Building cellular connectivity into your next IoT design

Kigen

White Paper

Cellular connectivity options are available for a wide range of IoT use cases and solutions are in place to simplify the production, deployment, and operation of cellular-enabled devices.

Considerations for a cellular IoT project

One of the key requirements for many IoT use cases is reliable, secure, and extensive wireless connectivity. Cellular networks answer all these requirements, providing a stable, proven, and global service, with a history of strong security. Most countries worldwide are covered by at least one cellular network and the well-established principles of roaming allow devices to move easily between networks. Cellular networks already host billions of phones and have existing capacity available to support many more IoT devices.

Devices that use non-cellular network technologies often require complicated configuration as part of the deployment process. Cellular devices, however, can benefit from zero-touch provisioning. When a newly deployed device first connects to a network, it can be updated and configured automatically with settings that are tailored to both the customer and the deployment location.

Having decided to use cellular networks to provide connectivity for an IoT product, there are a number of factors to consider when starting a project:

- **Which cellular network technology to support:** As well as 2G, 3G, 4G, and 5G, cellular Low Power Wide Area Network (LPWAN) technologies are also being deployed by carriers.
- **Whether to use an eSIM or an iSIM:** Traditional Subscriber Identity Module (SIM) cards are not well suited to IoT use cases. Embedded SIMs (eSIMs) and Integrated SIMs (iSIMs) provide different benefits depending on the use case.
- **What to look for in a SIM OS:** The SIM operating system must provide support for the selected cellular network technology, as well as the eSIM hardware or iSIM security enclave.
- **How to provide out-of-the-box connectivity:** eSIMs and iSIMs require a special type of carrier subscription to provide initial connectivity for devices, wherever they are deployed.

- **What is required from a SIM personalization partner:** SIMs must be given a unique identity and loaded with the sensitive data that enables network authentication when they are manufactured.
- **How to integrate with an RSP platform:** Remote SIM Provisioning (RSP) is the mechanism by which carrier subscriptions can be changed on eSIMs and iSIMs once a device has been deployed.
- **Whether to partner with a connectivity management provider:** Connectivity management platforms offer services from a range of carriers, allowing enterprises to select the best subscription plan for their requirements without having to negotiate with each carrier.
- **Which standards and specifications are relevant:** Carriers require compliance with various industry standards and specifications for any devices that connect to their networks.
- **What to test before starting production:** Manufacturers should verify that the various elements of their solutions are interoperable before moving ahead with production.

In addition to the 2G–5G cellular technologies, there are variants that are designed for IoT devices.

Cellular network technologies

In addition to the familiar 2G, 3G, 4G, and 5G technologies, cellular standards bodies have created variants that address the needs of low power and low cost IoT devices. The global standards organization 3GPP has developed two LPWAN specifications that are based on the widely used Long Term Evolution (LTE) cellular standard: LTE Machine Type Communication (LTE-M) and NarrowBand-IoT (NB-IoT).

These technologies are specifically designed to facilitate cellular connectivity for machines through lower bandwidth and increased power efficiency. LTE-M has the advantage that it can use the LTE antennas on the existing network infrastructure, making it easier for carriers to deploy. Although NB-IoT requires carriers to install additional equipment, it is gaining in popularity because the infrastructure is less complex compared to LTE.

For more about business and revenue opportunities in cellular IoT, see:

- **Unlocking the cellular IoT potential for chipset makers**
- **eSIM and the Trillion-Device Opportunity**

LTE-M

LTE-M is designed to reduce device complexity and power consumption while retaining the existing LTE radio interface. The technology supports voice calls and connected mobility, and also provides a choice of power saving modes.

The LTE-M designation, where 'M' is a simplification of the original MTC (Machine Type Communication), covers several standards. It is typically used to refer to the Enhanced MTC (eMTC) standards LTE Cat M1 and LTE Cat M2, where 'Cat M' stands for Category Machine. The specification for LTE Cat M1 was finalized in 2016, with the additional device category LTE Cat M2 following in 2017.

LTE Cat M1 operates over a reduced bandwidth of 1.4MHz (as opposed to 20MHz for LTE) with peak data upload and download rates of around 1Mb/s. LTE Cat M2 increases the bandwidth of 5MHz with peak data rates in the region of 7Mb/s for upload and 4Mb/s for download. The LTE Cat M2 specification is fully backward compatible with LTE Cat M1. As a result, an LTE Cat M2 device can operate as an LTE Cat M1 device if the network does not support the later specification.

NB-IoT

NB-IoT technology targets ultra-low power edge devices. It provides a new low power radio interface and enables additional cost savings over LTE-M by further reducing device complexity. Unlike LTE-M, NB-IoT does not support voice calls or connected mobility, but it does include the same power saving modes as LTE-M. The NB-IoT specification was first released alongside LTE Cat M1 in 2016.

As indicated by the name, NB-IoT operates over a restricted bandwidth of 200kHz, with peak data rates of less than 100kb/s. The narrow bandwidth allows for more connections per cell, potentially up to 100,000 devices on a single cell tower. NB-IoT also offers greater radio signal penetration than LTE and LTE-M, which gives greater signal reliability under challenging conditions. It should also be noted that SMS availability on NB-IoT networks is not mandated so if your use case requires this, then it is a question to ask. This also can have an impact on the ability to leverage remote SIM provisioning. Understand more in our Remote SIM Provisioning over Narrowband IoT white paper.

Cellular technology choice is likely a compromise between hardware capability and the needs of the use case you're addressing.

Choosing a cellular technology

Ultimately, the choice of technology is determined by the use cases that are targeted by a System on Chip (SoC), radio baseband module, or device. A number of sometimes competing factors must be balanced. For example:

Power consumption: NB-IoT is specifically designed for power-constrained devices and so is likely to be considered for very small devices or applications where changing the battery is impractical or impossible. However, LTE-M is

Cellular modules go some way to aid design flexibility with optimized multi-mode options offering global operation and at a variety of price points.

more flexible, includes the same power saving modes as NB-IoT, and still offers improvements over 4G and 5G. So, LTE-M is worthy of consideration for all but the most demanding of power budgets.

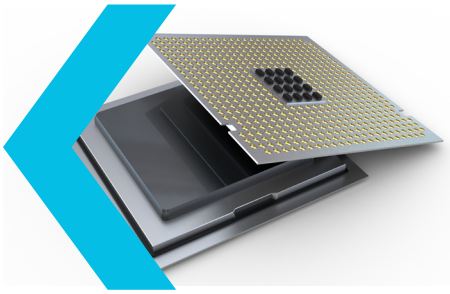
Performance: For scenarios where small amounts of data are transferred infrequently, such as static monitors or sensors, NB-IoT is the obvious choice. If larger amounts of data must be exchanged (cameras), or if latency is an issue (automotive), LTE-M offers similar performance to 3G and 4G. If these capabilities are still insufficient and ultra-low latency is required (remote control of critical infrastructure), then 5G must be considered.

Range: LTE-M and NB-IoT both offer increased range and improved penetration into buildings compared to 2G–5G, with NB IoT providing the best range and penetration.

Cost: Both LTE-M and NB-IoT should reduce device cost compared to 4G and 5G, with NB IoT expected to produce the greatest savings due to its simplicity. Additionally, NB IoT subscription plans are likely to significantly cheaper for enterprises compared to the other technologies.

Mobility: NB-IoT does not support seamless cell handovers. While it might meet the power and performance requirements of, for example, an RFID tag on a mobile asset, NB-IoT might not be the best choice for such an application. In this scenario, LTE-M could be considered. However, NB IoT does allow for cell reselection (at the cost of increased power consumption), so it could still be used in situations where the asset does not move often.

Voice: Unlike NB-IoT, LTE-M supports voice calls and so can be used as an alternative to 2G–5G in low traffic applications, such as always-on emergency call buttons. However, voice calls on LTE M are made over the data bearer, as with 4G and 5G, which requires additional service registration. So, LTE-M might be less suitable for voice applications than 2G and 3G, which use circuit switching.



Design longevity: Both LTE-M and NB-IoT are being aligned with the 5G standards, so a design that supports these technologies will have a long lifetime. Existing 4G networks are expected to be maintained in parallel with the forthcoming new 5G networks for some time.

Global SKUs: LTE-M and NB-IoT connectivity is not yet available in all markets. If minimizing the number of product options is paramount, the inclusion of multiple cellular connectivity technologies through a multi-mode modem

should be considered. In addition, the modem must provide coverage over the range of radio frequency bands that are used in the target geographies.

Flexibility: In cases where the choice between LTE-M and NB-IoT is unclear, or to increase the range of applications for a design, dual-mode LTE-M/NB-IoT modules are an option.

Application flexibility can be further enhanced by including 2G or 3G connectivity as a fallback option.

SIM types

Regardless of the technology, any device that connects to a cellular network must include a SIM for identification and authentication. SIMs are responsible for securely storing values that uniquely identify the SIM itself, which is associated with a subscription plan in the billing system of the carrier. Most importantly, the SIM also holds the sensitive credentials that are used to establish a connection with the carrier network.

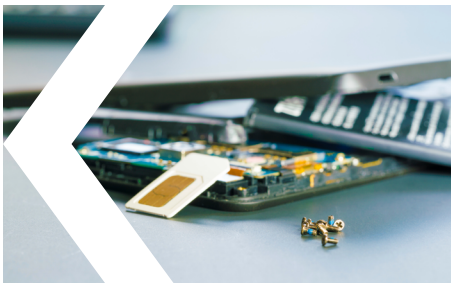
The chip in the traditional SIM card contains secure memory to store the identifiers and connection information. A secure processing element is also included to carry out the cryptographic operations that are involved in authenticating to a network.

The structure and operation of SIMs is highly standardized to ensure security, and for interoperability between devices and carriers. These capabilities mean that the SIM is also ideally placed to act as the hardware root of trust in an IoT device. Accordingly, the cellular network industry has developed IoT SIM Applet For Secure End-to-End Communication (IoT SAFE). This initiative allows the SIM to be used for credential storage and authentication to device management infrastructure instead of a proprietary hardware secure element.

The traditional SIM card suffers from drawbacks that make it less than ideal for IoT use cases.

The traditional SIM card was originally designed for cellular telephony and suffers from a number of drawbacks that make it less than ideal for IoT use cases. For example:

Size: Even the nano-SIM or 4th Form Factor (4FF) card that is widely used in phones today measures 12.3mm x 8.8mm. Along with the card tray and associated contacts, a SIM card can occupy a significant proportion of the space that is available in an IoT device.



Power: The power that is used by a traditional SIM card is largely out of the control of a module or device designer. However, some IoT use cases require battery lifetimes in excess of ten years, leading to highly constrained power budgets. In such scenarios, being unable to manage the power usage of the SIM and the SoC as a whole is a significant disadvantage.

Management: With traditional SIMs, changing networks usually means manually swapping cards. For IoT use cases, getting physical access to a fleet of devices can be expensive, impractical, or in some deployment environments, impossible.

Device durability: If it is to be removable, the SIM card cannot be sealed in the device. Leaving an opening for a SIM card increases the chances of water or dust penetrating the casing. In addition, traditional SIMs can be dislodged or damaged if the device experiences an impact.

Security: Making SIMs accessible for maintenance operatives to remove and replace also means that they are vulnerable to theft.

To address the concerns about traditional SIMs, the cellular network trade body GSMA developed specifications that enabled the creation of eSIMs and iSIMs.

eSIMs provide the same secure memory and processor as a traditional SIM card on a smaller, separate chip that can be soldered directly onto the device board. However, eSIMs still consume the same amount of power as removable SIM cards. iSIMs introduce further efficiencies by taking the functionality of the separate SIM chip and integrating it into a secure area within the SoC.

The key to enabling the use of eSIMs and iSIMs is the development by GSMA of two standards, an M2M and a Consumer specification, governing how SIMs can be updated remotely, without the need for physical access. This process, which is known as remote SIM provisioning, is discussed in a later section.

eSIM and iSIM enable use cases that are impractical or impossible with a traditional pluggable SIM.

eSIMs and iSIMs enable module designers and device manufacturers to design cellular-enabled products for IoT use cases that are impractical or impossible with traditional SIM cards. SoCs and devices can be smaller, cheaper, and in the case of iSIMs, can operate on less power. As a result, manufacturers can inexpensively add cellular connectivity to products that previously could not have had this feature.

For more about the advantages of eSIM and iSIM, see our other resources, including:

- SIM, eSIM, iSIM. What's the Difference?
- eSIM for Industrial IoT Applications
- Who can benefit from eSIM?

An eSIM is a chip that provides SIM functionality in a fraction of the area of a nano-SIM card.

eSIM

An eSIM is a discrete chip that provides SIM functionality in a fraction of the area of a nano-SIM card. The size of an eSIM chip in the Machine-to-Machine Form Factor 2 (MFF2) has been set at 6mm x 5mm by the ETSI standards body. Recently, some vendors have also started producing eSIMs in Wafer-Level Chip-Scale Packages (WLCSPs) that measure around 2mm x 2mm.

Because an eSIM is soldered directly onto the device board, there is no need for a card tray or the contacts that dictate the minimum size of a traditional SIM. The space that is saved provides the flexibility to specify larger batteries and more components, or to reduce the device size.

Manufacturers can add out-of-the-box global connectivity to their devices by arranging for a bootstrap profile to be included on their eSIMs during manufacturing. This initial connectivity enables remote provisioning of a local operator profile to the eSIM upon device deployment. As a result, device owners do not need to purchase locale-specific SIM cards for each device, and they do not need physical access to their devices to change the cards. This approach allows device manufacturers to greatly reduce the number of regional variants that they need to produce.

Because eSIMs are not removable, they are less vulnerable to theft or accidental damage than traditional SIMs. In addition, devices can be sealed to provide greater protection against harsh environments. Replacing the SIM card with an eSIM makes cellular connectivity viable for scenarios where accessing a SIM card is difficult. For example, where the deployment location is hazardous, where permission must be requested from the property owner to access the device, or where the number of devices makes individual management impractical.

As well as the different form factors, eSIMs are available in various of grades for different applications. For example, eSIMs for industrial and automotive applications are designed to withstand more extreme environmental conditions and to provide higher endurance than eSIMs for consumer IoT applications.

iSIMs are a combination of secure, dedicated physical circuits and an embedded SIM OS.

iSIM

Unlike traditional SIMs and eSIMs, iSIMs are not separate pieces of hardware. Instead, the SIM functionality is integrated onto the SoC with the application processor and, sometimes, the cellular modem. The iSIM is hosted in a secure enclave that is fully partitioned from the other SoC components.

The secure enclave is a physically isolated subsystem with a processing element to handle the sensitive data that is associated with cellular network authentication and other cryptographic functions. It is important to note that iSIMs are not purely implemented in software. Rather, they are the combination of secure, dedicated physical circuits and an embedded SIM OS. This design ensures that iSIMs are just as secure as discrete SIM cards and eSIMs. In addition, iSIMs are more resistant to theft or physical tampering than other SIM types, as iSIMs are much more difficult to identify or remove.

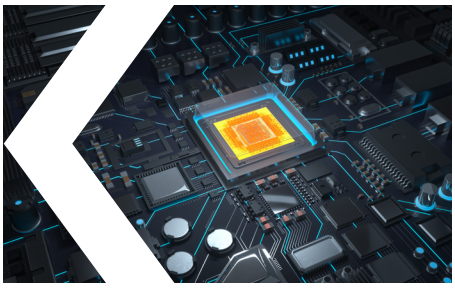
Integrating SIM functionality onto the SoC makes iSIMs far more space-efficient than eSIMs or nano-SIMs, and provides opportunities for significant power savings through optimization of power usage across the SoC. By incorporating an iSIM into their designs, manufacturers can enable cellular connectivity for devices that are too small to incorporate an eSIM or traditional SIM card. iSIMs can also be used to extend the battery life of power-constrained devices.

Like eSIMs, iSIMs are designed for remote provisioning through an RSP service.

Choosing between eSIM and iSIM

There are few, if any, IoT use cases for which the use of a traditional SIM card provides an advantage, so the choice is between an eSIM or an iSIM. Considerations include:

Size: An iSIM does not require a separate chip, so it offers significant advantages over an eSIM for use cases where space is at a premium. For the smallest devices, an iSIM might be the only option to provide cellular connectivity.



Power consumption: Because an iSIM is part of the SoC, designers can optimize iSIM power usage as part of the overall power management across the chip. An eSIM is a discrete component, so there is less scope for making power savings.

Design longevity: eSIM and iSIM behavior and functionality is standardized according to global specifications, so any design that incorporates an eSIM

should remain compatible in the future. However, designs that incorporate an iSIM offer the greatest scope for future innovation.

Product differentiation: For module designers, integrating an iSIM is a way to set their product apart from competitors. After an iSIM design has been created, it can be reused in other SoCs, giving device manufacturers more options when exploring potential markets.

Manufacturing efficiency: For device manufacturers, including a SoC with an iSIM rather than a separate eSIM reduces the number of components in the supply chain and simplifies the assembly process.

Supplier choice: Although more iSIM designs are being brought to the market, device manufacturers currently have a greater choice of eSIM suppliers. However, because many eSIMs use the standardized MFF2 form factor, there is less differentiation between eSIM products than there is between iSIMs.

Certification: eSIM certification has been defined by GSMA as part of their eSIM Group activities. The means by which iSIMs will be certified is currently being defined.

All SIMs need an OS to provide the functionality that is required to authenticate to cellular networks.

SIM operating system

All SIMs need an OS to provide the functionality that is required to authenticate to cellular networks. Typically, the OS consists of a proprietary layer that provides basic functions such as input–output handling, memory management, and cryptographic services. Higher level features, such as support for different cellular network types and the associated authentication algorithms, are provided by various libraries, APIs, and applications that integrate with the OS. The behavior of most of these components is defined by global standards and specifications to ensure interoperability across networks and carriers.

Choosing an OS

When assessing an OS for an eSIM or iSIM, the following criteria should be evaluated:

eUICC support: All OSs that are intended for use with IoT devices that are equipped with eSIMs or iSIMs must support Embedded Universal Integrated Circuit Card (eUICC) for M2M functionality. Since eSIMs and iSIMs are non-removable, changing carriers requires remotely downloading a new

profile. The GSMA SGP.02 specification defines the interfaces and behavior that must be implemented to enable remote profile management. Using an OS that does not support eUICCs will result in a device that only authenticates to a single network for its operational life.

Global standards compliance: To ensure compatibility with as many carriers as possible, the SIM OS should be compliant with the relevant standards from GSMA, ETSI, 3GPP, and the Trusted Connectivity Alliance (TCA), formally the SIMalliance. Numerous standards from these bodies define the behavior of various aspects of the OS, and carriers expect and require this behavior to be demonstrated, through testing and certification, for devices that connect to their networks.

Network support: Clearly, the SIM OS must, at minimum, support the cellular network type that is used by the SoC or device modem. However, it is prudent to specify an OS that supports 2G, 3G, 4G, 5G, LTE-M, NB-IoT, and IMS in order to minimize the changes that are required if the design is updated to use a different modem.

Network authentication: Various authentication methods are in use around the world and different carriers can use different authentication algorithms within those methods. Examples of widely used algorithms for which SIM OS support might be required include COMP128, Milenage, and TUAK.

Toolkits and APIs: To ensure interoperability, carriers use various standardized toolkits and APIs to provide specific commands and functions on the SIM. Carriers will likely require that the SIM OS supports Card Application Toolkit (CAT), USIM Application Toolkit (USAT), Java Card APIs, and GlobalPlatform APIs.

Minimal footprint: The SIM OS should have a compact codebase to minimize the amount of space that is required to store and run the OS on the eSIM or iSIM. This consideration is particularly important for constrained IoT devices such as those that are equipped with iSIMs and are designed for NB-IoT networks.

The chosen SIM OS should be chip hardware agnostic and offer deployment flexibility with a broad support of cellular network attach authentication technologies.

Hardware support: For eSIM implementations, the OS must support the hardware form factor (MFF2 or WLCSP) and the specific chip to be used in the device. An OS that supports a wide variety of chips and vendors enables greater flexibility in the device design.

Secure enclave support: For iSIM implementations, the OS must support the secure enclave to be used in the SoC. Specifying an OS that supports a range of secure enclaves ensures that the design is not reliant on a single vendor.

All M2M eSIMs and iSIMs require a bootstrap profile that enables the device to connect to a network when first powered up.

SIM profiles

Just as cell phone users need a subscription plan with a carrier to access a cellular network, devices with cellular connectivity also require carrier subscriptions. The data that uniquely identifies each subscription plan to the carrier network plus the secret information that is used to authenticate to the network are contained in a profile. The profile also defines carrier-specific configurations of the operating system, SIM applications and device behaviors, such as network interaction requirements and security settings.

All M2M eSIMs and iSIMs must be configured with a bootstrap or initial connectivity profile that enables the device to connect to a network when first powered up. Once the device is connected to the network, the bootstrap profile can be disabled or replaced. Bootstrap profiles can also act as fall-back profiles, which are used when no other installed profile can provide connectivity, to ensure that device connectivity cannot be removed accidentally, rendering it unusable or unmanageable.

A global roaming profile that enables connections to multiple carriers can be used to provide both bootstrap and fall-back connectivity. While roaming profiles provide basic connectivity and can be configured to switch carrier as a device moves between regions, they do not necessarily provide the most cost-effective connectivity solution. Regional profiles offer similar multi-carrier coverage, but only within in a specific geographical region.

When an eSIM or iSIM-enabled device is deployed within a specific country or region, particularly if it is a static device, then a carrier-specific (or operational) profile can be used. Operational profiles typically limit the device to a single network and specify a particular set of tariffs. As with cell phones, operational profiles can be configured to roam across networks, although the costs involved depend on the carriers and the agreements between them.

Choosing a bootstrap profile

The choice of a profile to provide the initial connectivity for a module or device should take the following parameters into account:

Cost: Typically, operational profiles are the most cost-effective option. However, using an operational profile restricts the module or device to the specific areas where the carrier network provides coverage. Global roaming profiles are generally more expensive, but this extra cost must be balanced

against the savings that can be made when manufacturing and supporting a single product for multiple locales. Regional profiles offer a solution that is intermediate in cost between operational and global roaming profiles. This type of profile could be used in circumstances where, for example, regulatory differences mandate the production of locale-specific product versions.

Coverage: The bootstrap profile must be able to provide connectivity over the entire geographical area within which the module or device could be deployed. This consideration is particularly important for devices that are deployed in remote locations, such as agricultural equipment. In such circumstances, a global roaming or regional profile with multi-carrier coverage should be considered.

Flexibility: Specifying a multi-carrier bootstrap profile allows the same product to support diverse use cases. For example, a CCTV camera might be deployed in a city center, where cellular network coverage is high and available from several carriers. However, the same camera could also be installed at, for instance, a rural railway crossing where coverage is only available from a single carrier. Using a profile with flexible connectivity options can increase the range of applications for a module or device.

When a SIM is created, it must be personalized, that is, given a unique identity and loaded with the sensitive data that is used to authenticate to the carrier network.

SIM personalization

When a SIM is created, it must be given a unique identity and loaded with the sensitive data that is used to authenticate to the carrier network. This process is known as personalization. Traditionally, SIM card manufacturers were responsible for personalization, taking input data from carriers, processing the data, and loading it onto the SIMs as part of the card production process.

For eSIMs and iSIMs, the personalization process is divided between a data generator and an eUICC manufacturer (EUM). The organization that is responsible for fabricating the eSIM chips or iSIM-enabled SoCs can act as the EUM, or a separate personalization provider can be engaged. In this model, the carrier that is providing the bootstrap connectivity for the SoC or device sends SIM profile specific data and parameters to the data generator. The data generator creates individualized SIM profiles for loading onto each eSIM or iSIM, and sends the data to the EUM. The eSIMs or iSIMs are personalized by the EUM, who then provides the personalized eSIM chips or iSIM-enabled SoCs to the device manufacturer.

The EUM sends details of the chips or SoCs onto which each SIM profile was personalized back to the data generator. Likewise, the device manufacturer provides identity information and specifications for the devices into which those chips or SoCs were installed. The data generator is responsible for reconciling all this data and sending the necessary information to various platforms.

The bootstrap carrier receives from the data generator details of any chips or SoCs that were not personalized due to manufacturing faults, so that the unused profile data can be purged. The data generator may also be responsible for making the SIM data available for loading onto the RSP platforms that will be used to administrate the eSIMs or iSIMs, as well as any device data needed by the connectivity management orchestration system.

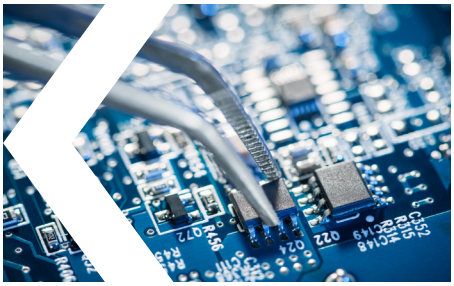
Choosing a personalization partner

Module designers and device manufacturers should consider the following aspects when selecting partners to personalize their SoCs or to provide personalized eSIM chips:

Existing relationships: Data generators that have existing business relationships with multiple carriers and SIM personalization facilities can remove complexity for module and device designers by coordinating the personalization process.

GSMA accreditation: Carriers require that both the data generation process and the personalization of this data onto eSIMs or iSIMs are carried out in GSMA-accredited facilities. Module and device designers must ensure that their personalization partner has the appropriate certification.

RSP and connectivity platforms: To enable device owners to manage device connectivity, data about each device and its eSIM or iSIM must be uploaded to an RSP platform and, optionally, a connectivity management provider. A data generator that operates such platforms can handle this requirement on behalf of module and device designers.



Remote SIM provisioning

When an eSIM is embedded in the device or an iSIM is integrated into the SoC, it cannot be removed and replaced to change settings or switch carriers. To address this limitation, GSMA developed standard structures and processes that enable eSIMs and iSIMs to be updated remotely. The GSMA SGP.02 specification defines remote SIM provisioning methods, the architectures that are required on eSIMs and iSIMs, and the capabilities that must be provided

by RSP solutions. This standard is specifically designed to address use cases for M2M (IoT) devices. A further variant of this specification is being developed to address low power, constrained IoT devices. A separate specification (GSMA SGP.22), which is not discussed here, has been developed for consumer applications, such as phones, tablets, and laptops.

M2M RSP allows carriers to establish secure communication channels to devices and switch the active profiles on those devices.

Essentially, M2M RSP allows carriers or their approved partners to establish secure communication channels to devices in the field and add new profiles or switch the active profile. Device owners must work with a carrier or connectivity management provider to change the profiles on their devices.

Access to devices by carriers is restricted to managing the profiles that they own on the SIM. They cannot access any other software or data on the device.

All devices must contain a designated fall-back profile that can be used in the absence of an alternative, ensuring that a device cannot be left without connectivity and therefore unusable. This approach ensures that carrier networks are protected from unauthorized access, while giving device owners full control over their equipment and any data it generates.

RSP allows module and device designers to build a single product with initial connectivity anywhere that has cellular network coverage.

RSP, along with eSIMs and iSIMs, allows module and device designers to build and supply a single product with a bootstrap profile that enables connectivity anywhere with cellular network coverage. When deploying their eSIM or iSIM-enabled devices, enterprises can engage with local carriers, who can then update the devices with the appropriate profiles using RSP.

Module and device designers can simplify their product lines by not having to produce locale-specific versions, allowing them to manufacture once and ship anywhere. Device owners get the ability to deploy large numbers of devices across multiple networks and the flexibility to select and change carriers and thus service plans.

To enable RSP for their products, module and device manufacturers must arrange the upload of information about the eSIM or iSIM to an RSP platform. This data is known as the eUICC Information Set (EIS). It contains details such as a globally unique identifier and cryptographic values that are used when establishing a secure channel to the eSIM or iSIM. GSMA-compliant RSP solutions provide an API endpoint to receive EIS data, allowing the SIM manufacturers to integrate data transfer with the production process.

For more information about RSP, see:

❮ How Remote SIM Provisioning Works

Choosing an RSP partner

The following measures should be assessed when comparing RSP platform providers:

GSMA accredited solution: All solutions are required to obtain certification from GSMA in order to be able to participate in the RSP ecosystem.

GSMA accredited solution: All solutions are required to obtain certification from GSMA in order to be able to participate in the RSP ecosystem. Platforms and suppliers are audited to ensure that they comply with the relevant standards. Accredited solutions receive GSMA PKI certificates, which are required for authentication between the RSP platform and the SIMs that are being managed. An RSP solution that is not GSMA accredited cannot manage compliant eSIMs and iSIMs, and will not be interoperable with accredited third-party RSP platforms.

Ease of integration: It should be straightforward for module and device manufacturers to integrate their chosen EUM with the RSP solution to automate the registration of EIS data with the platform. Solutions should be flexible and scalable to adjust to the needs of the manufacturer.

Interoperability: The GSMA SGP.02 specification defines methods for transferring data for management of eSIMs and iSIMs between different RSP platforms. Module and device manufacturers should ensure that the selected RSP platform is interoperable with other accredited providers to offer device owners maximum flexibility.

Continuous development: The GSMA RSP specifications are not static and are continually being improved and extended. RSP providers should follow the developments in the specifications, continually improving their products. Ideally, vendors should be active participants in GSMA and other standards bodies, giving them in-depth knowledge of the latest advances.

Connectivity management

Connectivity management platforms typically aggregate services from a range of carriers across multiple locales.

After deployment, device owners and operators will want to switch to profiles that are more closely tailored to their use cases and that are cost-effective for their particular location. Enterprises might need to manage connectivity for a large fleet of devices or, where the fleet extends across different geographies, to manage different profiles on those devices. In such circumstances, it is likely that a device owner will need a connectivity management platform to deploy, track, and maintain their fleet.

Connectivity management platforms typically aggregate services from a range of carriers across multiple locales, enabling device owners to select from existing subscription plans without having to negotiate with each provider. To allow profiles to be delivered to eSIMs and iSIMs, connectivity management platforms must be integrated with an RSP platform. Partnering with a connectivity management provider removes the need for module and device manufacturers to negotiate with various carriers to obtain a profile with the required coverage and data parameters.

Some module manufacturers are partnering with connectivity management providers to offer modules that are pre-connected to a connectivity management solution. Device manufacturers can reduce business complexity and accelerate the time-to-market for their products by incorporating pre-configured connectivity components in their designs.

Integrating a connectivity management platform offers opportunities for module and device manufacturers to provide additional services. For example, continuous monitoring of device data consumption and cost can be combined with automated profile management to minimize operational costs. Devices can be deployed with capabilities that anticipate future developments, such as 5G network rollouts. Being able to take advantage of new services or profiles after deployment not only provides cost benefits, it also extends the deployment lifetime for devices.

Choosing a connectivity management partner

When considering connectivity management platforms and providers with which to partner, the following capabilities should be appraised:

Importance must be placed on connectivity provider selection; one who offers competitive tariffs and capable service for your deployment.

Choice of subscription plans: It is important that the connectivity management provider can give access to a wide range of carriers in every region, including multiple carriers in each locale. A provider that fulfills this requirement should offer a bootstrap profile with global coverage, while also providing device owners with profile options for every country and use case. Module and device manufacturers should verify that connectivity management providers can offer worldwide coverage for the cellular technology that they intend to use, whether 2G, 3G, 4G, 5G, LTE-M, or NB-IoT.

Support for eSIM, iSIM, and RSP: Profiles for traditional SIM cards are not compatible with eSIMs and iSIMs, and need to be redefined. Connectivity management providers must be able to offer profiles that comply with the GSMA SGP.02 specification for M2M devices. In addition, the connectivity management platform must integrate with an RSP provider so that profiles can be swapped remotely when the devices have been deployed.

Extensibility: Connectivity management platforms should make it easy to deploy new devices and to quickly add more devices to existing deployments. Some platforms allow for automation of profile updates based on specific triggers, such as devices crossing geographic boundaries or breaching data usage limits. Platforms that provide APIs offer further opportunities for integration of connectivity functions into external business systems.

Consolidation: The connectivity management provider should deal with all the carriers and present the device owner with a single consolidated account statement. However, it is also important that a full breakdown of usage and charges is available for analysis, reporting and any onward billing.

Integrated device and data management: A platform that also provides device and data management capabilities allows device owners and operators to collect and analyze device data. For example, device performance could be analyzed to predict when maintenance will be required and pre-empt a failure. Device data could also be combined with other business data sources to provide insights into customer behavior, for example.

Compliance with the relevant standards is usually a condition of access to cellular networks.

Standards and certification

To ensure interoperability and common security levels between carriers and infrastructure vendors, cellular standards bodies have created specifications for the design and operation of eSIM and iSIM-enabled devices. It is recommended that module and device designers familiarize themselves with these standards as compliance is usually a condition of access to cellular networks.

Cellular technologies

Cellular modules must comply with the following specifications, depending on the networks to which they are designed to connect.

2G: Since there is no single definition of the technical specifications of 2G, the technology was developed under various proprietary and regional standards. Global System for Mobile Communications (GSM) was standardized by ETSI in a number of specifications that integrated into 3GPP, culminating in 3GPP Release 98. Code Division Multiple Access (CDMA), marketed as cdmaOne, was defined in Interim Standard IS-95 of the Telecommunication Industries Association (TIA). Time Division Multiple Access (TDMA) is defined in IS-136 of the TIA, although it has largely been replaced by CDMA.

3G: The capabilities that are required for a 3G technology are defined by the International Telecommunications Union (ITU) in the IMT 2000 specification.

Two main 3G technologies are currently used in networks globally. 3GPP created Universal Mobile Telecommunications System (UMTS), which evolved into High Speed Packet Access Plus (HSPA+), first introduced in 3GPP release 5. Meanwhile, 3GPP2 developed the competing CDMA2000 specification.

4G: The requirements for 4G are defined in the ITU IMT-Advanced specification. 4G networks worldwide use the 3GPP technology LTE, which achieved 4G compliance with the introduction of LTE Advanced in 3GPP release 8.

5G: The specifications that must be achieved by a 5G technology are set out in ITU IMT-2020, which is not yet complete, although some component documents have been released. In response, 3GPP is developing 5G New Radio (NR) specifications, first added in 3GPP release 15.

LTE-M and NB-IoT: The specifications for LTE-M and NB-IoT were standardized by 3GPP and are intended to coexist and evolve with 5G NR. LTE-M and NB-IoT were first described in 3GPP release 13, with enhancements following in subsequent releases.

eSIMs and iSIMs

As set out in the GSMA SGP.16 v1.1 compliance process, today M2M eSIMs and iSIMs can be certified against the Common Criteria protection profiles BSI-CC-PP-0084 and BSI-CC-PP-0089 to an assurance level of EAL4+. For iSIMs however, the security evaluation requirements are under reveiw so these are subject to future change. The underlying hardware is evaluated against BSI-CC-PP-0084, including the product development and manufacturing processes. GSMA SGP.05 v1.1 introduced BSI-CC-PP-0089 testing to covers the SIM-specific functionality of the complete eSIM or iSIM component, including the SIM OS.

For these security evaluations, assessments must be performed by an accredited security laboratory and certificates are issued on the basis of the evaluation report from them.

For more information about eSIM, iSIM, and RSP standards and certification, see An essential guide to GSMA eSIM certification.

Modules and devices

Before allowing cellular-enabled modules or devices to join their networks, carriers often require that manufacturers certify their products with PTCRB in the US or Global Certification Forum in Europe. Certification typically

involves testing the module or device on a network simulator, then testing on a live network, and finally interoperability testing. When certification is achieved, each carrier will also conduct their own specific verification processes for modules and devices that connect to their networks.

Beyond the cellular certification of a module's capabilities, the IoT industry recognise a need to also insure devices against security vulnerabilities. The protection against rogue actors' malicious intents require a device holistic approach that covers both hardware and firmware and extends beyond just the device itself. The IoT industry is fast converging on the adoption of a set of common security principles that are easily translatable into system requirements and interfaces. These can be used by everyone, from module and device designers to network infrastructure and software vendors, to build products which are easily progressed through an established and trusted security certification programme such as the Platform Security Architecture (PSA). Achieving this kind of certification for your device proves security functions have been tested and provides assurances to deployers, integrators and users that their ecosystem is robust, as well as adding product value.

Protection requires a device holistic approach, covering hardware and firmware, and may extend beyond the device itself.

SIM personalization

Both vendors that generate individualized data for eSIM and iSIMs, and organizations that personalize the data onto the SIMs must be accredited under the GSMA Security Accreditation Scheme for UICC Production (SAS-UP).

Operational sites are audited against the requirements of the GSMA FS.04 and GSMA FS.17 standards to ensure that sensitive data is handled appropriately. The audits assess physical security, network security, personnel and organization, data management, and production processes. All accredited sites must be re audited every two years to retain their SAS-UP certification.

eSIM and iSIM profiles must comply with the Trusted Connectivity Alliance's (TCA), formally known as the SIMalliance, eUICC Profile Package: Interoperable Format Technical Specification. This specification defines a standard format that must be used to ensure that profiles are interoperable across all eSIMs and iSIMs, and are compatible with the RSP requirements.

Remote SIM provisioning

All M2M RSP platforms that operate in the GSMA ecosystem must present a GSMA digital certificate when authenticating to eSIMs and iSIMs, and to other RSP platforms. Certificates are only issued to providers who have been accredited according to the GSMA Security Accreditation Scheme for Subscription Management (SAS-SM), in accordance with in the GSMA SGP.16 compliance process.

Each data center that houses an RSP platform instance must be audited against the GSMA FS.08 and GSMA FS.17 requirements. The physical security, network security, personnel and organization, data management, and operational processes at the site are all assessed. In addition, the design and implementation of the solution itself is validated against the GSMA SGP.11 specification. Certificates for accredited data centers expire after two years and each site must be re audited to regain SAS-SM certification.

Implementing a project

After studying the market and identifying opportunities and areas for product differentiation, manufacturers should have a list of requirements and constraints for their design. These considerations will likely include the required time to market, the expected product life span, and the estimated design and production costs. Module designers will also have power, performance, and area requirements for the SoC.

At this stage, a high-level design proposal can be drawn up and evaluated against the various criteria. Device designers should identify the type of eSIM or iSIM module that they intend to use, as this has an impact on the testing and certification that will be required. For example, certified modules, for which the manufacturer has conducted compliance testing and carrier certification, can reduce the amount of testing that is required for the final product.

When the project has been evaluated and approved for development, the next stage in the process is to prepare and test a proof of concept. Testing of all elements is critical to avoid post-production product issues and for the success of the project. For example:

End-to-end testing is critical to avoid post-production product issues and for a successful project.

Profile development: First, a business relationship must be agreed with a carrier. When this agreement is in place, the bootstrap profile must be developed and integrated with the SIM operating system. The SIM OS might also need to be ported to and tested on the eSIM or iSIM.

SIM personalization: The process for generating, transferring, and personalizing data onto individual SIMs must be validated to ensure that it is secure and can be scaled to production.

RSP platform: The process for generating and uploading EIS data to the RSP platform, that will manage the eUICCs within the devices when

they are deployed, must be tested. Carriers must ensure that operational profiles can be uploaded to and managed through the RSP platform.

Network compatibility: The device must be tested to ensure that it is compatible with the carrier networks to which it will connect. Profile management on the device using the RSP platform should also be tested to ensure that operational profiles can be added and removed.

After testing and validation is complete, the product can move into production. Device manufacturers should allow between 8 and 15 weeks for a SIM module order to be fulfilled, although repeat orders will be quicker. Around 1–2 weeks are required for SIM personalization.

Kigen