LPWA Technology Security Comparison

A White Paper from

Franklin Heath Ltd

Executive Summary

In this report we compare and contrast the security features of five of the latest Low-Power Wide Area (LPWA) network technologies: LTE-M, NB-IoT, EC-GSM-IoT, LoRaWAN and Sigfox. The security features of each technology are laid out in a comparison table, in which some non-security features are also listed, to illustrate that security may not be the deciding factor when choosing a LPWA technology.

We describe the different contributions that each feature makes to the overall security of a system and illustrate how the security features may or may not be relevant to your selection of a LPWA technology, depending on the intended use case.

We consider whether the security features of each technology are appropriate for a set of use cases representing typical deployments for each technology. Based on an evaluation of the appropriate features, we estimate the effectiveness of the security of each of the five technologies for each of the five use cases.

The conclusions table shows that, although not all technologies have adequate or good security for all use cases, all technologies have adequate security for some use cases, and therefore all may, in particular circumstances, be a sensible choice. This emphasises the value of taking a risk-based approach to evaluating the security needs of a specific application. We note that, if the security provided by the network is not adequate for a particular use case, it may be possible to compensate for this by adding secure hardware and/or implementing higher-level security protocols in software, potentially incurring additional cost as a consequence. Finally we note that there are several optional features of LPWA networks which network operators may or may not choose to enable; it is therefore essential to understand which security options are enabled by particular network operators before committing to a choice based on your security needs.

Contents

Introduction

Although the focus of this report is on security, it should be acknowledged that, in the majority of cases, security will not be the principal criterion on which a LPWA technology is selected; there are other differentiators which are likely to have a big influence, such as: cost, availability in target locations, signal strength, ease of implementation, associated managed services and so on. We also acknowledge that different use cases will have different security needs, and more security features are not necessarily "better"; unneeded security features will, in most cases, have some associated cost, whether in bill-of-materials, power or bandwidth consumption, or just additional complexity increasing the potential attack surface.

At an extreme, we can imagine use cases where there is no perceived need for security:

- Transmitting freely available data, with no privacy implications
- which is not relied on for critical operations
- where there is no incentive or opportunity for an attacker to tamper with it

With typically very limited power and data rates, there may be less incentive to attack devices on LPWA networks for Denial-of-Service (DoS) botnet purposes, and the more prevalent threats may be due to data being processed by the devices, although there is still a threat of DoS attacks directed at the devices and the network. Devices using non-IP networks may also be difficult for attackers to reach from the Internet. Very simple sensors processing public domain data could, therefore, have minimal security needs.

However, in most use cases there will be security needs, driven by concerns of privacy (where sensor data can be correlated with the actions of identifiable individuals) and safety (where devices have actuators affecting the physical world) as well as commercial interests. We should also note that it is in the nature of ICT systems to experience "feature creep", and what starts as a use case with minimal security needs may come to be relied upon for other, more critical purposes over time.

Specific deployments of systems using LPWA technologies should, as for any ICT system, have their security needs assessed using a risk-based approach. There are various suitable methodologies, such as are referred to in the GSMA IoT Security Guidelines, or the IoT Alliance Australia Security Guidelines; one essential step to emphasise here is that the threats to the system must be considered from a high-level, organisational perspective before drilling down to technical risks. A technical risk could be

irrelevant if there is no threat (i.e. a motivated attacker) to exploit it, conversely a high-level threat might be missed from a technical view lacking an understanding of the organisational and commercial context of the system's deployment. For the purposes of this report, we will consider some representative use cases and make assumptions about the high-level context of the deployment, but this is no substitute for a specific assessment of the threats and risks to each real-world system before it is deployed.

Technologies under Consideration

The defining characteristic of a LPWA network is that it supports devices that are low power, in terms of both processing power and transmission power; frequently there is a target of a battery life of 10 years or more. This is typically coupled with an objective of low cost, particularly in respect of the wireless module in the end devices. There is also a third common objective which is to provide coverage in hard-to-reach areas (distant from base stations, inside buildings, or below ground level).

There are five LPWA technologies considered in this report; three which are standardised by 3GPP and operate in licensed radio spectrum: LTE-M, NB-IoT and EC-GSM-IoT, and two which operate in unlicensed radio spectrum: LoRaWAN and Sigfox.

In most jurisdictions, use of unlicensed spectrum is regulated such that devices must meet requirements on maximum transmission power and duty cycle to minimise undue interference with other users; this may result in region-specific limitations on the data throughput and range of LPWA technologies using particular frequency bands. There is also a risk of degradation of service as the bands are shared with many other types of radio devices, the numbers of which may grow significantly.

LTE-M

LTE ("Long Term Evolution") is a 4G (fourth generation) cellular mobile technology standardised by 3GPP. The LTE standards accommodate multiple categories of device (UE, "User Equipment") with varying uplink and downlink capabilities. In 3GPP Release 13, LTE UE category M1 is defined to suit devices with simpler, cheaper wireless modules and very long battery life; use of LTE with this UE category is referred to as LTE-M for short. LTE-M also offers enhanced coverage compared to machine-to-machine UE categories in 3GPP Release 12.

NB-IoT

3GPP Release 13 also defines a further enhancement, described by UE category NB1 (NB for "Narrow Band", simply put giving a lower data rate but greater penetration). Similarly to LTE-M, the characteristics are optimised for cheaper wireless modules and very long battery life. The term NB-IoT encompasses the use of this technology within the LTE bands and also includes use of the same protocols in other, licenced radio spectrum outside the normal LTE bands.

EC-GSM-IoT

EC-GSM-IoT is an evolution of the GSM 2G GPRS and 2.5G EDGE packet-switched data services, allowing for lower power devices and greater coverage using existing GSM network infrastructure and modem technology. EC-GSM-IoT, also specified in 3GPP Release 13, adopts enhanced security features from 3G UMTS including mutual authentication between the device and the network.

LoRaWAN

LoRaWAN is a public specification for LPWA technology developed by members of the non-profit LoRa Alliance. With a low-cost base station available, it is being used for self-managed private network installations as well as by providers of public networks. "LoRa" alone describes the underlying, proprietary, physical radio layer which can also be used for peer-to-peer communications, whereas "LoRaWAN" describes the link layer protocol.

Sigfox

Sigfox is a licensable LPWA technology developed by the French-based company of the same name. A particular characteristic of Sigfox is its use of "Ultra Narrow Band" radio transmission, which is claimed to enable good coverage with a very low transmission power, but it is limited to a very low data rate compared to some of the other LPWA technologies covered here and has very limited downlink capability. Wireless modules are very low cost (and royalty free); network providers pay license fees to Sigfox, and Sigfox also run their own commercial networks in some territories.

Feature Descriptions

Table 1 - Feature Comparison

	LTE-M	NB-IoT	EC-GSM-IoT	LoRaWAN	Sigfox
Bandwidth	1.08MHz	180kHz	600kHz	125kHz (500kHz d/l)	100Hz (1.5kHz d/l)
Max. Coupling Loss	approx. 160dB [1]	164dB [1]	164dB [1]	157dB [1]	153dB [1]
Typical Freqcy. Bands	Below or above 1GHz	Below or above 1GHz	Below or above 1GHz	Below 1GHz	Below 1GHz
Max. Downlink Peak Data Rate	1Mbps	250kbps	74kbps	50kbps	600bps
Max. Uplink Peak Data Rate	1Mbps	250kbps	74kbps	50kbps	100bps
Typical Downlink Daily Throughput	Limited only by battery power	Limited only by battery power	Limited only by battery power	~ 200B [2]	24B
Typical Uplink Daily Throughput	Limited only by battery power	Limited only by battery power	Limited only by battery power	~ 200kB [2]	1.64kB
Typical Module Cost	Medium	Low	Low	Low	Very low
Globally Unique Identifiers	IMSI	IMSI	IMSI	Optional (DevEUI)	Yes (32 bits)
Device / Subscriber Authentication	UICC or eUICC [3]	UICC or eUICC [3]	UICC or eUICC [3]	Device or Subscriber [4]	Device
Network Authentication	LTE AKA	LTE AKA	UMTS AKA	Optional	No
Identity Protection	TMSI	TMSI	TMSI	Partial (DevAddr)	No
Data Confidentiality	Yes (EEAx)	Yes (EEAx)	Optional (GEA4/5)	Yes (AppSKey)	No
End-to-Middle Security	No	No [5]	To visited network	Yes (AppSKey)	No

[1] These figures are provided as a guide only; precise comparisons may be misleading as link budget assumptions vary in the calculations for each technology

[2] Based on The Things Network Fair Access Policy (in https://www.thethingsnetwork.org/forum/c/nodes)

[3] UICC and eUICC both authenticate the mobile subscription, for a non-removable eUICC the EID also serves to uniquely identify the device

[4] Pre-provisioned NwkSKey authenticates the device, or default AppKey (permitted by TTN) authenticates the subscriber, or unique AppKey authenticates both

[5] Under discussion for a future 3GPP release (SA3 work item "Battery Efficient Security for Very-Low-Throughput MTC Devices")

	LTE-M	NB-IoT	EC-GSM-IoT	LoRaWAN	Sigfox
Forward Secrecy	No	No	No	No	No
Data Integrity	Limited [6]	Optional (with DoNAS)	Limited [6]	Limited [6]	Variable [7]
Control Integrity	Yes (EIAx)	Yes (EIAx)	Optional (GIA4/5)	Yes	unknown [8]
Replay Protection	Yes	Optional (with DoNAS)	Limited [9]	Yes	Yes
Reliable Delivery	Yes	Yes	Yes	No	No
Critical Infrastr. Class	Access Classes 11-15	Access Classes 11-15	Access Classes 11-15	No	No
Updatability (Device)	Possible	Possible	Possible	Limited [10]	No
Updatability (Keys / Algs.)	Optional (SIM OTA)	Optional (SIM OTA)	Optional (SIM OTA)	Limited	No
Nwk. Monitoring and Filtering	Yes	Yes	Yes	Limited	Monitoring only
Key Provisioning	pre-provisioned or RSP	pre-provisioned or RSP	pre-provisioned or RSP	pre-provisioned (ABP) or OTAA	pre-provisioned
Algorithm Negotiation	Yes	Yes	Yes	No	No
Class Break Resistance	Yes [11]	Yes [11]	Yes [11]	Optional [12]	Yes [11]
Certified Equipment	Required	Required	Required	Optional	Required
IP Network	Optional	Optional	Yes	No	No

Bandwidth, Maximum Coupling Loss and Frequency Bands

Although these features are not security features, they are included in the table above as they may be significant factors in the choice of which LPWA technology to use. They all affect the range and penetration of the radio signals, but there is no simple calculation which can usefully predict that range or penetration as local environmental factors also play a big part. However, other things being equal, a lower bandwidth, a higher maximum coupling loss and/or a lower frequency band will result in a longer range and better penetration through buildings and other structures.

The bandwidth, frequency selection and radio modulation also influence how susceptible the signal is to malicious jamming.

Maximum Downlink and Uplink Data Rates

These features are also not security features as such, but they may limit the sorts of security features which are included in the network protocol or which can be layered on top by applications. Low rates may

[6] Where data encryption is in use, modifying ciphertext will corrupt the data unpredictably
[7] A 16-byte Message Authentication Code is truncated to fit within a fixed size packet: only 2 to 5 bytes are transmitted, depending on the space available in each packet.
[8] Sigfox does not disclose the algorithm for calculating the Message Authentication Code, thus it is unknown how much of the control information (if any) is covered.
[9] Where data encryption is in use, replaying ciphertext will not result in the same plaintext
[10] Firmware update broadcast capability is under discussion for a future LoRaWAN version
[11] No private or secret keys are shared between devices
[12] Devices may share a default AppKey, which is thus subject to a class break

not suit sophisticated handshaking (e.g. for security algorithm negotiation and key agreement) due to the consequent high latency.

The maximum rates experienced in a real deployment will vary due to optionality in the network, network load and environmental factors; the numbers shown in the table here are chosen to be representative of a deployment with favourable to ideal conditions.

Daily Downlink and Uplink Throughput

Because of the low-power requirements, and also due to regulatory constraints, devices using LPWA technology will not be continually transmitting or receiving. In practice, the duty cycle (percentage of time on-air) and dwell time (maximum length of time on air in a continuous burst) will both be constrained. In order to understand how much data can be sent over extended periods, and therefore understand the limitations on security features such as over-the-air updates, we have listed the maximum amount of data (measured in bytes) that can be typically be sent, uplink or downlink, in 24 hours.

Regulatory duty cycle restrictions apply equally to base stations and, where many devices are communicating with a single base station, downlink capacity has to be shared between all of them, meaning that the downlink throughput that each individual device sees will be greatly reduced. One exception to this is where the network protocol allows for broadcast messages which are simultaneously received by all listening devices.

It could be argued that an uplink-only device would have good security characteristics, as there would be no possibility for an attacker to contact the device and attempt to tamper with it over the air; however, in practice all the LPWA technologies considered here have some downlink capability to provide optional acknowledgement of uplink messages.

Module Cost

The last non-security feature we have listed is a typical range of cost for the device communications module. This may also be a significant factor in choosing a LPWA technology, particularly for use cases with large numbers of very low cost sensor devices; nevertheless, care should be taken that the cost influence does not cause necessary security features to be omitted.

Globally Unique Identifiers

Authentication procedures (see below) are usually based on the subject first asserting a particular identity, so that the relying party can then verify that the subject's credentials match that identity. There is an underlying assumption therefore that the identifier is unique to a particular subject. If this is not the case, then any authentication of that identity might potentially be subverted.

One example of a potentially subvertible identifier is the IMEI (International Mobile Equipment Identity) used in 3GPP networks; the registration protocol ensures that the network accurately receives the IMEI asserted by the mobile device, and device certification requirements include the requirement that the device manufacturer prevent tampering with the IMEI; nevertheless, for various reasons false and duplicate IMEIs can be seen, for example when counterfeit devices are cloned.

A good example of a reliable unique identifier is the IMSI (International Mobile Subscriber Identity) embedded in 3GPP SIMs or USIMs. Certification programmes ensure that both the IMSI itself, and the associated subscriber authentication key *Ki*, are provisioned in a highly secure environment and stored in strongly tamper resistant storage.

Authentication: Device, Subscriber and Network

There are various parties involved in the establishment of network connectivity, each of which may desire to authenticate themselves to the other parties. For our purposes here we are considering the device itself, which may have embedded authentication credentials, the subscriber (individual or organisation) responsible for the connection, that may provision their authentication credentials to the device, and the network provider, that may share authentication credentials with the device so it can avoid connecting to an inauthentic (spoofed) network provider.

Authentication credentials (typically a shared secret key, or a public / private key pair) may be held in a high-security environment isolated from the normal operation of the device. Hardware elements may be removable (e.g. a UICC), fixed to the device circuitry (e.g. an embedded UICC – eUICC) or, in the future, integrated with the baseband processor system-on-chip (e.g. an integrated UICC – iUICC). The specification for iUICC is, at the time of writing, in the early stages of standardisation (requirements are being considered as part of ETSI project TS 103 465). A Trusted Execution Environment sharing the baseband processor may be used as an alternative to an independent hardware secure element, although this may provide less assurance of security.

As well as being concerned with secure storage of authentication (and encryption) keys, we need to also consider how those keys are initially provisioned, whether as part of the manufacturing process or via an Over-the-Air (OTA) activation mechanism; similarly, keys may need to be replaced, either periodically, as a precaution, or at need, following a key compromise. Further consideration is in the Key Provisioning section below.

The choice of authentication algorithms and protocols may be constrained by limitations of data throughput and/or power requirements for the necessary computations, but still need to be appropriate for the chosen use case.

Identity Protection

Some protocols include privacy-preserving measures to minimise the use of permanently allocated identifiers which could be intercepted and correlated with device activity over time. An example of this is the TMSI (Temporary Mobile Subscriber Identity) allocated by 3GPP networks to address the mobile device instead of the IMSI (International Mobile Subscriber Identity) which is only used once each time the device is powered on.

Data Confidentiality

For wireless networks, data confidentiality is almost always achieved by encryption of the data, as it is assumed that an attacker may be able to intercept the transmission and physical access controls would be infeasible. Although a lot of attention is paid to the strength of encryption algorithms and the length of encryption keys (perhaps because it is easy to compare numbers) in practice these are not the most important factors in the effectiveness of the security; real-world breaches of encrypted data are usually down to the keys being exposed due to weaknesses in key generation, derivation or storage, or due to weaknesses in algorithm negotiation.

It is commonly accepted that shared-secret 64-bit symmetric keys are not adequately secure against "brute force" key search given today's computing capabilities[13], but it should be appreciated that each extra bit doubles the computational power required for exhaustive key search, so 128-bit key lengths are expected to be secure for many years to come (see NIST 800.57). The calculation for public/private key pair lengths is somewhat more involved, but public key cryptography is not usually used for data encryption anyway, due to the significantly higher computational power needed.

A common technique for compromising data confidentiality by a "man in the middle" is to downgrade the selected encryption algorithm to an easily brute-forced, or even a null, cipher. Such "active" attacks can be mitigated by mutual authentication between the device and network prior to negotiating the encryption algorithm, or having a "white list" in the device which permits only strong encryption algorithms.

End-to-Middle Security

There will be more than one communication "hop" between the end device and the server which is the destination or source of messages; the radio interface is just the first of them. For cellular networks, it is usual for there to be concentrators between the radio base stations and the core network, as shown in the below diagram, which is based on the GSM network architecture. The concentrators (Base Station Controllers in this example) have communications links which an attacker could potentially intercept,

[13] GPRS networks are, at present, using 64-bit session keys; this is less than ideal, and migration to 128-bit keys is planned. It may nevertheless still be considered acceptable for some use cases as the duration of use of each session key is quite short.

particularly where these are wireless (such as the microwave link shown) so we need to consider the security protections of these links as well as radio link between the device and the Access Network.

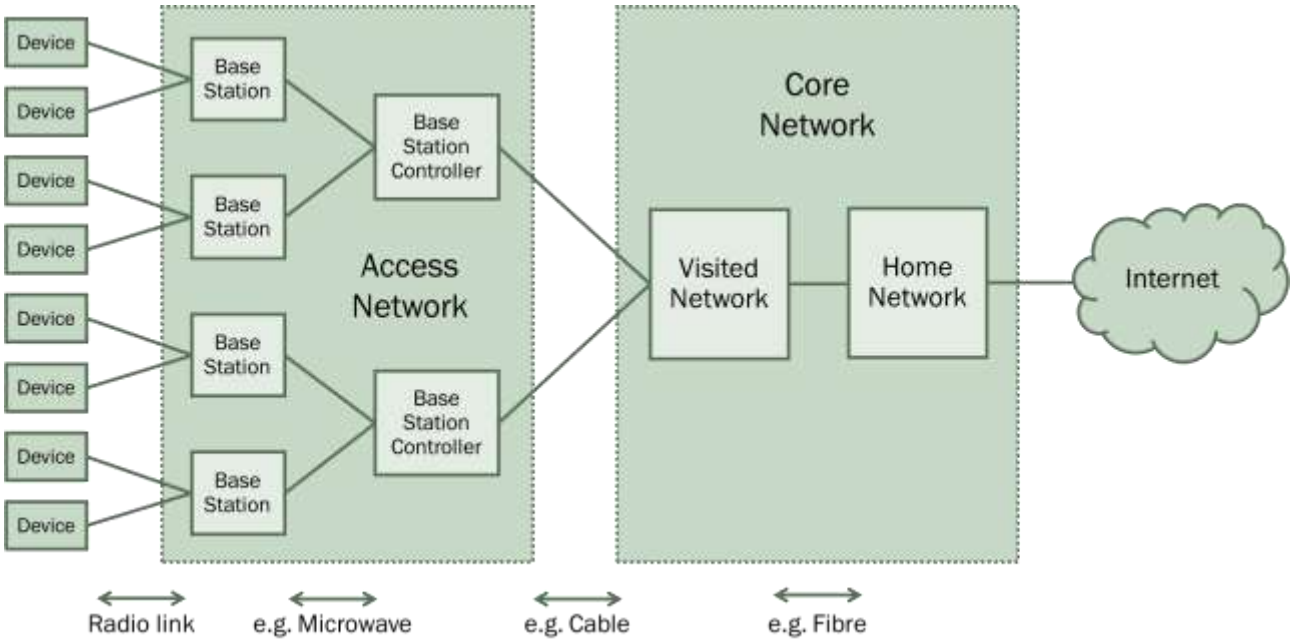

Figure 1 - Cellular Network Architecture with Intermediate Communications Links

There is a further, related concern for roaming use-cases, when the visited network may not be considered as trustworthy as the home network, and there is a desire not to depend on the visited network to provide confidentiality or integrity.

One way of addressing these concerns is to establish an end-to-end security context at the application layer, but this may be infeasible in some cases due to limited device capabilities, and can have adverse effects on network monitoring capabilities (see below). Another approach can be an end-to-middle security context, between the device and the core network (or, potentially, all the way to the home network for roaming scenarios) which avoids trusting intermediate communications links.

This issue potentially arises for any network with a "star of stars" topology (e.g. LoRaWAN) where multiple gateways connect to a common network server. In such cases "end-to-middle" would indicate a security context established between the end devices and the network server.

It is possible to provide an end-to-middle security context for integrity protection, confidentiality protection, or both. Some networks may choose not to provide end-to-middle confidentiality protection due to a desire to provide local law enforcement agencies with lawful interception capabilities.

Forward Secrecy

Encrypted communication connections typically use a "session key" for the encryption which is derived from stored long-term keys; this can be done for performance reasons (when the stored keys are public/private key pairs) and also for security reasons, as use of a new key each time means that an attacker intercepting the communications would have to break the key for each session separately.

There remains the threat of long-term keys being exposed, in which case there is a risk that an attacker could repeat the calculations that had been done during the key agreement part of the communications and thereby derive the session keys. Forward secrecy is a property of a protocol in which there is not enough information revealed by the key agreement communication for an attacker to derive the session key even if the long-term keys are later exposed.

Note that forward secrecy does not promise to protect any communications established *after* long-term keys are exposed because, for example, an attacker in possession of the long-term keys could impersonate a legitimate party and derive session keys as a "man in the middle".

Forward secrecy is typically implemented using Ephemeral Diffie-Hellman Key Exchange, which is a public-key-based algorithm and relatively computationally intensive, thus perhaps unsuitable for many low-power devices. It is not provided by any of the data-link-layer protocols we are considering here, but could be implemented for specific use cases at a higher layer, for example using TLS (Transport Layer Security) with Ephemeral Diffie-Hellman cipher suites.

Data and Control Integrity

Integrity protection ensures that any tampering with the content of the communication by a "man in the middle" can be detected by the intended recipient. It is similar in operation to error detection, but the algorithms used have a cryptographic component so that it is infeasible for an attacker to forge a valid integrity measure.

With layered network architectures, control information (for example, routing addresses) is processed at different layers. Integrity protection applied at higher layers may protect application data but not the lower level control information, so we consider control and data integrity protection separately.

Replay Protection

Replay protection is a security property of a protocol such that messages recorded by an attacker will not be accepted by their recipient as legitimate if they are reinserted into the communications link later. This is important in scenarios where the content of the message is linked to some kind of commercial transaction, or, for example, where an attacker wishes to evade detection by a surveillance device by disabling it and replacing its transmissions with previously recorded normal activity.

Reliable Delivery

This is a security issue, as it directly pertains to the availability category of the Confidentiality / Integrity / Availability triad and indirectly affects other security characteristics as, without reliable delivery of messages, attackers could potentially block delivery of certain messages without the device and/or the network being aware of it. This is a somewhat different issue than Denial of Service, as jamming at a large scale would be noticed due to the large change in the amount of network traffic, but selectively blocking a few messages could be unnoticeable and benefit an attacker, for example avoiding their being detected by a surveillance device.

LPWA technologies with limited acknowledgement capabilities, such as LoRaWAN and Sigfox, may therefore be considered unsuitable for some use cases in which confirmation of successful delivery of messages is required.

Critical Infrastructure Class

For networks where capacity is shared between critical infrastructure (e.g. use by emergency services) and consumers, the concept of access classes may be implemented, so that in situations of abnormal high load, service to devices in critical access classes may be prioritised over less critical ones. In 3GPP networks, this is achieved by Access Class Barring which, when enabled, rejects connections from devices in lower-priority access classes.

Updatability (Device)

Device security vulnerabilities are a perennial issue, from the first PC viruses in the 1980s through to today's botnets of IoT devices (see Flashpoint report). New vulnerabilities are discovered every day, and the most effective response to such vulnerabilities is to patch affected devices with updated software or firmware. This is of course an issue for any type of connected device on any network, but the nature of LPWA technologies may make it harder to distribute such patches, given low data throughput and possible lack of reliable delivery (see above).

If distribution of patches is infeasible, some other mechanism needs to be present to deal with serious vulnerabilities, such as network-based Intrusion Prevention Systems (IPSes) (see below) or, in the worst case, blocking service to, or otherwise disabling, affected devices.

Updatability (Keys / Algorithms)

Similarly to device update capability, a mechanism should be in place to update long-term stored keys in case they should be compromised, or algorithms, should they be deprecated. In the case where the keys, and potentially algorithm implementations, are stored in a separate secure element, this may be a separate update mechanism from device update.

The expected lifetime of IoT devices (10 years in some cases) considerably exceeds the NIST recommended "cryptoperiods" (the length of time before a key should be replaced, typically less than 5 years, but dependent on risk factors, see NIST SP.800-57 Part 1). A mechanism to replace long-term keys held in the device and network is therefore highly desirable, if not essential in many cases.

Network Monitoring and Filtering

Monitoring functions within a network can be important for security. One example of this is Intrusion Detection and Intrusion Prevention Systems (IDS and IPS), which inspect network traffic in order to look for and block malicious payloads. An IPS may be a necessary mitigation if a vulnerability is discovered in end devices and, for some reason, it is infeasible to update the devices to patch the vulnerability.

If data is being encrypted end-to-end at the transport or higher layers, then the ability to inspect the network traffic in this way is severely restricted, preventing techniques such as deep packet inspection.

Key Provisioning

Cryptographic techniques for authentication, confidentiality and integrity all rely on cryptographic keys being shared between the subject and the relying parties. For public keys, this can be as simple as downloading them from a known source, but secret and private keys must be distributed in a secure way. Often a "root of trust" public key is embedded in device firmware at manufacture time, which can then be used to authenticate keys which are distributed later, although the compute power and volume of data required for such distribution protocols could exceed the capabilities of some very low power devices used with LPWA technology.

Secret keys are often pre-provisioned to devices as part of the manufacturing process, sometimes coupling a secure element for key storage and processing on the device (for example a UICC) with a Hardware Security Module (HSM) at the service provider. The HSM mitigates the risk of a security breach at the service provider allowing an attacker to capture copies of secret keys for many devices in one go; this risk is similar in scope to that of a Class Break (see below).

There may also be a need for secret keys to be renewed after manufacture, in cases that a long-term key has been in use for longer than its recommended lifetime (see Updatability (Keys / Algorithms) above) or if the device is to be re-personalised for a different network. The RSP (Remote SIM Provisioning) facility is a recently standardised mechanism for doing this for devices with an eUICC on a 3GPP network.

Algorithm Negotiation

Over time, the use of certain cryptographic algorithms may be deprecated, either due to advances in computing power or to flaws being discovered in their mathematical basis or design. This has been the case, for example, for RC4, MD5 and, most recently, SHA-1. Advances in quantum computing could cause similar deprecations (particularly to public key ciphers) within the anticipated service lifetime of IoT devices being deployed now, and cryptologic researchers continue to find new flaws in established algorithms. These threats should be anticipated in LPWA protocols by enabling devices and networks to support multiple algorithms, and to negotiate which algorithm should be used when a secure context is established.

Class Break Resistance

In situations where there are a large number of devices of the same type deployed, the risk of a class break occurs when the system design is such that an attacker who finds a way to compromise one device is then able to easily use the same method to compromise other devices of the same type.

This risk frequently arises when devices share the same secret or private keys, so that if the key from one device is exposed, perhaps by a lengthy or difficult attack, it can then be easily used to compromise other devices. Best practice is to ensure that secret and private keys are unique to each device.

Certified Equipment

There is a legal requirement in most jurisdictions for devices with radio transmission capability to have authorisation before they may be sold, for example FCC approval in the US, or the European Radio Equipment Directive; such requirements exist for both licensed and unlicensed bands. The primary focus of these requirements is on preventing harmful interference to other radio devices, and not, for instance, on reliable operation or security.

Network operators using licensed bands have an opportunity to specify and enforce much more wide-ranging certification requirements, and this is done for the 3GPP technologies covered here in processes managed by the Global Certification Forum (and PTCRB in North America).

Where device certification is mandatory, this can be enforced by network operators by only issuing valid authentication keys to manufacturers who have undergone the certification process and who contractually undertake to ensure their devices remain compliant.

IP Network

The choice of network layer protocol to run over the WAN (Wide Area Network) link layer has security implications. The most obvious choice is IP and, where it is used, it can be an enabler for implementation of well-tried and trusted standard security protocols, such as TLS, above the network layer; however, there is some potential downside as the use of IP may create an attack surface for Internet-borne threats such as botnets, if the device is reachable from the public Internet.

Threats from the public Internet when using IP can be much reduced by using a “Private APN” on 3GPP networks, so in effect the device is connected to a subscriber’s intranet, and can be protected by firewalls and other enterprise network security measures. A network operator may also use IP masquerading techniques such as Network Address Translation (NAT) to allow a device to make uplink connections to the public Internet while making it effectively undiscoverable in the reverse direction.

It is also possible to avoid the issue on the device by using non-IP protocols, such as the native LoRaWAN and Sigfox packet formats, or NIDD (Non-IP Data Delivery) options with 3GPP networks. This has advantages in avoiding the complexity and overhead of IP and, where the non-IP data traffic is tunnelled over the control plane, for example with NB-IoT DoNAS (Data over Non-Access Stratum), control plane integrity protection is also applied to the data. Nevertheless, it should be noted that traffic within the Core Network (see Figure 1 above) will still usually be carried over IP connections so it is not completely isolated from the public Internet. End-to-Middle security (as detailed above) may be an effective defence in this case. With non-IP protocols, there is typically some gateway entity which enables communication between a non-IP device and an IP-based server. This gateway entity may be combined with, or connected to, an application server providing APIs for Internet-connected clients to control the end device. Both gateway and application server may be points of attack, although they may still be considered defensive barriers if firewall-style filtering and blocking functionality is implemented.

Care must always be taken with layering security protocols, to ensure that any sensitive metadata is not being leaked by lower layers, and also to ensure that operations are performed in a sensible order, for example applying any data compression before encryption – typically encryption will drastically reduce the compressibility of data.

Representative Use Cases

To compare the effectiveness of the security features of the various LPWA technologies we will consider a set of example use cases. To avoid undue bias, we have selected five use cases which represent a typical deployment for each of the five LPWA technologies we are looking at. We will not be going through a comprehensive risk analysis, but we will summarise some of the main and distinctive risks for example

purposes. To organise the risks, we refer to the STRIDE categories from the Microsoft Threat Modelling Process:

- **S** poofing (typically a violation of authentication properties)
- **T** ampering (typically a violation of integrity properties)
- **R** epudiation (a concern if a transaction required authorization which could then be disputed)
- **I** nformation Disclosure (typically a violation of confidentiality or privacy properties)
- **D** enial of Service (a violation of availability properties)
- **E** levation of Privilege (typically a violation of authorization properties)

Two of the these risk categories (Repudiation and Elevation of Privilege) primarily relate to authorization, a concept which typically involves human initiation of some action; for IoT use cases, which typically don't involve human interaction, these are less relevant.

In addition to specific risks, we also consider the overall criticality of the system; the more sensitive or high-value the operations are, the more security assurance is needed.

Use Case 1: Smart Pallet

RM2, a global supplier of pallets and supply chain management services, is trialling RM2ELIoT, a track-and-trace solution using AT&T's LTE-M network. The mobility and roaming capabilities of LTE-M seem well suited to this use case.

The security needs of this use case depend to some extent on the type of goods being transported on the pallet. For high-value consignments, the main threat could be theft, and the main benefit might be triggering of alarms if the pallet deviates from its expected route or stops transmitting. For lower-value consignments, the main benefit might be in advising the recipient of the consignment's location to reassure them of the delivery schedule, with little incentive for anyone else to interfere with this.

There is also benefit in tracking the location of unloaded pallets, to ensure they are used efficiently and located where they are most likely to be needed.

For this use case, notable risks involving wide area communications are:

Spoofing
: An attacker may attempt to disable the tracker and use another device to send fake location updates.

Tampering
: An attacker may attempt to modify the location data sent by the tracker, or disable it and replay old location data.

Information Disclosure
: An attacker might discover the identity of a pallet carrying high-value goods and use its location to judge when was a good chance of stealing it.

The principal controls mitigating these risks are Device Authentication, Identity Protection, Data Confidentiality, Data Integrity, Control Integrity and Replay Protection. A recall and replacement of faulty tracker units is feasible, and so Update Capabilities are less critical than some other use cases. Because of the possibility of high-value consignments, assurance needs are relatively high, so strong Key Provisioning, Class Break Resistance and Certified Equipment are important.

Use Case 2: Smart Agriculture

Orange, in conjunction with Sierra Wireless and Nokia, is trialling EC-GSM-IoT, with a view to deploying it in emerging markets such as Africa in a range of applications, including deployment of connected sensors in fields to help determine the best time to plant and harvest particular crops. EC-GSM-IoT is attractive in this scenario due to its ability to reuse existing GSM network infrastructure.

This use case seems to exist in a low-threat context, particularly with the emphasis on emerging markets where individual targets would have a low value to attackers. Competitors with a grudge would likely find it easier to physically tamper with the sensors, rather than try to attack the LPWA technology.

The principal risk for this use case involving wide area communications seems to be:

Denial of Service

An attacker might seek to disable large numbers of devices, or the network service to them, to blackmail the service provider.

The principal controls mitigating this risk are Class Break Resistance and Network Monitoring and Filtering. Update Capabilities may be less important, given the low threat and the possible mitigation of attacks on weak keys or algorithms by network monitoring and filtering.

Use Case 3: Smart Street Lighting

Flashnet SRL, a technology company headquartered in Romania, offer the InteliLIGHT® Streetlight Management System using LoRaWAN. It can be used with either public or networks, with private networks seeming to be the main target.

The main benefits offered are energy saving (the lights run on an autonomous dimming schedule without requiring regular communication from the server) and monitoring for power efficiency and maintenance needs.

There are a several potential threats to a street lighting control system: residents might wish to override the lighting schedule to provide brighter or longer illumination than the local government has budgeted for, and the safety implications of turning off street lighting might make it a potential terrorist target. Nevertheless, the feature of autonomous operation means that the risk of Denial of Service attacks is not a major concern and, as the operation of the network can be considered not be safety-critical, assurance needs are less. There does not seem to be any confidential data nor any personally identifiable information (PII) being processed.

For this use case, notable risks involving wide area communications are:

Spoofing

An attacker might seek to impersonate the legitimate network in order to override the lighting controls.

Tampering

An attacker might seek to modify commands sent to the device in order to override the lighting controls.

The principal controls mitigating these risks are Network Authentication and Data Integrity. A recall and replacement of faulty devices is probably feasible, as there would be maintenance crews for servicing bulbs and other components of the street lights, so Update Capabilities would be nice to have, but perhaps not essential.

Use Case 4: Water Metering

Vodafone and Aguas de Valencia are trialling water meters in Spain using NB-IoT; meters are installed in both domestic and commercial premises. NB-IoT is attractive for this use case because of the low power requirements and good propagation to hard-to-reach locations.

The main benefits are for the utility company to obtain more frequent meter readings and to obtain them without having to visit the meter location.

There are a range of threats, including interference by the utility customer with the aim of reducing their bills. Assuming that there is no facility to disable the water supply, there may be no personal safety concerns, but there may be privacy concerns as fine-grained water usage data from a domestic property could be used to draw conclusions regarding the activities of the occupants.

For this use case, notable risks involving wide area communications are:

Spoofing

An attacker might seek to replace a device with a counterfeit one which transmitted lower readings.

Tampering

An attacker might seek to modify the readings sent by the device in order to reduce them.

Information Disclosure

An attacker might seek to learn about the activities of an individual occupying a domestic property.

Denial of Service

An attacker might seek to disable large numbers of devices, or the network service to them, to blackmail the service provider.

The principal controls mitigating these risks are Device Authentication, Data Integrity, Identity Protection, Class Break Resistance and Network Monitoring and Filtering. A recall and replacement of faulty devices may not be feasible[14], as a significant benefit is avoiding the need for in-person visits to the deployment sites, so Update Capabilities are considered important for this use case.

Use Case 5: Domestic Smoke Detectors

Cobject SAS offers the SMOCKEO smoke detector using the Sigfox network to provide remote status monitoring, management and alerts. They cite the low subscription costs as a particular advantage of Sigfox, as well as long battery life. Sigfox is the sole communication technology implemented, there is no secondary fall-back.

The main benefit is for users to receive remote notifications of alarms, direct to their smartphones via a voice call, SMS, email or app notification. A secondary benefit is to receive a notification when battery replacement is necessary.

Threats introduced by the use of LPWA technology seem low. An arsonist might seek to prevent the alarm being triggered, but there does not seem to be a function which remotely disables an activated detector. As it is a safety device, we might expect there to be safety implications of the LPWA technology, but the worst case seems to be preventing the remote notification, and if the user is remote then their personal safety is not in danger. There is a potential threat of extortion of, or reputational damage to, the service provider by means of a denial of service, but as it would not disable the autonomous local operation of the detector, the consequences would not be catastrophic. A further threat could be a denial of service causing a low battery warning to be missed, but this is mitigated by the system design which includes a periodic status check, the absence of which would be noticed.

The principal risk for this use case involving wide area communications seems to be:

Denial of Service

An attacker might seek to disable large numbers of devices, or the network service to them, to blackmail the service provider.

The principal controls mitigating this risk are Class Break Resistance, and the use of a non-IP network. If a different LPWA technology were used with an IP network layer, then Network Monitoring and Filtering would be desirable to mitigate DoS attacks launched from the public Internet. The units do not have Update Capabilities; this may be acceptable given then general low threat level, although the anticipated unit lifetime of 5 years is quite long.

Conclusions

Ranking Security Capabilities

It is, of course, not the case that the security needs of two different use cases, or even the security features of two different technologies, can be easily compared using a single measure. Security is a holistic property of a system, not something that can be considered in isolation nor added on as a

[14] This assumption will of course not apply to all water metering deployments; we have made the assumption here in order to make our representative use cases more distinct.

separate component. The diagram below illustrates that the trust and confidence in a system, that it will be "secure", is built up from lower-level building blocks:

Figure 2 - Security Building Blocks

The first supporting level is an understanding of the rights and responsibilities of the various parties interacting with and within the system, coupled with assurance that those rights and responsibilities will be enforced by the system's architecture, design and implementation.

The next level is the classic "information security triad": confidentiality, integrity and availability. We have also added accountability here as a separate category, although it is sometimes included within the definition of integrity.

The next level is the set of security controls within the system. These concepts are essentially the same as those defined by the Trusted Computer System Evaluation Criteria ("orange book") in 1985, although the term "Renewable Security" came a little later.

The bottom level consists of individual security features like those we have listed in the Feature Descriptions section of this report. It should be clear that focusing on those in isolation will not tell us much about the security of the system as a whole; we need to understand whether those features are being used in the right part of the system for the right reasons.

Layered Security

In cases where the security provided by the LPWA link layer and physical layers are not adequate for a particular use case, it may still be possible to meet the security needs by adding additional layers of security; this will of course come at a cost, whether for additional hardware, additional software development or licensing, or additional power or bandwidth consumption, but in some cases this may be the best solution within the particular constraints of the business.

A typical hardware improvement, for those networks that do not mandate a secure element such as a UICC, is to add a secure element to store and process long-term keys. Many vendors are now offering secure elements for Sigfox and LoRaWAN, which embed the storage and processing of keys at the link layer and, in many cases, other keys for implementing data confidentiality at higher layers. Although a secure element would not be a requirement for all use cases, there does seem to be a trend in recommending their use by default.

Software improvements would typically be in implementing higher-level security protocols such as TLS to provide an end-to-end, or end-to-middle where the middle is an application server, security context. If properties such as non-repudiation are needed by the use case, these do typically need to be implemented at the application layer, as an understanding of the data flow and the consequences of a transaction are needed to implement it effectively.

It is rarely wise to invent a new protocol, even if the standard protocols available seem to have unacceptable overhead; often such overhead is necessary to cope with risks which have been discovered during open peer review or accumulated experience of deployment, and a developer creating their own protocol would not be in a position to discover such risks in a new protocol by themselves. Some optimisations of standard protocols may be achieved by "profiling", that is removing optionality which is not required by the particular use case, but care must still be taken that the assumptions behind such profiling will remain valid for the lifetime of the resulting system.

Ideally higher-level protocols should take advantage of security features present in, and security contexts established by, lower-level protocols. One good example of this is GBA (Generic Bootstrapping Architecture), an application-level technology which takes advantage of the security context established by an underlying 3GPP network to authenticate a user to an application server.

Security Suitability of LPWA Technologies by Use Case

To produce the table below, we have considered the relative importance of the principal controls listed for each of the use cases above, and how strong the implementation of the supporting features is in each of the LPWA technologies we have covered. Rather than show the many individual comparisons involved, we have summarised them with a single grading for each use case and technology below.

Where the grading is affected by optional controls highlighted in the Feature Comparison Table shown earlier in this document, we have shown the suitability assuming that appropriate optional controls are enabled, indicated by asterisks (*) in the table.

Table 2 - Security Suitability by Use Case

	LTE-M	NB-IoT	EC-GSM-IoT	LoRaWAN	Sigfox
Smart Pallet	Good	Good *	Adequate	Good	Poor
Smart Agriculture	Good	Good	Good	Adequate	Adequate
Smart Street Lighting	Adequate	Good *	Adequate	Adequate *	Adequate
Water Metering	Adequate *	Good *	Adequate *	Adequate	Poor
Domestic Smoke Detectors	Good	Good	Good	Adequate	Adequate

It can be seen from this table that there is not a simple ordering of these technologies from best to worst, and even those with fewer security features may be a sensible choice for some use cases.

IoT Security Recommendations

In the course of this analysis, we have noted that several potentially important security features of LPWA technologies are in some way optional (see the Feature Comparison Table), in that they may be directly enabled or disabled by the network operator, or they are dependent on other choices made by the network operator.

LPWA IoT security guidance therefore should include advice to those deploying devices to check whether their use case needs any of these optional features, and advice to the network operators to ensure they are aware of the security consequences of the choices they make in their network configuration and to ensure that the state of these options is clearly communicated to their customers. Some optionality is also in the control of the device manufacturer (such as whether to include a fixed secure element such as a non-removable eUICC) and the same duty to communicate the security implications of this to their customers applies.

Specific recommendations are to evaluate the following characteristics:

For All LPWA Network Technologies:

- Whether an IP network layer is implemented over the link layer.
- Whether a secure element is present, and if so, whether it is removable.
- To what extent data integrity is guaranteed.
- Whether any algorithms or key lengths supported by the technology are black-listed or should be deprecated (such as 64-bit encryption keys for GPRS).

For 3GPP LPWA Network Technologies:

- Whether Remote SIM Provisioning (RSP) is supported.
- Which integrity algorithms (EIAx/GIAx) and confidentiality algorithms (EEAx/GEAx) are implemented and permitted.

For LoRaWAN:

- Whether ABP (Activation By Personalisation) or OTAA (Over-The-Air Activation) is implemented, and for OTAA whether an AppKey may be shared between devices.

For All LPWA Devices:

- What form (if any) of security certification has been undertaken.

Glossary and Abbreviations

2G	2nd Generation
3GPP	3rd Generation Partnership Project
4G	4th Generation
ABP	Activation by Personalisation (pre-provisioned keys for LoRaWAN)
APN	Access Point Name
AppKey	Application Key (LoRaWAN, used in OTAA to derive NwkSKey and AppSKey)
AppSKey	Application Session Key (LoRaWAN, key used to ensure data confidentiality)
DevAddr	(LoRaWAN) Device Address (non-unique)
DevEUI	(LoRaWAN) Device EUI (IEEE format unique identifier)
DoNAS	Data over Non-Access Stratum
DoS	Denial of Service
EDGE	Enhanced Data rates for GSM Evolution (a "2.5G" technology)
EEA	EPA Encryption Algorithm
EIA	EPA Integrity Algorithm
EID	eUICC ID (part of the GSMA RSP specification)
EPA	Evolved Packet System (a 4G technology)
ETSI	European Telecommunications Standards Institute
eUICC	embedded UICC
FCC	Federal Communications Commission
GBA	Generic Bootstrapping Architecture (a 3GPP specification)
GEA	GPRS Encryption Algorithm
GIA	GPRS Integrity Algorithm
GPRS	General Packet Radio Service (a 2G technology)
GSM	Global System for Mobile Communications
GSMA	GSM Association
HSM	Hardware Security Module
ICT	Information and Communications Technology

IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
LoRa	Long Range
LPWA	Low Power Wide Area
LTE	Long Term Evolution (a 4G technology)
MTC	Machine-Type Communication
NAT	Network Address Translation
NB	Narrow Band
NIDD	Non-IP Data Delivery
NIST	(USA) National Institute of Standards and Technology
NwkSKey	Network Session Key (LoRaWAN, key used to ensure message integrity)
OTA	Over The Air (management interface for SIMs)
OTAA	Over-The-Air Activation (key distribution for LoRaWAN)
PTCRB	(originally) PCS Type Certification Review Board
RSP	Remote SIM Provisioning (a GSMA specification)
SA3	3GPP technical specifications group for Service and System Aspects, security subgroup
SIM	Subscriber Identity Module
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System (a 3G technology)
USIM	Universal Subscriber Identity Module
WAN	Wide Area Network

References and Further Reading

3GPP	TS 22.011 Section 4	Service Accessibility: Access Control	http://www.3gpp.org/DynaReport/22011.htm
3GPP	TS 33.220	Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)	http://www.3gpp.org/DynaReport/33220.htm
3GPP	TS 33.863	Study on battery efficient security for very low throughput Machine Type Communication (MTC) devices	http://www.3gpp.org/DynaReport/33863.htm
3GPP	TS 43.020 Annex H	Access security related functions for enhanced General Packet Radio Service (GPRS) in relation to Cellular Internet of Things (CIoT)	http://www.3gpp.org/DynaReport/43020.htm
ABI Research		Best Fit Use Cases for LPWANs	https://www.abiresearch.com/whitepapers/best-fit-use-cases-lpwans/
ERC	Rec 70-03	Relating to the use of Short Range Devices (SRD)	http://www.erodocdb.dk/docs/doc98/official/pdf/rec7003e.pdf

ETSI	TS 102 310	Extensible Authentication Protocol support in the UICC	http://www.etsi.org/
ETSI	TS 103 465	Smart Cards; Requirements for a new secure element	https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=50517
EU	Directive 2014/53	Radio Equipment Directive	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014L0053
Flashpoint	Article	New Mirai Variant Leaves 5 Million Devices Worldwide Vulnerable	https://www.flashpoint-intel.com/blog/cybercrime/new-mirai-variant-involved-latest-deutsche-telekom-outage
GCF	White Paper	GCF Certification: “Test once, use anywhere” certification for mobile devices	http://www.globalcertificationforum.org/images/downloads/GCF-WP-GCF_Certification_June2014.pdf
GSMA	CLP.11	IoT Security Guidelines Overview Document	http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/
GSMA	CLP.14	IoT Security Guidelines for Network Operators	http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/
GSMA	FS.04	Security Accreditation Scheme for UICC Production	http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme
GSMA	SGP.01	Embedded SIM Remote Provisioning Architecture	http://www.gsma.com/connectedliving/embedded-sim/
GSMA		Introducing Mobile Connect – the new standard in digital authentication	http://www.gsma.com/personaldata/mobile-connect
GSMA		3GPP Low Power Wide Area Technologies White Paper	http://www.gsma.com/connectedliving/wp-content/uploads/2016/10/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper.pdf
GSMA		Wireless Security in LTE Networks	http://www.gsma.com/membership/wp-content/uploads/2012/11/SenzaFili_WirelessSecurity_121029_FINAL.pdf
GSMA		The future of the SIM: potential market and technology implications for the mobile ecosystem	https://www.gsmaintelligence.com/research/2017/02/the-future-of-the-sim-potential-market-and-technology-implications-for-the-mobile-ecosystem/601/
UK ICO		Conducting privacy impact assessments code of practice	https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
IEEE	Journal Article	Low Power Wide Area Networks: An Overview	https://arxiv.org/abs/1606.07360
IETF	Draft	LPWAN Overview	https://tools.ietf.org/html/draft-ietf-lpwan-overview-01
IETF	RFC 4186	Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)	https://tools.ietf.org/html/rfc4186

IETF	RFC 5448	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)	https://tools.ietf.org/html/rfc5448
IoT Alliance Australia		Internet of Things Security Guideline	http://www.iot.org.au/s/IoTAA-Security-Guideline-v10-fh2z.pdf
IoTUK		Internet of Things Taxonomy	https://iotuk.org.uk/an-iot-taxonomy/
LoRa Alliance	V1.0.2	LoRaWAN™ Specification	http://portal.lora-alliance.org/DesktopModules/Inventures_Document/FileDownload.aspx?ContentID=1398
LoRa Alliance	V1.0	LoRaWAN™ Regional Parameters	http://portal.lora-alliance.org/DesktopModules/Inventures_Document/FileDownload.aspx?ContentID=1397
LoRa Alliance		LoRaWAN™ Certification Process	https://www.lora-alliance.org/Products/Certification-Overview
Microsoft	SDL	Security Development Lifecycle	https://www.microsoft.com/en-us/sdl/
NIST	IR 7298	Glossary of Key Information Security Terms	http://dx.doi.org/10.6028/NIST.IR.7298r2
NIST	SP.800-57	Recommendation for Key Management, Part 1 – General	http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4
Schneier on Security	Article	Class Breaks	https://www.schneier.com/blog/archives/2017/01/class_breaks.html
Sigfox		Make things come alive in a secure way	http://www.sigfox.com/en/resources/white-paper/make-things-come-alive-a-secure-way
SIM Alliance		5G Security – Making the Right Choice to Meet your Needs	http://simalliance.org/wp-content/uploads/2016/02/SIMalliance-5G-Security-Technical-Paper.pdf
US DoD	5200.28-STD	Department of Defense Trusted Computer System Evaluation Criteria	http://web.archive.org/web/20060101084525/http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

Acknowledgements

We wish to thank the GSM Association for the funding which enabled this study, and for their remit that our conclusions should be fully independent and unbiased.