Remote SIM Provisioning over Narrowband IoT

Kigen

White Paper | **November** 2020

Contents:

Is it plausible to employ remote SIM provisioning over Narrowband IoT? This is the question on the lips of many IoT innovators looking to leverage the benefits of NB-IoT cellular connectivity. In this whitepaper, we consider the key factors affecting the inclusion of remote SIM provisioning capabilities on NB-IoT enabled devices.

NB-IoT is gaining momentum

The Internet of Things (IoT) is growing rapidly, with 27 billion connected devices predicted to be deployed by 2025 (Machina Research 2016). All these devices will require safe, reliable and ubiquitous connectivity to deliver valuable insights that help drive efficiencies and gain competitive edge. Cellular technologies are ideally positioned and scaled to deliver this, but the increasing variety of new IoT devices and services is calling for new cellular technologies to satisfy specific connectivity needs.

Narrowband IoT (NB-IoT) is one of the top emerging low power, wide area networking (LPWAN) cellular technologies that satisfy the growing demand for off-grid connectivity for very large deployments of low-complexity IoT devices.

NB-IoT technology offers great power efficiency, system capacity and spectral efficiency at a low price. Easy to set up, it has already been launched by 96 Operators across 54 countries, where they continue to invest in its rollout, footprint and inter-operator global roaming agreements (Figures as of August 2020).

It promises a wide range of benefits to different stakeholders:

For manufacturers of IoT devices, it is a more economical alternative if compared to LTE-M, due to the lower device complexity and device build and connectivity costs.

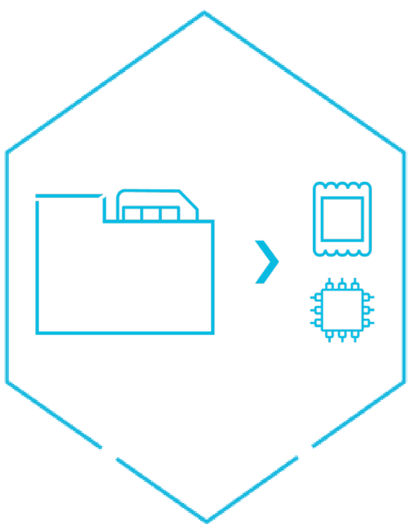
For enterprises managing large IoT deployments, it offers lower cost, reduced power consumption and a simple protocol.

For mobile network operators (MNOs), it compliments existing 3G and 4G access networks and can be integrated into the common core network and BSS platforms. Additionally, flexibility is afforded to MNOs with the option of three possible modes of operation to make best use of their frequency allocation resources.

Overcoming limitations with remote SIM provisioning

Typically, the use cases that are best suited to employing NB-IoT connectivity are isolated, battery-powered deployments that are monitored remotely on a fleet basis and over an extended lifetime in excess of 10 years. Whether static or mobile, such IoT devices can expect to see changes in the network availability or competition for connectivity supply over their lifetimes. This means that a permanent tie to a single MNO network could be limiting or liable to future increases in connectivity costs.

Changing the carrier network is a straightforward commercial interchange. However, it requires to swap the SIM which is a costly logistical nightmare for the owners of widely distributed and hard to access IoT devices. To solve the limitations of a SIM that is permanently tied to a single MNO network, GSMA worked with the telecoms industry to standardize a SIM that could support the change of the carrier network without any visits to the device and physical SIM swapping.



Conceiving an NB-IoT device with this RSP capability would on the surface appear to be a very simple task. It would include an NB-IoT connectivity module and a GSMA accredited and complaint M2M eSIM, followed by completing some device assurance and interoperability testing. It is at the selection of the cellular components stage that the process ceases to be straightforward, however.

The GSMA remote SIM provisioning (RSP) specification delivers a comprehensive solution and security framework to enable the remote management of operator profiles in any supporting eSIM device. Its accompanying robust accreditation and compliance processes ensure functional interoperability and maintains and assures network access protection.

Let's look at the M2M RSP process to understand the key factors for enabling RSP over NB-IoT.

In simple terms, M2M RSP is the delivery to and management of operator profiles within the eSIM. RSP is conducted via the SM-SR (Subscription Manager – Secure Routing) over existing cellular connectivity (over the air) using either an out-of-the-box connectivity bootstrap profile or the currently active operational profile. The SM-SR keeps track of the eSIM state and holds the necessary network integrations, keys and certificates associated with the eSIM in order to authorise and execute profile management events.

Upon triggering, a management event commences with the sending of a SIM data SMS, via the active profile's network, through an integration (an SMPP bind) from the SM-SR to the serving message server (SMSC). Upon successful receipt of this, the card will either execute the command or - for a profile download event - establish a tunnelled data session with the SM-SR over which the profile is delivered followed by installation and optionally enablement. Upon successful conclusion of the event, successful or otherwise, the card and the SM-SR exchange further acknowledgment messages to ensure the status of the card's profiles remain in sync.

NB-IoT roaming: work in progress

If your device distribution aspirations are truly global, then the first stumbling block will be sourcing a bootstrap profile, to have included on your eSIM, that will offer ubiquitous out-of-the-box connectivity from a spread of the NB-IoT networks globally. The delivery of a profile that offers this relies on a wide enablement of network roaming capabilities. Without roaming, NB-IoT enabled devices cannot be deployed easily across national borders.

With NB-IoT still so new, a sustainable roaming environment and full framework for NB-IoT are still to be established. However, there is every reason to believe that the work in progress (See below) will soon add global roaming capability, with market pressure increasing MNO focus to expedite this. It is anticipated that the roaming capability will initially be offered strategically, between operators from the same MNO group or key players, however, today it is far from realised.

MNOs are trialling NB-IoT roaming agreements.

Vodafone and Deutsche Telecom and completed the first European NB-IoT roaming trial in 2018. They were able to test power saving features including Power Saving Mode (PSM), Long Periodic Tracking Area Update (TAU) and more. In 2019, Vodafone and AT&T signed an NB-IoT roaming agreement between Europe and the USA.

Devices need to handle multiple NB-IoT bands.

One of the advantages with NB-IoT is MNOs have spectrum options for implementation. Roaming gets more challenging when MNOs operate in different bands. Multi-band antennas can deal with all defined bands at a slightly higher cost per device. IoT device makers may be accustomed to optimizing antennas on a single band. Now, with roaming a possibility, more robust NB-IoT antenna designs are in order.

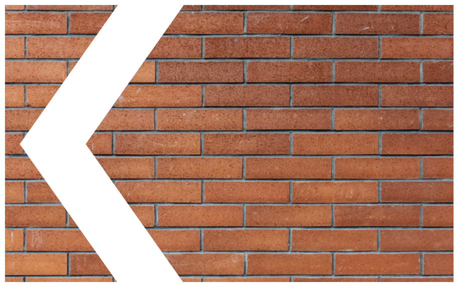
The GSMA has interoperability tests.

In 'Mobile-IoT Roaming Testing' released in March 2019, the GSMA defines a complete set of test instances for NB-IoT roaming. The test cases are agnostic of control plane versus user plane options, so they can test any implementation. These tests do not replace compliance testing, but rather verify roaming capability.

NB-IoT and MNOs

Aside from the absence of NB-IoT roaming, actually getting access to a NB-IoT subscription will, in many places, be difficult as the network operators are still in the process of expanding and commercializing this network footprint.

NB-IoT networks are expanding.
In many ways, NB-IoT looks and feels like LTE. MNOs can often support NB-IoT with a software upgrade on their network. Security measures are similar, with the same SIM-based authentication and traffic encryption.



NB-IoT goes where other networks struggle.
In live trials, Vodafone found NB-IoT penetrates double-brick construction better than alternatives. This makes for more reliable sensor connections in hard-to-reach places. NB-IoT avoids interference and network collisions, even with 100,000 devices on a single cell tower.

MNOs are accelerating NB-IoT rollouts.
GSMA's Mobile IoT Forum tracks cellular IoT progress. Adoption data as of August 2020:

- 96 operators have NB-IoT rollouts launched or in-progress;
- NB-IoT is supported in 54 countries at the moment
- By comparison, 46 operators have LTE-M rollouts launched or in-progress.

Despite this, whilst many can claim an NB-IoT network deployment, they are not yet in a position to offer commercialized propositions to the market or if they are, the network coverage is still localized at best. Furthermore, unlike 2G/3G/4G networks, all operators in a single country cannot boast an NB-IoT deployment, meaning that those that do can monopolize the market with little external pressure to force the tariffs down.

However, for a specification at the three-year mark, intent to adopt is already outstanding. It shows that the massive IoT opportunity is real and sustainable in the eyes of MNOs across the globe. Their only limitation is time to delivery, and this will be competing for engineering space with investment into the race for 5G which is seen as a priority.

Therefore, unless conducted in conjunction with an MNO's ongoing NB-IoT network trialing, anyone trying to develop an NB-IoT device will struggle to source the connectivity they need to bring a product to fruition.

Data messaging, protocols and availability

As we have outlined previously, most M2M RSP implementations require SMS and data via which the events are triggered and managed. Additionally, the device needs to be awake and available to receive the server instructions.

SMS support in the existing consumer centric cellular networks is a given, as despite the rise of data-oriented messaging apps, it is still seeing steady traffic and is an expected capability due to its historic support. Yet, for an NB-IoT network deployment, SMS support was not a mandated element, and many deployers have chosen not to support it in order to reduce initial network establishment engineering complexity; at least for now.

To date, there is no clear common industry wide approach to solve this current omission of SMS. A number of possibilities spring to mind, but these have to be considered in conjunction with the IoT device's use case. One such approach is to include support for an additional cellular technology, such as LTE CAT M1, to which the device can cut over and via which SMS is supported and RSP can be conducted.

In many deployments, SMS fits the usage pattern for NB-IoT devices – low cost, low power, long idle and short bursts of transmitting data. Supporting SMS on NB-IoT networks and devices opens the full potential of NB-IoT including RSP support and more efficient data transfers. In NB-IoT use cases, shorter, more efficient messages are ideal and not just for RSP profile management. For this reason, it is no wonder that the GSMA's NB-IoT Deployment Guide is lobbying hard for wider adoption of SMS in NB-IoT networks for transferring data.

Many IoT use cases are off-grid, where power saving is a must, with these devices spending most of their life in stasis and only waking for a specific activity. Devices serving such scenarios pose a problem to RSP, because for an event to proceed, the device needs to be awake to receive the call to action. An SMS, regardless of its purpose, typically has a time to live on the message server (SMSC) and MNOs will not be keen to hold these indefinably. As the number of sleeping devices associated to the network increase with the growth of massive IoT, long term storage of these SMS components is likely to impact the capacity and presents issues around message validity.

For RSP specifically, today the flow of events also requires the triggering to be time limited in order to ensure synchronicity and request freshness. With a device in a dormant state and not knowing when it is expected to be back online, the RSP servers face an impossible task without help. Such help could come from the device deployer's orchestration platform which may know either when the device has come online or have logic to be able to predict when this will occur. With careful orchestration, the device deployer can intelligently instruct the RSP platform to commence an event only when it knows it is likely to be successful. This type of approach increases efficiency and saves costs in the system.

NB-IoT modules ready for RSP

We have now considered the NB-IoT network and network services required for the support of M2M remote SIM provisioning. Let's finally focus on cellular module selection strategies and the support required from them for an NB-IoT device and RSP.

Typically, module manufacturers' portfolios contain products that offer support for the most common combinations of radio technologies and the frequency bands for these for the key target regions. The choice of radio technology support by these is often selected strategically to follow the direction that region's networks are evolving. Targeting the modules in this way allows for radio optimisation and reduces their frequency determination logic, ensuring the lowest price. It also assists when looking to achieve product certification from the industry and target networks. Modules offering global support also exist but will again target the most sought-after radio technology combinations and often come at a higher cost as they have to incorporate additional radio tuning and optimisation logic.

An IoT innovator's module selection therefore has to consider the devices geographical distribution intentions. If the intent is for a single model for the global market and or it is expected that the device will need to function outside its initial deployment country or region, then greater regional or even global support needs to be considered. With NB-IoT modules, the same considerations need to be applied, although uncertain network strategies and minimal deployments currently make it harder for the manufacturers to define their portfolio. Additionally, the limited NB-IoT deployments and support makes it trickier for module R&D.

The selection of SIM technology and its support also has a bearing on geographical device enablement. Whilst a removable SIM allows for a change of serving operator globally, this requires a maintenance action for an unattended IoT device and is at risk of theft. A soldered down embedded SIM minimalizes theft risk but results in being locked to one connectivity provider for the life of the product and limits global connectivity to roaming agreements with uncontrolled off-net quality of service. The utopia combines the ability to change serving carriers but removes the complexity of physically accessing the device and the risk of SIM theft whilst ensuring best possible cellular service. Selecting an embedded SIM with GSMA remote SIM provisioning (RSP) capability solves this, however, the module selected has to offer RSP support also.

For a cellular module to support RSP, it needs to include a few key features aside from the routine support needed to deliver standard telephony or data services. Often these are included as standard in a mainstream module used in a consumer handset. However, when it comes to modules targeting IoT devices and use cases, this is not always the case because unnecessary capabilities come at a cost. Therefore, regardless of which cellular bearer the IoT device is targeting, due consideration for the module's capabilities is to be paid if the support for RSP is being targeted. The support of Bearer Independent Protocol (BIP), as defined by ETSI, is a critical aspect as this ensures the modem can establish the secure data channel between the SIM and the RSP server over which the new profile is delivered. Support for SMS is also necessary in the server push mode in order to tell the eSIM it needs to carry our an RSP task.

Another key aspect that needs to be considered for a device that will support RSP is ensuring that the RSP event is allowed to conclude, which includes the sending and receipt of synchronisation transactions. The device must therefore ensure that it does not tear down the cellular connection prematurely so as not to leave the server and the card out of sync and an eventual failure of the requested action.

Further requirement details for M2M RSP capable devices can be found in Annex G of SGP.02.

When a technology is still in its infancy, those in a position to consider delivering any aspect of it have three options. They can take a punt and strive to be first to market as support emerges around them, they can wait for more mature deployments with a clearer market demand, broader support and proven interoperability or they can decide not to have a stake in market play.

The combination of NB-IoT and RSP bring two emerging technologies to the fore, making delivery of proven components more difficult which has an impact on those wanting to integrate these. Achieving a viable product cannot therefore be done in isolation, so realising a working solution where more than one party is developing, delivering and deploying an aspect of it, takes collaboration and an anticipated return on investment.

Growing the ecosystem

Kigen is in a prime positions to drive and enable NB-IoT adoption by lowering the barriers to entry and creating flexibility for device and module makers and MNOs. We want IoT devices to be ready with NB-IoT and RSP anywhere on the globe as soon as possible.

- MNOs and application providers can integrate RSP capability into their provisioning environment with Kigen Remote SIM Provisioning services. Our Data Centers in UK and US are SAS-SM accredited.
- Kigen SIM OS's helps OEMs create low power, low cost, secure eSIMs or iSIMs. Its secure, GSMA-compliant eUICC SIM OS stack is optimized for compactness and portability to multiple hardware form factors.

NB-IoT and enabling ubiquitous RSP for it are a big part of Kigen's vision. Scaling the massive IoT is creating opportunities unlike any seen in technology before. We're here to help grow the ecosystem, solving challenges and spurring IoT innovation everywhere.

Kigen