Internet of Things

Mobile IoT: The Ideal Fit for Smart Cities

About the GSMA
The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

For more information, please visit the GSMA corporate website at **www.gsma.com**

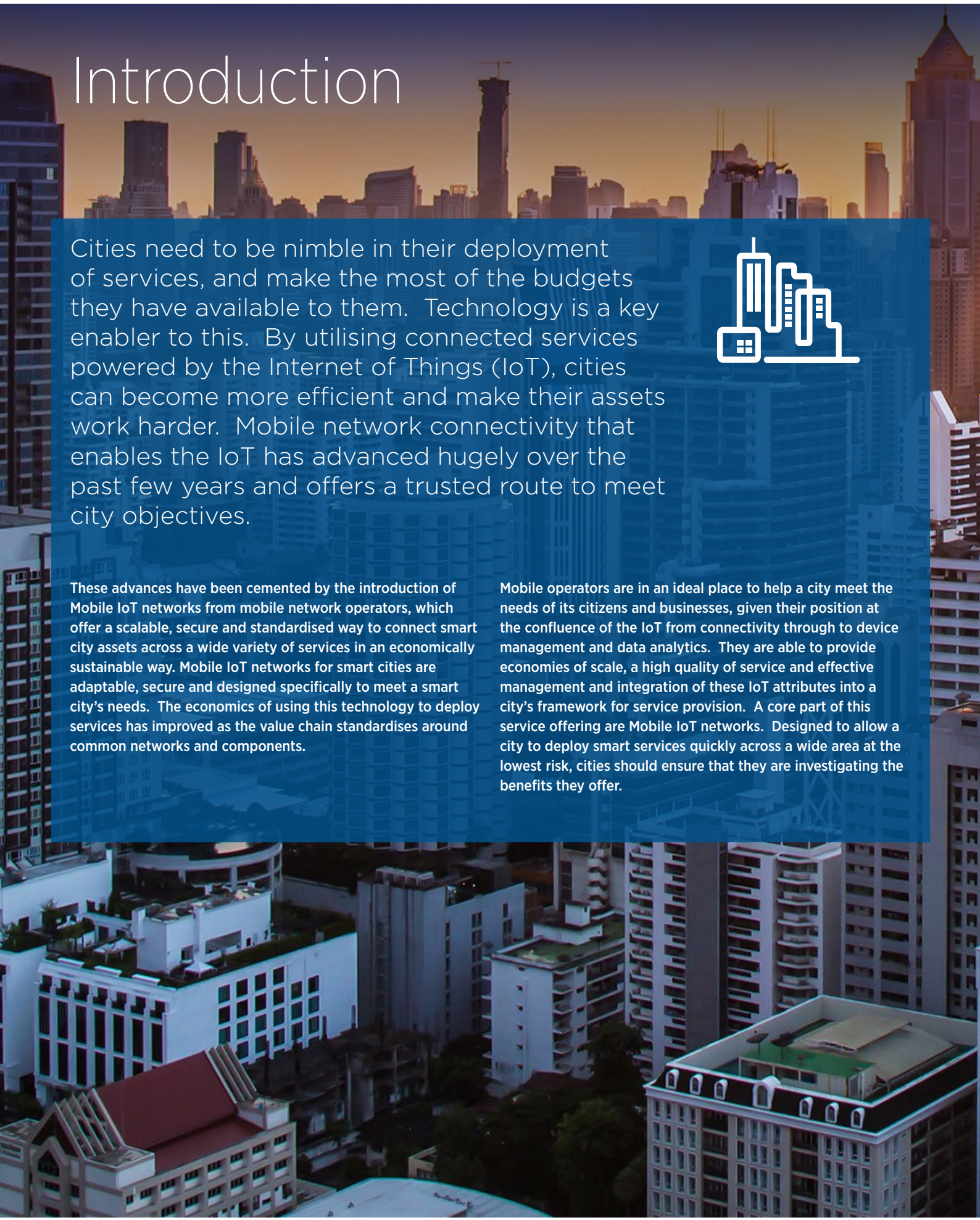
Follow the GSMA on Twitter: **@GSMA**

About GSMA Smart Cities
Cities are getting smarter every day, using information and communications technologies to enrich and enhance city life. The growth of the Internet of Things will have a fundamental impact on the development of smart cities, helping to drive efficiencies and delivering rich new services. However, without effective strategies in place, cities will be unable to capitalise on these benefits. As part of the GSMA Internet of Things programme, the Smart Cities project is working with mobile operators and cities to create real, long-term benefits for businesses and citizens through IoT technologies.

To find out more visit: **www.gsma.com/smartcities**

To contact us email: **smartcities@gsma.com**

Introduction



Cities need to be nimble in their deployment of services, and make the most of the budgets they have available to them. Technology is a key enabler to this. By utilising connected services powered by the Internet of Things (IoT), cities can become more efficient and make their assets work harder. Mobile network connectivity that enables the IoT has advanced hugely over the past few years and offers a trusted route to meet city objectives.

These advances have been cemented by the introduction of Mobile IoT networks from mobile network operators, which offer a scalable, secure and standardised way to connect smart city assets across a wide variety of services in an economically sustainable way. Mobile IoT networks for smart cities are adaptable, secure and designed specifically to meet a smart city's needs. The economics of using this technology to deploy services has improved as the value chain standardises around common networks and components.

Mobile operators are in an ideal place to help a city meet the needs of its citizens and businesses, given their position at the confluence of the IoT from connectivity through to device management and data analytics. They are able to provide economies of scale, a high quality of service and effective management and integration of these IoT attributes into a city's framework for service provision. A core part of this service offering are Mobile IoT networks. Designed to allow a city to deploy smart services quickly across a wide area at the lowest risk, cities should ensure that they are investigating the benefits they offer.

Unique connectivity issues faced by cities

Many cities suffer from issues such as traffic congestion, air pollution, high asset maintenance costs and creating a safe environment in which to live and work. In order to solve these issues, sensors are typically used to monitor the environment, control assets remotely and collect data for the city to analyse and act upon. Once these sensors are in place, intelligent decisions based on the data retrieved can be made, and efficiency savings can be introduced. Traffic can be re-routed away from problematic areas, street lighting can be dimmed when it is not needed and waste can be collected only when bins are full. Services throughout the city can be optimised in ways that have just not been possible in the past.

In order to install and connect these sensor types, a network that meets certain attributes is needed. Cities will find that they have several network options from a large range of different providers.

When making their selection, cities need to consider networks that offer:

SCALE

Across cities, there can be hundreds or thousands of sensors, all measuring and monitoring different assets and attributes. A city needs a single network that can scale to connect these sensors, in regards to both number and geography. Additionally, a network should be able to communicate with these sensors at any time of day, whether on a scheduled basis or ad-hoc as real-time data is needed. A network that requires additional hardware to expand to new areas of the city or a network that can only support slow download of data is not best suited to a city's needs as they require ongoing investment and heavy-touch management to ensure that they are optimised for the city.

LOW COST

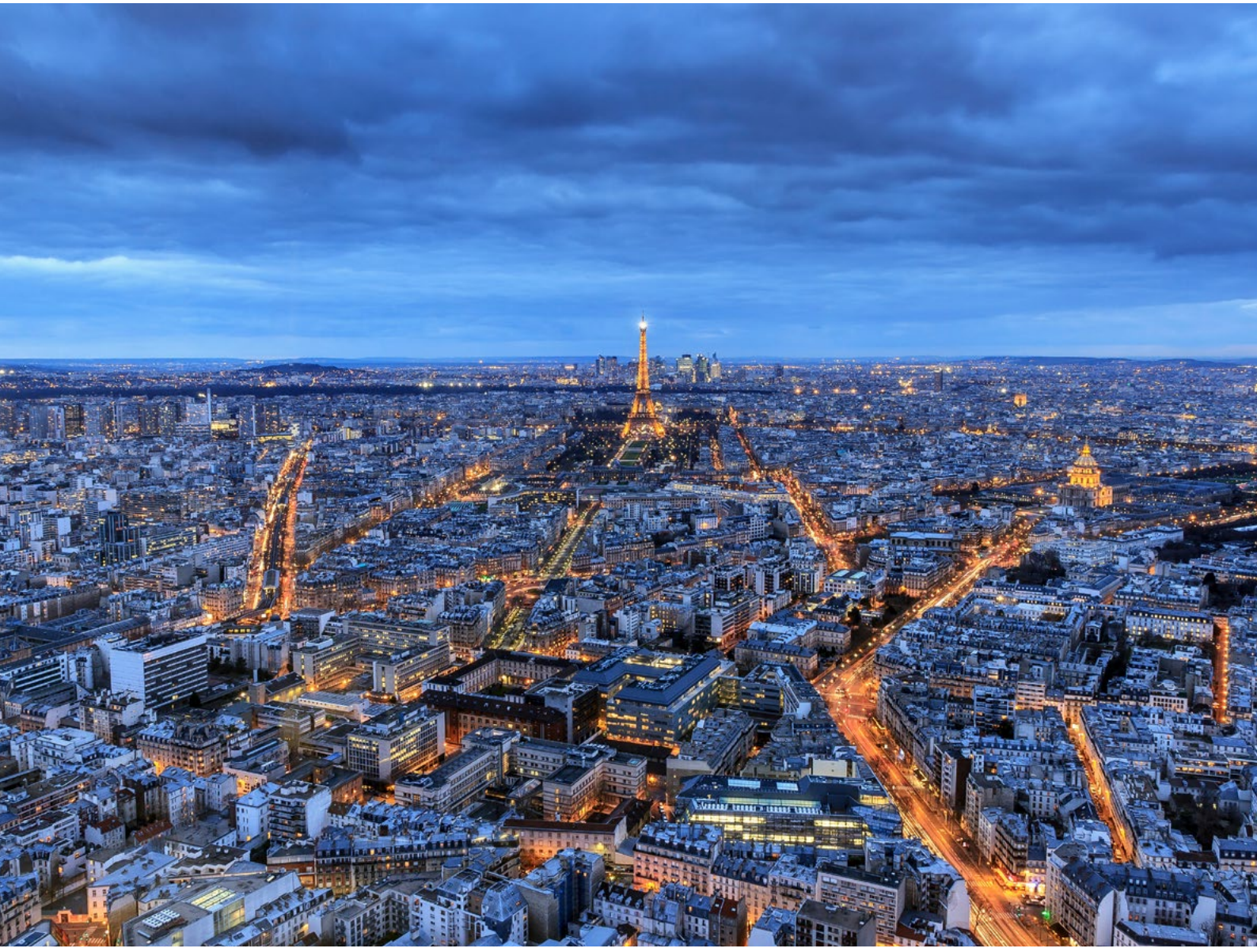
Cities need to avoid the unnecessary costs of building communications networks, and at the same time maximise the savings that communications networks can bring to new smart cities services. This means that more budget is available for services where it counts. The city must weigh up the balance of investing in a new network upfront before deploying services, or using an existing proven network, which will be updated over time as specifications change. Existing networks offer economies of scale for end-devices and modules, as the cost of devices and sensors to connect to the network can be much lower up-front.

QUALITY OF SERVICE

To offer high quality services to its citizens, a city should consider the quality of its communications networks which link and control these services and sensors. A network which is not able to offer adequate bandwidth to meet the city's needs, or one whose provider is unable to offer good local support for it is unlikely to be a good investment, as issues with the network will lead to issues with the cities services, which will impact citizen satisfaction. Networks that operate in licenced spectrum will offer a high quality of service than those that do not, as the risk of interference is lower and bandwidth can be higher.

LONG LIFE SPAN

Once a city has invested in deploying a smart cities service, the city needs to be sure that the ongoing maintenance needs of the equipment and network behind the service are minimal. To minimise the risk of this, the city should look for a service provider who is established and has a good record of accomplishment for deploying and maintaining communications networks. If the city is looking for a service that will be in place for a long period of time, they should ensure that the service provider will be able to support it for its entire lifespan and can operate in-situ for a long time period without having to visit and upgrade the units regularly. Cities should also consider how to maintain sensors and devices that do not have access to mains power. Battery powered devices in particular will need careful consideration regarding network type, to ensure that their lifespan is maximised.



DATA SECURITY

Data security is essential to ensure that a smart cities service is trustworthy and data collected cannot be misappropriated. Smart cities services can collect sensitive data such as licence plates, or the movements of people. Therefore, it is imperative that the city considers the security attributes of any communications networks and devices that they are looking to deploy. A data breach of even anonymised data can lead to a loss of trust in the city and service and ultimately the services failure.

CITIZEN ENGAGEMENT

The way in which the city wants to engage with its citizens is a necessary consideration. If the city wants to have real-time interaction, and provide up to date information on traffic, air quality and other important information, then other factors needs to be considered that ensure the communications network and associated platforms are fit for purpose.

All of these factors needs to be considered by a city looking to deploy smart city services. Additionally, the type of service to be deployed will have a large impact on the network choice available. High bandwidth services such as connected CCTV will have different needs to a connected streetlight. A single network provider that can cover all of these different use cases is very positive partner for the city, and avoids the need of deploying and integrating different technologies to support different services into the future.

Cities need a partner who understand communications networks, devices and data, allowing them to focus on the service, not the technology.

Introducing Mobile IoT

Mobile IoT networks are available exclusively from mobile operators. They are a new technology, sometimes referred to as LPWA (Low Power, Wide Area), which enables cities to build low cost, long life smart city services at a high quality threshold on a communications network specifically designed for the role. In the past, cities may have had to compromise on network coverage, cost or interoperability. Mobile IoT networks remove all of these barriers to adopting smart cities services and allow a city to become smarter, faster.

Mobile IoT networks are based on 4G LTE networks that have already been deployed by mobile operators, so offer exceptional coverage and quality across large urban areas. Because the networks are already deployed, the cost to connect to them is very low – there is no need to procure and manage network hardware beyond the device itself as all the infrastructure is already in place.

Mobile IoT networks are designed purely for IoT connections. They are intended to support high volumes of connections across a city with a high quality of service for a low cost. These networks are also standardised by the relevant industry bodies, and have extensive industry support, which means that the modules needed to connect IoT sensors are widely available from a large number of suppliers, at a competitive price point. As these networks are standardised, it also means that services can be deployed in a simplified manner, platforms and devices can be connected to the networks in a straightforward manner and network operator can be changed at the end of a contract period with minimal disruption.

There are a few Mobile IoT standardised technologies available from mobile operators, but they all have the same essential attributes:

- Very low power consumption
- Optimised for brief messages
- Very low device unit cost
- Operate in licenced spectrum so are reliable and secure
- Good coverage outdoors and indoors
- Easy network installation
- Scalable to support long term growth and investment
- Secure connectivity and support for authentication

There are two different types of Mobile IoT network – NB-IoT and LTE-M. Both of these are standardised, LTE based technologies that offer common attributes, and maintain the same ethos of being designed specifically for IoT connections. Both network technologies are available today.

VERY LOW POWER CONSUMPTION

Many smart city sensors will be located in places without access to a mains power supply. Parking sensors built into the pavement or temperature sensors in open spaces for example. If these sensors can run from battery power, ideally for their whole lifespan, then installation and maintenance costs are kept to a minimum. Even when connected to mains power, the cost of electricity could rise significantly if many thousands of sensors run from the cities power supply. Mobile IoT networks offer optimised power consumption, meaning very low energy demands. Sensors using Mobile IoT networks can potentially offer a battery life of ten years in many scenarios.

OPTIMISED FOR BRIEF MESSAGES

Mobile IoT networks are typically designed to deliver brief, intermittent messages, typically containing a few hundred bytes of data. The networks are optimised to efficiently handle these short messages thereby maximising capacity and minimising power consumption. The networks are flexible enough to meet the demands of different types of sensors, devices and connections. Some sensors may only need to report data, whilst others may need to be controlled remotely or need acknowledgement of message delivery, and so need 2-way communications. These networks can support both, as well as larger downloads such as firmware updates and other periodic data exchanges.

LOW DEVICE UNIT COST

Many cities will want to deploy thousands or even tens of thousands of Mobile IoT connected devices to cover the entire urban area, so the cost of each unit needs to be very low. As Mobile IoT technologies gain economies of scale, the mobile industry is aiming to ensure that most modules will cost just a few dollars, making it viable to deploy connectivity very widely.

OPERATE IN LICENCED SPECTRUM

Mobile IoT networks are deployed by mobile network operators in spectrum licenced for their exclusive use by the country or regions government. This means that interference is eliminated, and bandwidth controlled which removes the risk of congestion, and improves the quality of service available. Smart city services deployed using networks in licensed spectrum are more likely to be able to scale whilst maintaining service quality. Citizens using these services are less likely to be disappointed in the provision of the service, and the city can work with the local mobile network operator to ensure that data transmissions are received in real-time if needed.

EASY NETWORK ACCESS

As Mobile IoT networks are based on existing mobile network technology, and Mobile Operators are able to use their existing network infrastructure to provide service across a city. Mobile IoT networks use existing cell towers, backhaul networks and operations centres, meaning that the infrastructure needed to support Mobile IoT is already in place. This also means that the city does not need to invest in building or maintaining their own IoT communications network – one that is designed for purpose already exists.

GOOD COVERAGE OUTDOORS AND INDOORS

Some smart city services, such as water metering or alarms will require the connected equipment to be located inside a building or underground. Mobile IoT networks are designed to penetrate walls, ceilings and floors, through use of enhanced network coverage techniques. Outdoors, the coverage of Mobile IoT networks will improve on that offered by existing mobile networks for the same reasons.

SCALABLE

Mobile IoT networks are designed to scale. The network will be able to support a cities ambition as it grows and the number of sensors and data it wishes to collect multiplies. As Mobile IoT networks only operate in licensed spectrum, they are not constrained in the growth that they can support, and do not have to compete with other networks operating in the same band.

SECURE CONNECTIVITY AND SUPPORT FOR AUTHENTICATION

Mobile IoT has security designed in by default. Through use of a SIM card, mobile operators can enable cities to control access to the network, and bar specific devices where appropriate. Mobile operators can provide Mobile IoT connectivity with:

- 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 authentication of the device and network.
- Strong (and efficient) cryptography to provide secure communication channels.

Without a secure link, an IoT application will be more vulnerable to attacks and hacking

There are two variations of Mobile IoT:

NB-IoT

NB-IoT offers the essential elements of 4G mobile networks, re-scoped specifically for IoT connections, ensuring that the network is both future-proofed and cost-effective. NB-IoT is optimised for small sized messages that are transmitted over long distances on an infrequent or regularly scheduled basis. The devices are designed to go to sleep for extended periods so that battery power can be maximised over a period of years. As NB-IoT is based on 4G LTE networks, it uses the same infrastructure and pared down designs of the same modules and other equipment needed to connect to the network. Access to the network works the same way as with 4G LTE networks, and so allows for secure, encrypted joining of the network and transmission of data.

LTE-M

LTE-M is another technology designed for IoT, and based on existing 4G networks. It offers a lower cost than 4G itself, as the chipsets are less complex and cheaper to manufacture. It is also optimised for low power consumption and small size message transfer typical of IoT connections. LTE-M allows connections to move between different locations, offers bandwidth for complex interactions and updates, and has some other advanced functionality LTE-M is again an optimised version of 4G LTE and uses the mobile network operators existing 4G network, so all of the infrastructure needed to support IoT deployments across an urban area are already in place.

Why mobile operators are best placed to offer Mobile IoT networks

QUALITY OF SERVICE AT SCALE

Mobile operators already provide secure IoT enabled networks and platforms at scale around the world. They have large customer support functions and deliver a high quality of service to their customers. They are also involved in actively standardising mobile technology so that the whole ecosystem of industry players are able to obtain economies of scale quickly and meet global demands.

IoT EXPERIENCE

Mobile IoT networks will be integrated by mobile operators into their existing IoT management platforms, meaning that existing, proven processes can be followed for device and sensor management. Operators have experience of deploying services for connected cars, smart utilities and smart city services.

This also means that new services and applications can be brought to bear very quickly, as the existing systems are flexible enough to adapt to changing needs.

LICENCED SPECTRUM CONTROL

Finally, Mobile IoT networks are deployed in licenced spectrum, which is exclusively controlled by mobile operators. This means that Quality of Service can remain high, network attributes such as bandwidth and scale can flex as needed by the city, and data security is assured.

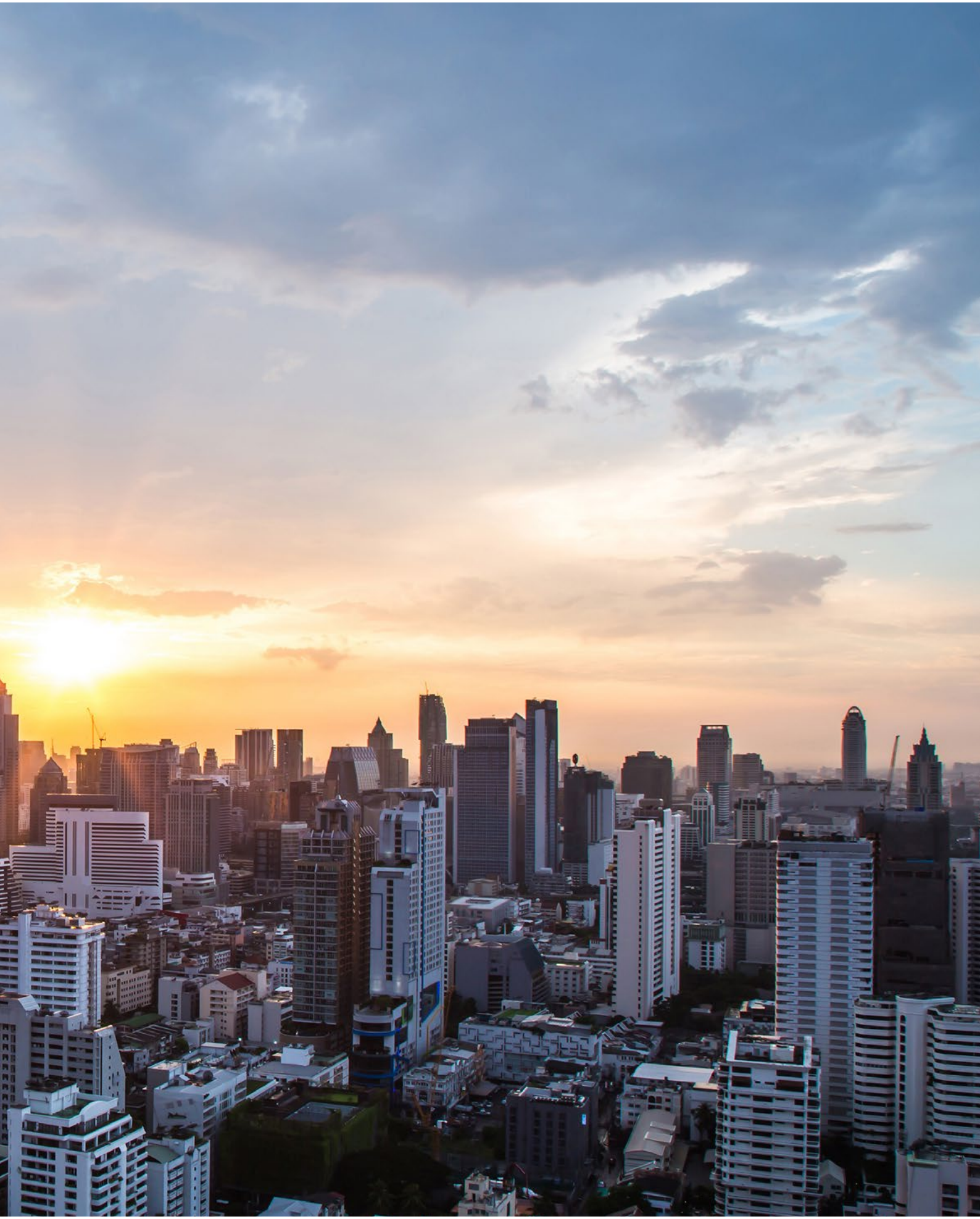
NETWORK MANAGEMENT

Mobile Network Operator platforms provide a single access to all of the mobile operators' networks, including 2G, 3G, 4G, Mobile IoT and others. The city can therefore access a full range of services to meet the specific requirements of their individual city and can pick the appropriate technologies and service providers to meet their needs. Every operator has a control centre where the status of networks is monitored, faults resolved and engineering teams despatched from.

Conclusion

Common across all cities is the hunt for the most cost effective, lowest risk path to becoming a smart city. Mobile IoT networks are a significant new tool to help cities become smart cities in a sustainable manner. By adopting Mobile IoT in their smart cities strategies, cities are able to focus on service provision and other core competencies, rather than the underlying networks or technologies. The standardised, low risk approach that mobile operators take with Mobile IoT allows the citizen to come first in any service design.

Mobile operators offer a trusted, local resource to assist in any deployments that the city wishes to undertake and are able to integrate their Mobile IoT networks with other services to create a low risk, future proofed route to service deployment.



Floor 2, The Walbrook Building
25 Walbrook, London EC4N 8AF UK
Tel: +44 (0)207 356 0600

smartcities@gsma.com
www.gsma.com/smartcities