72 (~ 22 min)	97.92 (~ 2 min)
655.36 (~ 11 min)	2621.44 (~ 44 min)	195.84 (~ 3 min)
1310.72 (~ 22 min)	5242.88 (~ 87 min)	391.68 (~ 5 min)
2621.44 (~ 44 min)	10485.76 (~ 175 min)	783.36 (~ 13 min)
		1566.72 (~ 26 min)
		3133.44 (~ 52 min)

Table 3: eDRX cycle lengths

It is important to note that the UE can request to enable both PSM and extended idle mode DRX. It is up to the network to decide whether to allow both, or only one, or none of the capabilities. However, the UE can request a different combination at each new attach or TAU/RAU procedure.

RELEASE 13 SYSTEM ENHANCEMENTS FOR CELLULAR IOT APPLICATIONS 4.2.3

In order to optimise the transmission of small amounts of data, 3GPP rel-13 introduces optimised EPS procedures for small data. The following optimisations are described below:

- Control plane CIoT EPS optimisation;
- User plane CIoT EPS optimisation;
- Attachment without PDN
- Support for non-IP data

These optimisations need to be analysed and chosen by service providers together with their mobile operator partner, in order to determine which one is best suited for their application needs and traffic model. The correct choice could lead to reduced signalling, and therefore even more optimised power consumption.

CIoT EPS optimisations are introduced in TS 23.401 [28]. The control plane CIoT EPS optimisation aims to concentrate the data transfer and control plane procedures in the MME. With this optimisation it is possible to transfer data between the UE and the MME using the procedures defined in TS 24.301 [10]. The MME connects the UE (using control plane CIoT optimisations with a PDN connection) either to the PGW (via the SGW) or directly to a new network element called SCEF (service capabilities exposure function - defined in TS 23.682 [26]) that connects to the MME via the T6a interface. The decision whether to use a PDN connection to a PGW or to the SCEF is based on APN subscription data in the HSS.

The user plane CIoT EPS optimisation avoids the need to renegotiate the UE-eNB security association at idle active transition by introducing the concept of suspending and resuming an Radio Resource Control (RRC) connection. Using a Connection Suspend procedure, the S1 is released, but the access stratum context is retained in the eNB. Using a Connection Resume procedure, the UE may attempt to recover the access stratum context that the eNB has stored at suspend time. For all other aspects the network and UE behavior would remain unchanged.

The user plane CIoT EPS optimisation provides the UE with the usual user plane connectivity and is suitable both for applications involving lower data volumes transfer and for applications where the possible range of data volume transmission is unpredictable and can vary quite significantly in frequency and volume. The control plane CIoT EPS optimisation, on the other hand, is more suitable for applications involving lower data volumes transfer as it uses the system control plane resources.

The control plane CIoT EPS optimisation support is mandatory in NB-IoT UEs and networks, while for LTE MTC the optimisation is optionally supported by the network and all LTE MTC UEs, including Cat-M1 UEs.

Another system enhancement introduced in Release13 is the support for attach without PDN connectivity - the ability of a UE to attach to the system without establishing a PDN connection. This allows, for instance, SMS-only type UEs or UEs that establish PDN connections on-demand, thus allowing a reduced number of PDN connections terminations in the network while supporting the ability to send an SMS trigger for mobile terminated services requiring the UE to establish a PDN connection.

Finally, the support of non-IP data delivery has been introduced for NB-IoT and LTE CAT-M1, as specified in 3GPP TS 23.401 [28], TS 23.682 [26] and TS 23.060 [27]. This may be offered via the Gi/SGi interface (at the PGW) or via a new network element that connects to the MME/SGSN via the T6a/T6b interface, called SCEF (service capabilities exposure function) defined in TS 23.682 [26]. This is useful to save data overhead and to enable the 3GPP system to use non-IP protocols suitable for low power and cost devices such as MQTT and AllJoyn. These protocols are useful for data transfer with devices with a small code footprint, which need to save on the energy used to transmit data and may be using connectivity offering only low bit rates.

4.3 LPWA TECHNOLOGY SECURITY CONSIDERATIONS

All 3GPP technologies included in this report share similar network architectures and provide similar transport layer security mechanisms and constraints. Several security mechanisms are available:

- Device/network mutual authentication
- Securing of communication channels
- Ability to support “end-to-end security” at the application level
- Secure provisioning and storage of device identity and credentials.

All three 3GPP LPWA technologies have similar characteristics for the authentication and security aspects. They all support mutual authentication between the device and the network and they require a UICC (note that the UICC can be of different form factors, including embedded UICC and the GSMA Remote SIM Provisioning, as described in [30]). LTE MTC and NB-IoT use the S1 interface; the work item SP-150844 in SA3 [36] provides the support for NB-IoT. All three technologies offer security mechanisms on both transport and application layers, although the use of all available mechanisms may not be necessary. For example, 3GPP security mechanisms can be used by the application layer for application authentication and data confidentiality, but encryption would not be used, if not needed.

LTE MTC (Cat 1, Cat 0 and Cat-M1) and NB-IoT support such mandatory mechanisms as user identity confidentiality, entity authentication, data integrity, and mobile equipment identification, as well as such optional mechanisms as user data and signalling confidentiality, TS 33.401 [12]. The following security mechanisms related to LPWA technologies are also included:

- Security procedures for data sent via the MME (Partial ciphering mechanism for user data confidentiality);
- Security procedures for RRC suspend and resume [12]

Enhanced security for LTE MTC and NB-IoT device triggering procedures are described in 3GPP TS 33.187 [6].

Compared to GSM/EDGE, the security framework for EC-GSM-IoT has been further improved. As a result, with an upgrade of the GSM/EDGE core network, EC-GSM-IoT supports an updated, LTE grade security framework comprising, for example:

- Ciphering (KASUMI and SNOW 3G encryption algorithms),
- Mutual authentication, and
- Integrity protection for user data and control plane supports

For further details see the 3GPP TS 43.020 – Annex H [13].

Generally, the use of 3GPP LPWA technologies will allow MNOs to choose different levels of security depending on the needs of each individual use case, with application requirements dictating the choice.

Cellular-supported LPWA will be subject to the same legal requirements as other cellular communication services. Where applicable, network operators already support legal intercept.

Both the battery consumption due to extra processing power (for example, for integrity protection/cyphering), and the battery consumption driven by security-related traffic (for example, for sending security patches) needs to be considered, as these can add roughly 10% or more of traffic overhead, on top of the daily load.

4.4 STANDARDISATION STATUS

The technologies described above have different levels of maturity in terms of standardisation, as highlighted in the table below.

TECHNOLOGY	STANDARDISATION STATUS FOR RAN FEATURES	STANDARDISATION STATUS FOR CORE FEATURES	CONSIDERATIONS, REFERENCE TO DOCUMENT
Cat-M1	The core part was completed in March 2016 as part of 3GPP Release 13. The performance part is set to be completed in September 2016 and the testing part is set to be completed in December 2016.s	The CORE network from 3GPP Release 12 can also be used. However the futher optimisation of the CORE are available in 3GPP Release 13 and they were completed in June 2016.	
EC-GSM-IoT	The core part was completed in June 2016 as part of 3GPP Release 13. Testing and performance parts are progressing, as part of 3GPP Release 13.	Security enhancement and support for non-IP for EC-GSM-IoT are available in 3GPP Release 13.	3GPP GERAN TR 45.820 [2], section 10. 3GPP TS 43.064 V13.0.0 Overall description of the GPRS radio interface [20].
NB-IoT	Radio interface progress: The core part was completed in June 2016 as part of 3GPP Release 13. The performance part is set to be completed in September 2016 and testing part is set to be completed in December 2016.	The CORE network is available in 3GPP Release 13, concluded in June 2016	

Table 4: Standardisation Status

4.5 SPECTRUM

One major benefit of using licensed spectrum is more efficient traffic management: as the spectrum is not shared with other operators, there is less interference, better reliability and quality of service (QoS). Mobile operators can also use licensed spectrum to offer the service globally and achieve larger scale.

When developing an IoT service, it is important to consider which frequency band best suits the service, since this has a significant impact on the size of the device module. Antenna size is inversely proportional to the used frequency: the higher the frequency is, the smaller the antenna and vice versa. If the frequency decreases, the size of the antenna increases. Use of higher frequency bands will allow smaller modules, which is important for IoT applications where size is an important factor, such as wearables.

Conversely, lower frequencies provide better coverage and are more suitable for extended coverage applications where antenna and module size is not an issue.

The table below provides an overview of the spectrum requirements for all the solutions proposed in this paper.

TECHNOLOGY	SPECTRUM	REQUIRED BANDWIDTH	CONSIDERATIONS
Cat-1, Cat-0 and Cat-M1	Same as legacy LTE Between 450 MHZ and 3.5 GHz	Standalone requires 1.4 MHz bandwidth	Licensed spectrum: already at the disposal of the operators if they support a LTE network. It allows dynamic multiplexing of the resources between LTE MTC and legacy LTE.
EC-GSM-IoT	Same as GSM. 850-900 MHz and 1800-1900 MHz bands	Same as GSM. 850-900 MHz and 1800-1900 MHz bands	Licensed spectrum: already at the disposal of the operators if they support a GSM network. When using 0.6 MHz, packet switched services (GPRS, EGPRS) are supported, since EC-GSM-IoT is intended for M2M/IoT traffic only. When supporting multiplexing with circuit switched voice services, the spectrum requirement is set by the circuit switched operation.
NB-IoT	Can be deployed in 2G/3G/4G spectrum (e.g. 450 MHz to 3.5GHz), Sub-2 GHz bands are preferred for NB-IoT applications requiring good coverage. Bands 1, 2, 3, 5, 8, 12, 13, 17, 18, 19, 20, 26, 28, 66 are prioritized in the Release 13 work item.	180 kHz for in-band and guard-band deployment, 200 kHz for standalone deployment	Licensed spectrum: already at the disposal of the operators if they support a 2G/3G/4G network.

Table 5: Spectrum Consideration

5 DEPLOYMENT CONSIDERATIONS BY TECHNOLOGY

The following section provides some information about the deployment options for each technology introduced in section 4. All these technologies rely on the core features of PSM and eDRX, as indicated in section 4.2 for delivering power-efficient solutions.

5.1 EXTENDED COVERAGE-GSM-IOT (EC-GSM-IOT)

GSM is unique among the global standards for mobile communications, as it is operates in a majority of the world. It continues to play a vital role by supporting extensive coverage, a large number of subscribers, low-cost terminals, globally-available frequency bands and established roaming procedures. EC-GSM-IoT is fully backwards-compatible and can take advantage of the GSM infrastructure and worldwide deployment, while supporting massive M2M traffic. Commercial base station functionality for EC-GSM-IoT is set to become available in the third quarter of 2016.

Today, there are commercial GSM networks using frequency allocations of just 1.8 MHz. GSM networks with full support for legacy services using just 1.2 MHz are already feasible through enhancements in, for example, DL and UL power control functionality. It has even been shown in the 3GPP-approved Work Item on EC-GSM-IoT that a spectrum deployment down to 600 kHz is supported, if the spectrum has been optimised specifically for M2M/IoT communication.

GSM can be deployed on either side of WCDMA (Wideband Code Division Multiple Access) or LTE carriers. This type of deployment is already in place today, and is especially a mature deployment option for WCDMA. Network sharing is another way to support GSM on a small frequency portion per operator. EC-GSM-IoT supports all these configurations. Importantly, EC-GSM-IoT does not require any additional frequency planning since the system is supported on top of existing GSM deployments. The most commonly-used spectrum bands for GSM are in 800-900 MHz and 1800-1900 MHz. Coverage considerations are likely to drive the first EC-GSM-IoT deployments in the lower bands. EC-GSM-IoT can be deployed with minimal impact on neighbouring 2G, 3G and 4G systems in a similar manner to standard GSM deployments.

On the network side, EC-GSM-IoT will not require any new core network nodes as it reuses current GPRS core network functionality. PSM and eDRX are software features for the core network and are the keys to achieving 10 years battery lifetime, as is the case with other 3GPP-based radio access technologies.

5.2 LTE MTC RELEASE 12 AND 13

Cat-1 is part of 3GPP Release 8, which means it could already be available in most LTE deployments. The main deployment scenario for Cat-0 and Cat-M1 (also referred to as LTE-M) is to roll out new software on the existing LTE installed base, reusing existing sites. In today's networks, GSM, WCDMA and LTE co-exist. The introduction of current LTE-MTC features in Release 12 and 13 do not affect the co-existence between these technologies.

Both Cat-M1 and Cat-0 can be multiplexed with LTE MBB traffic. Cat-M1 receives and transmits a signal over a part of the LTE carrier, e.g. 1.4 MHz. But other Cat-M1 devices may use other parts of the LTE carrier, which makes it possible to deliver high capacity and flexibly use the bandwidth for both MTC and mobile broadband.

Cat-M1 may also be used for more frequent and large data transmissions. It can, therefore, benefit from maintaining user plane transmissions and apply RRC resume/suspend for minimising signalling and increasing battery life times. This depends on the operator-specific use cases.

5.3 NB-IOT DEPLOYMENT CHARACTERISTICS

NB-IoT is optimised for IoT communications, according to the performance objectives of 3GPP GERAN study item [2]. It supports three different modes of operations according to the 3GPP RAN work item [33]. The supported operation modes provide for very flexible deployments for NB-IoT:

- Stand-alone operation: utilising any available spectrum, for example, by re-farming spectrum currently being used by GERAN systems, as a replacement of one or more GSM carriers, as well as scattered spectrum for potential IoT deployment.
- Guard band operation: utilising the resource blocks within a LTE carrier's guard-band.
- In-band operation: utilising resource blocks within a normal LTE carrier.

One of the design goals for NB-IoT was to provide a technology with high system capacity, and a low minimum system bandwidth in order to facilitate its rollout. As a result, NB-IoT is designed to be deployed using a bandwidth of just 180 kHz (FDD) for the entire IoT network (potentially with some additional guard bands depending on the nature of other systems occupying the adjacent spectrum).

Further, depending on spectrum and resource availability, multiple NB-IoT carriers can be defined for both DL and UL, facilitating efficient system scalability with an increase in the number of IoT devices. The frequency planning of a single anchor PRB, together with multiple additional (non-anchor) PRBs, is supported to further improve the spectrum efficiency.
For example, one PRB can be dedicated to broadcast transmissions from the network and other PRBs to unicast transmissions.

For the stand-alone operation mode, coexistence between NB-IoT and legacy 2G/3G/4G systems has been studied. For the guard band and in-band operation modes, coexistence between NB-IoT and legacy LTE system has been studied for the uplink, considering the downlink sub-carrier of NB-IoT is orthogonal with LTE PRB and both are transmitting from the same BS. These studies, which have been captured in 3GPP TR 36.802 [25], show that NB-IoT can coexist with legacy 2G/3G/4G in all three operation modes.

In-band and guard-band deployment is likely to be carried on existing LTE-capable radio units, with a power spectral density boosting of 6dB for one NB-IoT carrier, compared to average-power density of all LTE PRBs. With a carefully-selected NB-IoT boosting level (6dB required to meet the link budget) and NB-IoT carrier position, guard-band deployment fulfils existing LTE emission mask, without taking additional spectrum from LTE.

In terms of implementation on the RAN side, existing multi standard radio (MSR) BTS and multi-carrier GSM BTS (MCBTS) - the majority of BTS in operation today - can support NB-IoT by software upgrade.

5.4 CERTIFICATION OF MIOT DEVICES

There are two main certification authorithies that generally certify 3GPP modules and chipsets: the Global Certification Forum [31] and PTCRB [32]. Both these authorities define their terminal certification processes based on the test specification released by 3GPP, while for the interoperability tests they utilise the input from the GSMA Terminal Steering Group's set of guidelines for field and lab tests [34] and [35].

The GCF (Global Certification Forum) is providing device certification for 3GPP GERAN (GSM), UTRAN (UMTS) and E-UTRAN (LTE) families of technologies as well as for 3GPP2 (CDMA2000) technologies. Around 90 manufacturers are part of CGF. In 2015, the GCF certified 540 models (phones, tablets, M2M devices, etc.). Approximately 20% of these certified devices were modules, and 16 manufacturers certified modules during 2015.

The GCF evolves in step with 3GPP and 3GPP2 and relies on the test specifications provided by the standard bodies. As of today, there is no frozen date to get certified products from GCF for LTE MTC Cat M1, EC-GSM-IoT and NB-IoT, because the 3GPP test specifications are expected to be ready later during 2016.

North American MNOs established the PTCRB in 1997 as the wireless device certification forum. The purpose of the PTCRB is to provide the framework within which cellular GERAN (GSM), UTRA (UMTS) and E-UTRA (LTE) mobile devices and modules obtain certification for use on PTCRB operator networks. It had certified more than 10,000 devices by May 2016.

There is no publicly available timeline for LTE Cat M1, EC-GSM-IoT and NB-IoT certification at PTCRB yet, because the related 3GPP test specifications are expected to be ready later during 2016.

5.5 MODULE AND DEVICE CONSIDERATIONS

When deploying IoT services, IoT service providers (customers of MNOs) will need to take into consideration the availability and deployment characteristics of a given LPWA network in their target geographical area. The subscription costs charged by the MNOs for using that network, usually expressed per device and per year, will also be a key consideration for the IoT service provider.

Besides these considerations (features and costs) linked to the network service, service providers need to select the modules and modems that will be used in the end devices. Here too, it is important to consider the supported features and the upfront costs linked to these 33 devices, as well as their potential evolution over time (e.g. through physical replacement, or a software update over the air).

It is also important to take in account whether there is access to mains power or not. In case of a device that is battery charged, the selection of the LPWA technology might be limited by the battery technology. As a result, some of the options described in section 4 might not be applicable due to the incompatibility of the required output power.

COMPLEXITY AND COST 5.51

Mobile IoT technologies have very aggressive targets in terms of device low-complexity and cost efficiency, in order to address and realize the upcoming massive IoT market. These are fully comparable with unlicensed LPWA solutions, while having all the advantages of standards-based technologies.

To meet these targets, drastic measures of complexity reduction were taken for CAT-M1 and NB-IoT. For the EC-GSM-IoT technology, which is an evolution of the rather simple and proven E-GPRS technology that already meets these targets, no further complexity reduction was required. Costs are moreover expected to drop even more over time as market demand and thus production volumes, silicon process technology and the offering by a broad competitive supplier ecosystem all progress.

The final cost of a module/modem will vary depending on its features and options. The good scalability of the technologies will allow a broad variability, with the lower range for basic consumer grade thin modems and the higher range for rugged and enhanced industrial modules that could include application processing, user memory, location features, multiple bands, embedded device management features, additional communication protocols and rich array of interfaces, depending on the requirements of more demanding verticals.

For comparing the module complexity only estimates can be provided because most of the mentioned technologies do not exist in the market today or are just being introduced. Proprietary solutions follow the closed system commercial perspective, while for standardised cellular solutions a very granular market exists of single, modular commercial entities (chipset, module, network equipment, software, etc.). As described in section 5.4, for standardised module, certification by an independent certification body is required which guarantees a certain level of quality but at the same time extends time to market.

Depending on functionality and other aspects, there is a range of different modules possible, all based on the same core technology.

COMMERCIAL AVAILABILITY 5.52

Finally the commercial availability of standard LPWA solutions needs to be considered. The figure below provides a high-level overview of the expected introduction of standardised LPWA technologies to the market.

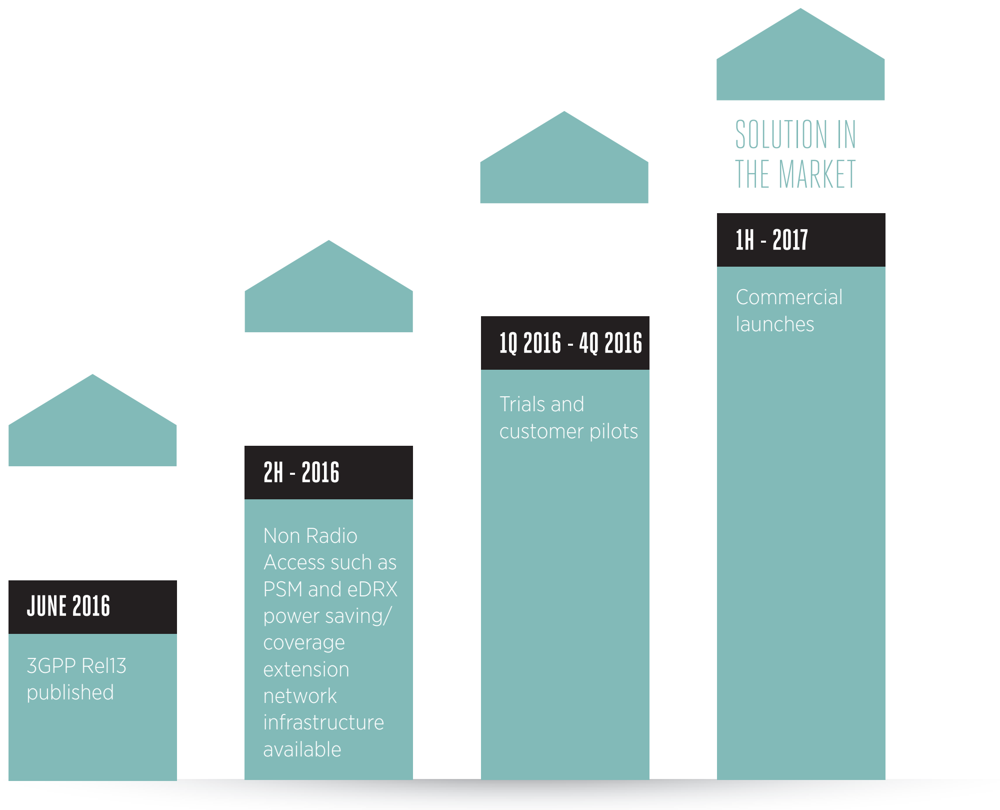


Figure 4: Commercial availability for 3GPP LPWA technologies

SUPPORT OF SEVERAL MOBILE IOT TECHNOLOGIES ON THE SAME UE 5.53

To extend the range of addressable use cases, some IoT devices may need to support more than one of the three licensed LPWA technologies. Support for several radio technologies may also facilitate the deployment of the IoT services over several networks.

Multimode UEs (e.g. supporting 4G, 3G and 2G) are a reality for voice and mobile data services, as this is in the interests of mobile operators and their customers alike: operators are able to capitalise on their strong network assets to provide global IoT coverage, and customers can benefit from easier deployments worldwide.

Of course, supporting several technologies on the same device also brings additional requirements, which are potentially not compatible with the target of developing low cost devices necessary to address some key LPWA use cases.

What will ultimately decide if a particular combination is appropriate will be determined by market factors.

Typical use cases that may require the support of more than one licensed LPWA include:

- Static IoT devices installed in location without prior knowledge of the mobile IoT technology available. E.g. meters / environ ment sensor / connected white goods
- Nomadic / mobile IoT devices able to move in and out of a given mobile IoT coverage area in a domestic market. E.g. wearables / trackers / cars
- Nomadic / mobile IoT devices roaming in countries with a different mobile IoT technology in home and visited networks. E.g. wearables / connected cars / trackers

ROAMING AND FALLBACK 5.54

An IoT service provider that wishes to deploy an IoT service and the associated IoT devices in a particular geographical area and over a given time period will enjoy two of the key benefits of using cellular technologies: roaming and fall back to legacy cellular technologies.

Indeed, the very architecture of mobile technologies worldwide also apply to cellular LPWA, allowing for seamless roaming of devices between different network operators in different countries (or even within the same country – national roaming). This is a key benefit as many IoT service providers are looking to deploy their service across several countries, and this is easily possible, under the same roaming agreements that are already used today between different network operators. This is useful not only for devices actually moving across different countries, but also to easily deploy the same stationary devices across different countries without having to contract connectivity services specific to each target country.

Another key benefit of using mobile LPWA IoT technologies is that modules/modems are likely to offer fallback capabilities to legacy cellular technologies. For example, a service provider may deploy EC-GSM-IoT modules that also support E-GPRS, so that the devices can benefit from the advanced features of EC-GSM-IoT where the network services are already available, and fall back to regular E-GPRS where they are not yet available.

6 BATTERY LIFETIME AND THE RELATIONSHIP TO TRAFFIC MODEL AND COVERAGE SCENARIO

This section provides a high level description of the relationship between a device's lifetime on a single battery charge, its expected traffic load and its coverage scenario.

Batteries have a specific advertised capacity (usually in milliAmp hours and voltage from which total energy stored can be obtained). Battery power consumption occurs both when a device is active (transmitting and receiving) and also when the device is 'asleep'. Separate power consumption models will apply for these two modes.

Simply, while ignoring the effect of battery power leakage over time, the lifetime of a device powered by a specific battery is defined by adding together the products of the power consumed during each mode and the time spent during each mode.

During the active mode, the power consumed by the device will depend on the coverage scenario in which the device is placed. If the device location and network coverage is static, it can be assumed that the power consumption model is also largely static.

More power is consumed by far as a function of time when the device is active, compared to asleep.
For this reason, battery-powered IoT devices tend to be put into sleep mode for as long as possible to conserve limited battery power.

6.1 POWER CONSUMPTION AND TRAFFIC LOAD

If it is assumed that all other things are static, including the device's data throughput, the amount of power consumed by a device will largely depend on the amount of traffic it needs to serve. If a service case requires hourly messages/updates to be sent, then there will be a consequent reduction in battery lifetime compared to a service case that requires a single, similarly-sized message every 24 hours.

Note: If a single 24-hourly message conveys data representing hourly samples, there will be significant power conservation through data overhead reduction, reduction in the radio network access process and other signalling procedures.

6.2 POWER CONSUMPTION AND COVERAGE

For a given, fixed message length, the amount of power consumed by a specific radio device during transmission depends largely on the coverage situation of the device. If the device is in poor coverage, the techniques used to enable connection involve lowering the modulation scheme and repetition of the transmission. The first requires the device to transmit fixed length messages over a longer time and the second requires a larger number of transmissions. Both of these techniques cause the device to consume more power during a single message event, leading to a lower lifetime on a single battery charge, for an equal traffic model.

For a device in a good coverage area, with a flexible modulation scheme capability, a specific message can be transmitted in a much shorter time due to choosing a higher state modulation scheme and also due a greater statistical likelihood of a successful reception of the data, with lower repetitions. In this case, the lifetime of the device on a single battery charge will be extended, compared with similar devices in poorer coverage areas.

7 CONCLUSION

The following conclusions are derived from the GSMA's analysis of the market situation and technical LPWA solutions:

a. The mobile industry has developed three standard LPWA technologies. These have now been standardised by 3GPP in Release 13, and the specifications are availble.
b. Each technology can be selected depending on the regional needs and infrastructure of the mobile operator.
c. These technologies offer solid and well known security mechanisms, since they reuse the existing telco infrastructure.
d. Due to the limitations of LPWA technologies in unlicensed spectrum, such as capacity, scalability, security and regulatory constraints, operators have a clear preference to utilise standardised LPWA technologies operating in licensed spectrum to enable a sustainable long-term global IoT market presence.
e. LPWA technologies in licensed spectrum can be deployed in a simplified and cost effective manner, without sacrificing key customer requirements, such as battery lifetime and security.
f. MNOs can rapidly deploy the three 3GPP-standardised LPWA technologies over their existing 2G and 4G mobile network footprint, paving the way for the worldwide availability of mobile LPWA solutions in the next three years.
g. MNOs can scale their resources quickly to support the expect rapid growth of LPWA devices, through the efficient use of existing spectrum and traffic management.
h. As with any other 3GPP technologies, the LPWA technologies have a well established and large ecosystem that allows to provide scalability and support a potential high demand.

ANNEX A LPWA APPLICATION REQUIREMENTS

A.1 LPWA APPLICATION TRAFFIC MODEL CALCULATION

In order to map a selected set of LPWA applications to the LPWA technologies analysed in this document, the traffic model calculations were performed according to the following parameters set by 3GPP GERAN TR [2]:

- Model 1: 50 bytes 2 hours (1200 bytes)
- Model 2: 200 bytes, 2 hours (4800 bytes)
- Model 3: 50 bytes, 1 day (50 bytes)
- Model 4: 200 bytes, 1 day (200 bytes)

The battery life, coverage, latency and other requirements were then mapped to each technology's performance parameters for the same traffic model.

The traffic assumptions were based on the contributions from the GSMA Low Power Use Case project members, reconciled with the data provided in the ETSI TR 103 055 Annex C [5].

APPLICATIONS	APP FAMILY	NUMBER OF MESSAGES PER DAY	SIZE OF MESSAGE	TOTAL DAILY LOAD (BYTES/DAY)	3GPP TRAFFIC MODEL
Consumer – wearables	Type 1	10 messages/ day	20 bytes	10*200 = 2000 bytes	Model 4
Consumer – VIP / Pet tracking	Type 1	2 every hour (2*24=48)	50 bytes	2*24*50 = 2400 bytes	Model 2
Consumer – smart bicycles	Type 1	8 every hour (8*24=192)	50 bytes	8*24*50 = 9600 bytes	Model 2
Assisted Living / Medical	Type 1	8 messages/day	100 bytes	8*100 = 800 bytes	Model 1
Microgeneration	Type 2	2 messages/day	100 bytes	2*100 = 200 bytes	Model 1
Smoke detector – home/enterprise	Type 2	2 messages/day	20 bytes	2*20 = 40 bytes	Model 3
Agriculture – live-stock tracking	Type 2	100 messages/day	50 bytes	100*50 = 5000 bytes	Model 2
Environmental – near real-time monitoring	Type 2	5 messages/day	50 bytes	5*50 = 250 bytes	Model 4
Industrial – asset tracking	Type 2	100 messages/day	50 bytes	100*50 = 5000 bytes	Model 2
Industrial – tank process/ safety monitoring	Type 2	2 messages/day	100 bytes	2*100 = 200 bytes	Model 4
Water/gas metering	Type 3a	8 messages/day	200 bytes	8*200 = 1600 bytes	Model 1
City – parking	Type 3a	60 messages/day	50 bytes	60*50 = 3000 bytes	Model 2
Building automation – alarms, actuators	Type 3a	5 messages/day	50 bytes	5*50 = 250 bytes	Model 4
Home automation	Type 3a	5 messages/day	50 bytes	5*50 = 250 bytes	Model 4
Industrial – machinery control	Type 3a	100 messages/day	50 bytes	100*50 = 5000 bytes	Model 2

APPLICATIONS	APP FAMILY	NUMBER OF MESSAGES PER DAY	SIZE OF MESSAGE	TOTAL DAILY LOAD (BYTES/DAY)	3GPP TRAFFIC MODEL
Smart grid	Type 3a	10 messages/day	20 bytes	10*20 = 200 bytes	Model 4
Propane tank monitoring	Type 3b	2 messages/day	100 bytes	2*100 = 200 bytes	Model 4
Agri – stationary tracking/monitoring	Type 3b	4 messages/day	100 bytes	4*100 = 400 bytes	Model 4
City - Waste Management	Type 3b	1 message/hour	10 bytes	24* 10 = 240 bytes	Model 4
Environmental monitoring: data collection	Type 3b	1 message/hour	200 bytes	24*20 = 480 bytes	Model 2
City - lighting	Type 4	5 messages/day	100 bytes	5*100 = 500 bytes	Model 4
Consumer – white goods	Type 4	3 messages/day	20 bytes	3*20 = 60 bytes	Model 4
Vending machines – general	Type 4	1 message/day	1 kbytes	1*1000 = 1000 bytes	Model 1
Vending machines – privacy/data verificationl	Type 4	100 messages/day	100 bytes	100*100 = 10000 bytes	Model 2

A.2 LPWA APPLICATION BATTERY AND COVERAGE REQUIREMENTS

APPLICATIONS	APP FAMILY	BATTERY REQUIREMENT	COVERAGE REQUIREMENT	COVERAGE, +DB FROM 144DB REFERENCE
Consumer – wearables	Type 1	1 - 3 years	Outdoor/indoor	+10dB
Consumer – VIP / Pet tracking	Type 1	1 - 4 years	Outdoor/indoor	+10dB
Consumer – smart bicycles	Type 1	2 - 5 years	Outdoor	+0dB
Assisted Living / Medical	Type 1	2 - 5 years	Outdoor/indoor	+10dB
Microgeneration	Type 2	10 years	Outdoor	+0dB
Smoke detector – home/enterprise	Type 2	5 years	Indoor	+10dB
Agriculture – live-stock tracking	Type 2	5 years	Outdoor	+0dB
Environmental – near real-time monitoring	Type 2	5 - 10 years	Outdoor	+0dB
Industrial – asset tracking	Type 2	2 - 10 years	Outdoor/indoor	+10dB
Industrial – tank process/ safety monitoring	Type 2	5 - 10 years	Outdoor	+0dB
Water/gas metering	Type 3a	15 years	Deep indoor	+20dB
City – parking	Type 3a	5 years	Outdoor/indoor	+10dB
Building automation – alarms, actuators	Type 3a	10 years	Indoor	+10dB
Home automation	Type 3a	5 years	Indoor	+10dB

APPLICATIONS	APP FAMILY	BATTERY REQUIREMENT	COVERAGE REQUIREMENT	COVERAGE, +DB FROM 144DB REFERENCE
Industrial – machinery control	Type 3a	10 years	Indoor	+10dB
Smart grid	Type 3a	10 years	Outdoor/ deep indoor	+20dB
Propane tank monitoring	Type 3b	10 years	Outdoor	+0dB
Agriculture – stationary tracking/ monitoring	Type 3b	10 years	Outdoor	+0dB
Waste Management	Type 3b	10 years	Outdoor	+0dB
Environmental monitoring: data collection	Type 3b	10 years	Outdoor	+0dB
City - lighting	Type 4	10-15 years (powered)	Outdoor	+0dB
Consumer – white goods	Type 4	10 years (powered)	Indoor	+10dB
Vending machines – general	Type 4	10 years (powered)	Outdoor/indoor	+10dB
Vending machines - privacy/data verification	Type 4	10 years (powered)	Outdoor/indoor	+10dB

ANNEX B
DOCUMENT MANAGEMENT

B.1 DOCUMENT HISTORY

In order to map a selected set of LPWA applications to the LPWA technologies analysed in this document, the traffic model calculations were performed according to the following parameters set by 3GPP GERAN TR [2]:

VERSION	DATE	BRIEF DESCRIPTION OF CHANGE	APPROVAL AUTHORITY	EDITOR / COMPANY
1.0	1 Sept 2016	New PRD (WG Doc nn/nnn).	WG #nn EMC #nn	Svetlana Grant (GSMA)
1.1		Minor CR nnn (WG Doc nn/nnn).<description of change><reason for change>	WG #nn	
2.0		Major CR nnn (WG Doc nn/nnn).<description of change><reason for change>	eVote EMC #nn	

B.2 OTHER INFORMATION

TYPE	DESCRIPTION
Document Owner	GSMA Mobile IoT Industry Alignment group
Editor / Company	Svetlana Grant (GSMA)

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.

ABBREVIATIONS

TERM	DESCRIPTION
Application Server	3rd Generation Partnership Project
AS	Application Server
BS	Base Station
BTS	Base Transceiver Station
CAT-M1	Category M1
CAT-NB1	Category Narrowband IoT 1
CIoT	Cellular Internet of Things
dB	Decibel
DRX	Discontinuous Reception
DL	Downlink
ETSI	European Telecommunications Standards Institute
EC-GSM-IoT	Extended Coverage GSM for the Internet of Things
EDGE	Enhanced Data Rates for GSM Evolution
eDRX	Extended Discontinuous Reception
eGPRS	Enhanced General Packet Radio Service
eNB	Evolved Node B
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Mobile Telecommunications System Terrestrial Radio Access Network
FDD	Frequency Division Duplexing
GERAN	GSM EDGE Radio Access Network
GHz	Giga Hertz
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GSMA	GSM Association
HARQ	Hybrid Automatic Repeat reQues
HSS	Home Subscriber Server

TERM	DESCRIPTION
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
LPUC	Low Power Use Case
LPWA	Low Power Wide Area
LTE	Long-Term Evolution
LTE eMTC	Long-Term Evolution Enhanced Machine Type Communications
LTE MBB	Long-Term Evolution Mobile Broadband
LTE MTC	Long-Term Evolution Machine Type Communications
M2M	Machine-to-Machine
MHz	Megahertz
MIoT	Mobile Internet of Things
MME	Mobile Management Entity
MNO	Mobile Network Operator
MSR	Multi Standard Radio
MTC	Machine Type Communications
NAT	Network Address Translation
NB	Narrowband
NB-IoT	Narrowband IoT
PA	Power Amplifier
PAPR	Peak to Average Power Ratio
PDN	Packet Data Network
PGW	Packet Gateway
PRB	Physical Resource Block
PSM	Power Save Mode
QoS	Quality of Service
RAN	Radio Access Network
RAU	Routing Area Updating
RF	Radio Frequency
RRC	Radio Resource Control
Rx	Receiver
SCEF	Service Capabilities Exposure Function

TERM	DESCRIPTION
SCS	Service Capability Server
SGW	Signalling Gateway
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module (an application running on a UICC)
SMS	Short Message Service
TAU	Tracking Area Updating
TDD	Time Division Duplexing
TR	Technical Report
TS	Technical Specification
UE	User Equipment (User Device)
UICC	Universal Integrated Circuit Card (sometimes known as the SIM card)
UL	Uplink
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
VPN	Virtual Private Network
WAN	Wide Area Network
WCDMA	Wideband Code Division Multiple Access

REFERENCES

REF	DOC NUMBER	TITLE
[1]	LPUC 3_005	Analysys Mason, Review of LPWA network market size and technology options, Report for GSMA, April 2015
[2]	3GPP TR 45.820	Cellular System Support for Ultra Low Complexity and Low Throughput Internet of Things
[3]	3GPP TR 36.888	Study on provision of low-cost Machine-Type Communications (MTC) User Equipments (Ues) based on LTE
[4]	3GPP TS 45.005	Digital cellular telecommunications system (Phase 2+); Radio transmission and reception
[5]	ETSI TR 103 055	Electromagnetic compatibility and Radio spectrum Matters (ERM); System Reference document (Srdoc): Spectrum Requirements for Short Range Device, Metropolitan Mesh Machine Networks (M3N) and Smart Metering (SM) applications
[6]	3GPP TS 33.187	Security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements
[7]	3GPP TR 33.889	Feasibility Study on Security Aspects of Machine-Type Communications Enhancements to facilitate communications with Packet Data Networks and Applications
[8]	3GPP TR 33.860	Study on EGPRS Access Security Enhancements with relation to cellular IoT
[9]	3GPP TR 33.863	Study on battery efficient security for very low throughput Machine Type Communication Devices
[10]	3GPP TS 24.301	Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3
[11]	3GPP TS 36.101	Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception
[12]	3GPP TS 33.401	3GPP System Architecture Evolution (SAE); Security architecture
[13]	3GPP TS 43.020	Security related network functions
[14]	3GPP TR 37.857	Study on Indoor Positioning Enhancements for UTRA and LTE
[15]	GP-151039	3GPP GERAN Work Item on Extended Coverage GSM (EC-GSM) for support of Cellular Internet of Things
[16]	RP-141660	3GPP Work Item on Further LTE Physical Layer Enhancements for MTC
[17]	RP-141102	3GPP Work Item on Indoor Positioning Enhancements for UTRA and LTE
[18]	RP-150493	3GPP Work Item on RAN enhancements for extended DRX in LTE
[19]	GP-160040	Impact on EC-PDCH in a reduced BCCH spectrum allocation
[20]	3GPP TS 43.064	Overall description of the GPRS radio interface
[21]	3GPP TS 45.010	Radio Subsystem synchronization

REF	DOC NUMBER	TITLE
[22]	3GPP TS 45.008	Radio Subsystem link control
[23]	SP-150462	3GPP Release 13 Work item on EGPRS Access Security Enhancements in relation to Cellular IoT
[24]	3GPP TS 24.008	Mobile radio interface Layer 3 specification; Core network protocols; Stage 3
[25]	3GPP TR 36.802	Evolved Universal Terrestrial Radio Access (E-UTRA); NB-IOT; Technical Report for BS and UE radio transmission and reception
[26]	3GPP TS 23.682	Architecture enhancements to facilitate communications with packet data networks and applications
[27]	3GPP TS 23.060	General Packet Radio Service (GPRS); Service description; Stage 2
[28]	3GPP TS 23.401	General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
[29]	3GPP TS 36.304	Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode
[30]	GSMA SGP.02	Remote Provisioning Architecture for Embedded UICC Technical Specification
[31]	GCF	Global Certification Forum; http://www.globalcertificationforum.org/
[32]	PTCRB	https://www.ptcrb.com/index.cfm
[33]	RP-151621	3GPP Work Item on NB-IoT
[34]	GSMA TS.34	TS.34 IoT Device Connection Efficiency Guidelines v3.0
[35]	GSMA TS.35	TS.35 IoT Device Connection Efficiency Test Book v3.0
[36]	3GPP SP-150844	3GPP Work Item on Architecture enhancements for Cellular Internet of Things