Security Features of LTE-M and NB-IoT Networks

Mobile IoT Security Report

www.gsma.com/IoTSecurity

LTE-M NB-IoT

Contents

1. Executive Summary

By making it cost-effective to deploy secure low power wide area (LPWA) connectivity, Mobile IoT technologies are driving a major expansion of the Internet of Things around the world. Some 118 Mobile IoT networks using either LTE-M or NB-IoT technologies have been deployed, with more than 100 Mobile IoT modules available from vendors.

This report describes the security features being deployed by mobile operators, highlighting how LTE-M and NB-IoT are 'secure by design', in contrast to alternative technologies reliant on unlicensed spectrum. As Mobile IoT networks use dedicated spectrum bands under the terms of the licences issued by regulators, interference from other radio technologies is kept to a minimum. Moreover, all mobile operators employ Subscriber Identity Modules (SIMs), which contain highly secure integrated circuits, to authenticate the devices accessing their networks and services.

This report explains how mobile operators are supplementing these inherent capabilities with the following four security features, creating significant value for their customers:

SECURE COMMUNICATION CHANNELS:

Mobile operators can ensure that customer/user data is encrypted while travelling across their own infrastructure. In cases when the data is traversing a less secure environment (e.g. the Internet), mobile operators can provide and manage secure connections using virtual private networks (VPNs) and encrypted Internet connections. Operators can also enable individual customers to use dedicated communication channels to ensure that no data traverses a public network, such as the Internet. These methods can be used in conjunction with secure, private, access point names (APNs) dedicated to a specific customer to keep their data communications isolated from other traffic.

MANAGED COMMUNICATIONS:

For IoT applications, devices typically only need to communicate with a specific set of servers. It is, therefore, good security practice to restrict the communication from this device to these specific servers, meaning a compromised device will be unable to communicate with any other destination, thus limiting any potential threat. Such restrictions could be implemented, for example, using a whitelist of IP addresses, IP address ranges or URLs. Moreover, superfluous connectivity capabilities can be disabled in the devices' HLR/HSS (home location register/home subscriber server), thereby ensuring they can't be misused. For example, if the devices in question only use SMS and voice, the data connectivity should be disabled.

DATA OVER NAS (DoNAS):

Data over NAS (DoNAS) allows the network to transport user data within signalling messages. This feature transports data via the MME (mobility management entity) by encapsulating them in NAS (non-access stratum) signalling. DoNAS can be used to transport both IP and non-IP traffic. The customer/user data is encrypted and integrity protected using the same mechanism reserved for network signalling, thus ensuring similar levels of protection. This feature works well for short data transactions, for example with UDP (user datagram protocol) traffic, where a few packets are sent per connection.

NON-IP DATA DELIVERY (NIDD):

NIDD is used in conjunction with DoNAS to allow a device to send data to the network without an IP stack, without an IP address, and without an IP header or transport header. NIDD can transport data using a Point-to-Point (PtP) Serving Gateway interface (SGi) tunnel to the application server or by using the service capability exposure function (SCEF). The SCEF provides a means to securely expose service and network capabilities through network application programming interfaces (APIs).

2. Introduction

Delivering low power wide area (LPWA) connectivity using licensed spectrum, Mobile IoT technologies are driving a major expansion of the Internet of Things (IoT) around the world. These versatile technologies are designed to connect everything from sensors monitoring the environment and smart meters to asset trackers and digital locks. Standardised by 3GPP, the two main Mobile IoT technologies – LTE-M and NB-IoT – are supported by large numbers of mobile operators and equipment suppliers, enabling the ecosystem to benefit from economies of scale and low production and deployment costs. As of August 2019, 118 Mobile IoT networks had been deployed around the world, while more than 100 Mobile IoT modules supporting LTE-M, NB-IoT or both technologies are available from vendors.

Unlike some forms of connectivity, Mobile IoT networks are carefully managed and secured by mobile operators. As such, the growing usage of NB-IoT and LTE-M will help to counter security threats to the IoT, such as the hijacking of devices by botnets and the hacking of sensitive data belonging to individuals or organisations. By supporting an array of security features and safeguards, Mobile IoT networks are set to play a pivotal role in building trust in the Internet of Things, while giving enterprises the confidence they need to bring mission-critical assets online, so they can be remotely monitored and controlled.

Building on the rollout and usage of LTE-M and NB-IoT connectivity, this report considers the security capabilities of Mobile IoT networks. It describes the security features being deployed by mobile operators, highlighting how the 'secure by design' characteristics of these technologies differentiates them from alternative technologies reliant on unlicensed spectrum.

To help explain the key security features of Mobile IoT networks and how they can be employed in practice, the report includes commentary from leading mobile operators Deutsche Telekom and Vodafone that have implemented these features. The GSMA interviewed these operators to gauge the commercial availability of these features, how effective they are in enhancing security and how IoT service providers can benefit from using them.

To be distributed worldwide by the GSMA, this report will raise awareness of the security capabilities of Mobile IoT technologies among mobile operators, their partners and the broader IoT ecosystem. By highlighting the value of various security features, it aims to encourage their use by both mobile operators and service providers, helping to safeguard the integrity of the IoT.

3. Mobile IoT Security Features

3.1 USE OF LICENSED SPECTRUM, SIMS AND SECURITY STANDARDS

Mobile operators' networks use dedicated spectrum bands under the terms of the licences issued by their national regulators. The use of licensed spectrum ensures interference from other radio technologies is kept to a minimum, as any unauthorised use of this spectrum will be subject to prosecution. Moreover, the use of licensed spectrum and dedicated radio bands helps ensure the mobile operator can carefully plan its network coverage and capacity maximising network availability for their customers.

All mobile operators employ SIMs, which contain highly secure integrated circuits, to authenticate the devices accessing their networks and services. SIMs can also support additional security capabilities that can be leveraged by IoT services. For example, a SIM can provide a secure 'root of trust' to provision and store digital certificates and other kinds of security credentials, such as passwords. A mobile operator can use its existing provisioning infrastructure as a secure channel through which to cost-effectively install, validate and update the security credentials safely housed in a SIM. For more information, please see the GSMA Case Study: Leveraging the SIM to Secure IoT Services.

The 750 mobile operator members of the GSMA provide connectivity using standardised network technologies, such as GSM, UMTS and LTE, as specified by standards body 3GPP. As well as assuring interoperability between mobile operators, the use of standardised technology enables a mobile operator to benefit from the scrutiny the technology is subjected to by standards bodies and their members during its development. Furthermore, this process draws on the security lessons from previous generation networks to help shape and enhance security features and functions so that improvements are built-in to the standards. The end result is a network that is typically far more secure than a network based on proprietary technologies developed by a single company and using unlicensed spectrum.

3.2 SECURE COMMUNICATION CHANNELS

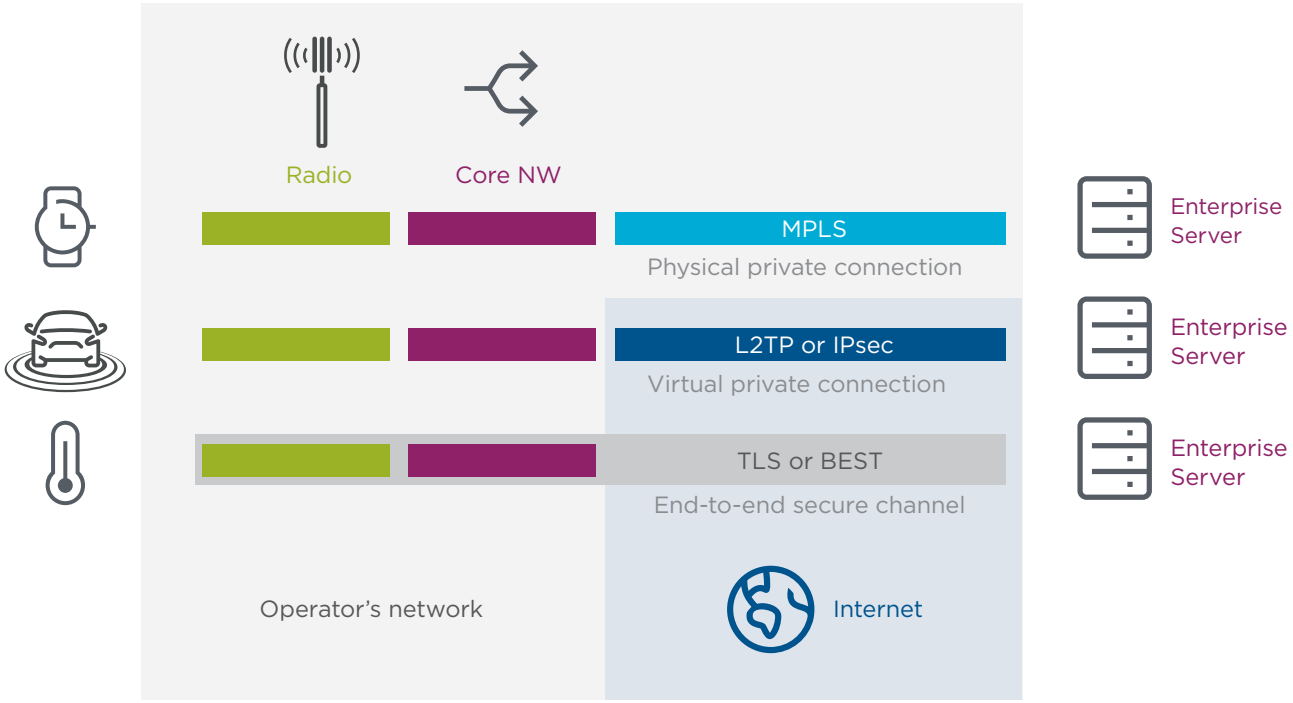
Mobile operators can ensure that the customer/user data that transits their public network infrastructure is encrypted between the point that the data enters its network infrastructure to the point that it leaves the network. This encrypted communication channel is designed to ensure that the data being sent over the channel is not processed, used or transmitted without the knowledge and consent of the data subject.

There are cases when the customer/user data may need to traverse a less secure environment, such as the Internet, between the mobile operator's public network infrastructure and the customer's enterprise network. In these cases, operators can provide and manage secure connections to enterprise networks using virtual private networks (VPNs) and encrypted Internet connections. As shown in the diagram below, this could be done in several ways:

1. By using a tunnelling protocol such as Layer two Tunnelling Protocol (L2TP), or using a secure protocol such as Internet Protocol security (IPsec) that creates a VPN;

2. By providing customers with end-to-end security between the user equipment and the application server using, for example, Datagram Transport Layer Security (DTLS) or Battery Efficient Secure Transport for very low throughput devices (BEST) protocols.

Mobile operators can also provide private networks in which the customer uses a dedicated communication channel to ensure that none of their data traverses a public network, such as the Internet. The operator can do this by using a physical private connection, such as dedicated MPLS (multiprotocol label switching) links, between the mobile operator's public infrastructure egress point and the enterprise network (see diagram).



These methods can be used in conjunction with secure private access point names (APNs) dedicated for a specific customer's use to ensure isolation of the customer's data communications. For example, the combination of customer-specific private APNs and an IPSec-based VPN produces an additional layer of security: the secure APN segregates the customer's traffic, which is also encrypted over the Internet.

Secure Communication Channels: the Mobile Operator Perspective

For Vodafone, security is an integral part of its connectivity proposition and is designed into any IoT solution from the beginning. To that end, it offers all of its IoT customers the opportunity to use secure communications channels, providing a menu of options. "We aim to give the customer the optimal solution for their requirements that maximises their security controls," says Tim Snape, Head of IoT Security at Vodafone Group Enterprise & Technology. "So maybe they want to use IPsec with failover or without failover – it's the customer's decision. We have a collection of building blocks they can choose from." If necessary, Vodafone can offer a private APN that makes use of its own backhaul network, keeping the customer's traffic away from the public Internet.

For customers employing Vodafone's Mobile IoT connectivity, private APNs are the default option. "With low power wide area networks, a lot of the power saving features, such as high latency communications and eDRX (extended discontinuous reception), only really come into their own with private APNs," explains Tim Snape. "You actually need that much safer environment of a private APN. Private APNs provide better usability and security." For Vodafone, the end-goal is to provide customers with the optimum combination of simplicity, speed and trust. "It's in everybody's blood at Vodafone that trust is a really, really important thing," notes Tim Snape. "It is part of Vodafone's DNA."

3.3 MANAGED COMMUNICATIONS

For most IoT solutions, the connected devices only need to communicate with a specific set of servers. For example, in a logistics tracking application, a device reports its location information to a location-tracking server. From time to time, the device may also need an application software update from a different server. As these are the only two servers that the device needs to communicate with, it is good security practice to restrict the communication from this device to only these two servers. In the event that it is compromised, the device will be unable to communicate with any other destination, thus limiting any potential threat. This makes the device's communication capability less attractive to bad actors looking to hijack the connectivity. This feature can be implemented, for example, using a whitelist of IP addresses, IP address ranges or URLs.

In a similar vein, there are IoT applications that don't need to use all the connectivity capabilities of cellular devices. For example, there are applications that rely only on SMS, or data connectivity, or voice. For these application types, the superfluous connectivity capabilities can be disabled in the devices' HLR/HSS (home location register/home subscriber server) subscription, thereby ensuring they can't be misused. For example, if the devices in question only use SMS and voice, the data connectivity should be disabled.

Managed Communications: the Mobile Operator Perspective

Vodafone, for example, enables its IoT customers to restrict their connected devices to accessing specific servers and specific services. This approach can dramatically lower the risk that an IoT device could be compromised. "It is very effective because all customer traffic is totally logically separated from other traffic," explains Martin Bell, IoT Technologist at Vodafone Global Enterprise. "We never have any chance of one customer seeing another customer's traffic. It's like a private network – it is completely isolated, at almost no cost to the customer. It's a really simple control and it is very effective."

Vodafone also enables customers to use traffic management tools to set thresholds that will trigger alerts. By setting its own business rules, the customer can help Vodafone distinguish expected traffic patterns from suspicious traffic patterns. "They understand what is abnormal behaviour much better than we do," says Martin Bell. "So we might see a customer generating an awful lot of traffic to a small set of devices, which could suggest they have been compromised and being used in a DDOS attack, whereas in actual fact, they are doing firmware updates as part of a scheduled campaign. But if a device is talking too much, then it probably shouldn't be on a low power network." If a device gets stolen and repurposed for free Internet access, Vodafone says customers can quickly spot it and disable it.

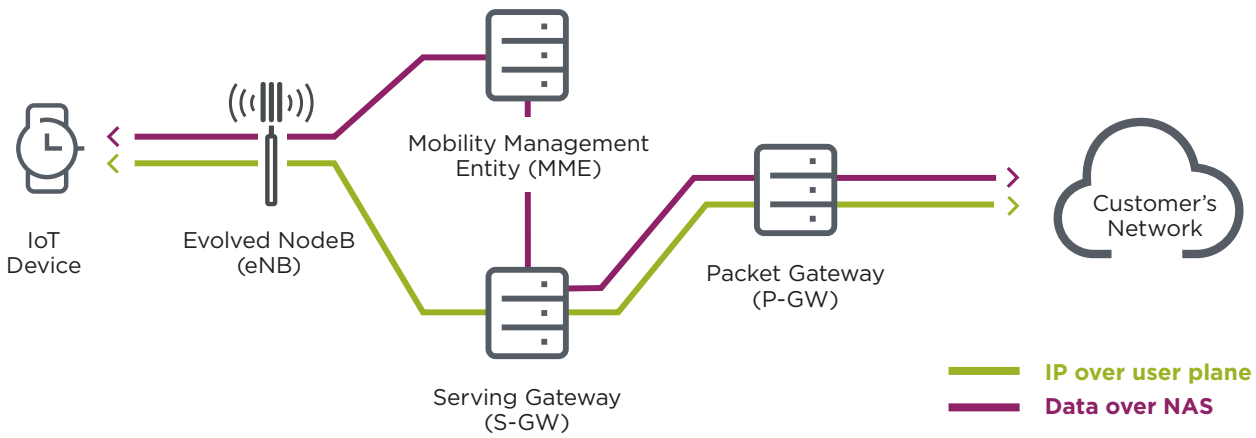
But Vodafone only gives customers so much flexibility, generally forbidding any requests that could leave an IoT solution dangerously exposed. “Sometimes we lose business because of it,” notes Tim Snape, Head of IoT Security at Vodafone Group Enterprise & Technology. “If a customer wants something that, in our view, presents a major security risk, such as direct peer-to-peer connectivity between devices, we will generally not allow that because one device can be used to attack another device. What we can do instead is to provide the same capability, but using the core network to secure the traffic.”

3.4 DATA OVER NAS (DoNAS)

Information has traditionally been transported over a network via a “IP over User Plane’ mechanism. Although User Plane IP data transport works well when a large volume of data needs to be transmitted, it can be inefficient when transporting the small amounts of data required for Mobile IoT solutions.

Data over NAS (DoNAS) is a control plane cellular IoT optimisation that allows the network to transport user data within signalling messages. This feature transports user data or SMS messages via the MME (mobility management entity) by encapsulating them in NAS (non-access stratum) signalling. DoNAS can be used to transport both IP and non-IP traffic. One key security benefit of this feature is that the customer/user data is encrypted and its integrity protected using the same mechanism reserved for network signalling, thus ensuring similar levels of protection.

The diagram below shows the data path for DoNAS and contrasts it with the traditional data path for IP over user plane.



As well as strengthening security, DoNAS offers other benefits. Employing the control plane to transmit user data significantly reduces the signalling overhead needed to allow a sleeping device to transition from idle mode to connected mode and send the data. That improves the network efficiency. The device battery life is also improved because the amount of signalling required and the "air time" is reduced. This feature works well for short data transactions, for example with UDP (user datagram protocol) traffic, where only a few packets are sent per connection.

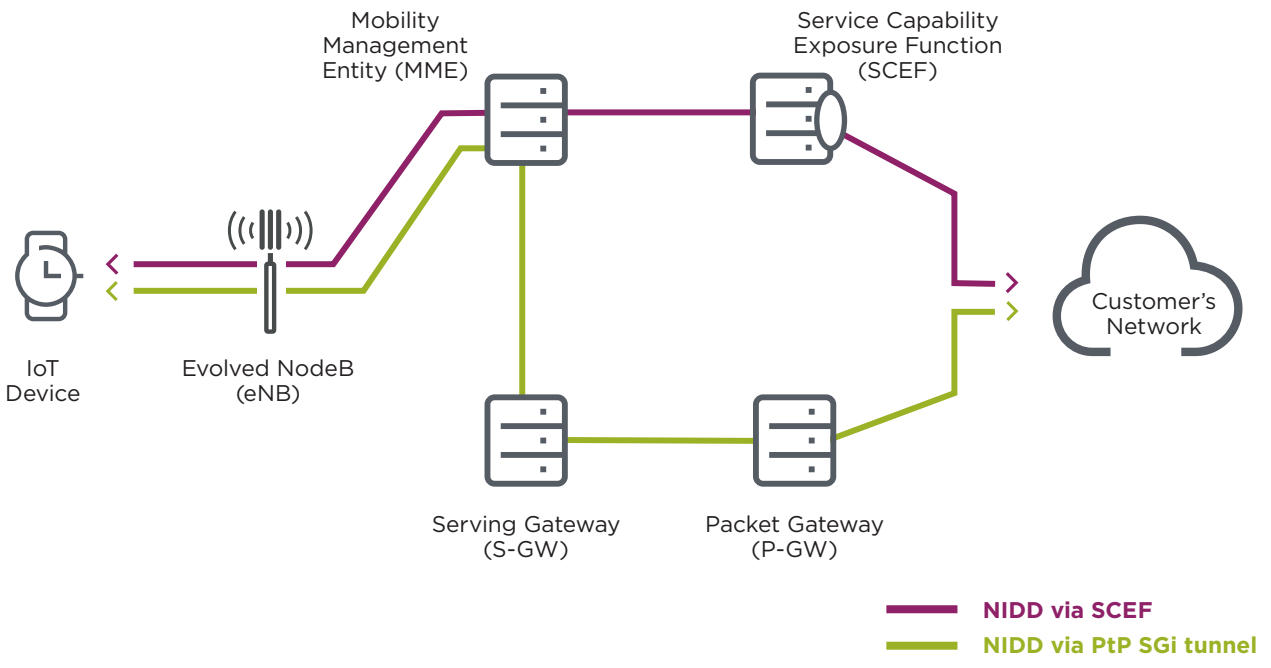
DoNAS: the Mobile Operator Perspective

Deutsche Telekom, for example, provides its NB-IoT customers with DoNAS as a default feature of the connectivity. "As there is no explicit user data channel with DoNAS, the user data is protected using the same mechanism reserved for the control plane data" notes Mona Parsa, Product Manager for New Access Technologies at Deutsche Telekom. "We are providing integrity protection by default, whereas with alternative technologies, it needs to be done in the application layer."

Deutsche Telekom emphasises the security features of NB-IoT in its marketing materials, seminars and customer workshops. "Being based on LTE technology standardised by 3GPP, NB-IoT leverages the same security features as LTE," explains Mona Parsa. "Data transmitted over the air interface is encrypted using standard LTE encryption and we use IPSec tunnelling between our core network and customer's network, making the device inaccessible from the Internet. Towards our customers we emphasise the security features which are a clear differentiator between our services and those operating in unlicensed spectrum i.e. NB-IoT uses longer encryption keys (128-256 bits) and a secure key management and storage which increases the security level."

3.5 NON-IP DATA DELIVERY (NIDD)

A number of IoT applications send such small amounts of data, e.g. temperature readings, that sending this data as an IP packet results in an inefficient data-to-overhead ratio due to the large size of the IP headers. For this reason, the feature known as Non-IP Data Delivery (NIDD) was introduced, allowing the network to transport non-IP data.



NIDD is used in conjunction with DoNAS to allow a device to send data to the network without an IP stack, without an IP address, and without an IP header or transport header.

NIDD can be supported by the network in two different ways:

1. Transport data using a point-to-point (PtP) SG interface tunnel to the application server. This means that the device can only communicate with the pre-defined application server, making the communications link more secure by restricting the destination, as discussed in the Managed Connectivity section.

2. Transport data using the service capability exposure function (SCEF). The SCEF provides a means to securely expose service and network capabilities through network application programming interfaces (APIs). In this way, access to the IoT devices are restricted to application servers that have been authenticated and authorised to access the IoT devices.

The device subscription must be provisioned with the appropriate SGi or SCEF option in the HSS, and the Non-IP transport is requested by the user equipment via a PDN (packet data network) connectivity request (as part of an attach request or separately), by selecting "PDN-type = Non-IP".

NIDD: the Mobile Operator Perspective

Deutsche Telekom's NB-IoT network supports NIDD, enabling customers to exercise tight control over the volume of communications with their IoT devices, explains Saher Salem, Senior Product Manager for NB-IoT at Deutsche Telekom. "We use NIDD for customers who want to shrink down the data transmitted over the air, it removes the IP addresses and protocol between the device and IoT core, which shrinks the header, lowers the payload and reduces the traffic and energy consumption". Saher Salem further explains, "In this way the amount of attack scenarios is further reduced because there is no IP and TCP/UDP layer".

Larger enterprises are showing interest in NIDD because of the significant benefits in lower power consumption and payload transmission. Application servers can still communicate with IP protocols, whilst on the air interface less data is transferred."

4. Conclusions

Beyond the inherent security built into mobile networks using the 3GPP standards, mobile operators are providing Mobile IoT customers with an array of additional security features. As a result, Mobile IoT networks can provide both consumers and companies with connectivity that is far better protected than networks that make use of unlicensed spectrum.

As regulated entities with spectrum licensees, mobile operators also have to comply with a range of requirements established by the regulatory authorities in the markets in which they operate. In most countries, mobile operators now have long track records of keeping their networks secure, building trust among regulators, governments and policymakers. "You have got the national regulatory oversight," notes Tim Snape, Head of IoT Security at Vodafone Group Enterprise & Technology. "You've got regulatory authority oversight in terms of the behaviour of operators in each and every country. That gives them reassurance, as compared with connectivity providers using unlicensed spectrum, which have almost zero oversight and with which local regulatory authorities have almost zero control."

Of course, it is almost impossible to eliminate every risk. The distributed nature of the Internet of Things means many connected devices, such as environmental monitors or smart lighting, will be vulnerable to vandalism or theft. But mobile operators are taking measures to ensure that Mobile IoT devices are very difficult to repurpose or tamper with. "We have hard-to-spot SIMs that are difficult to remove from the board," explains Tim Snape. "We also have tamper-resistant SIMs and SIM locking. If you take one SIM out of device and put it in another, the hardware can't be hijacked. The SIM is actually inside the NB-IoT device, so if it gets stolen, it is quite hard to do anything with it."

For more information please visit:
www.gsma.com/IoT

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601