End-to-End IoT Connectivity with Embedded SIM

A Kaleido Intelligence Whitepaper

sponsored by

Telit

June 2022

Contents

Executive Summary

Legacy SIM solutions (plug-in SIMs, single profile MFF2 SIMs) raise significant challenges in terms of IoT connectivity longevity, commercial risk and customer flexibility. Any requirement to change connectivity provider during the device lifecycle may result in large, unforeseen cost overheads to physically change SIM cards and arrange new commercial terms.

Many cellular IoT devices roam on visited networks for long periods of time in a practice referred to as permanent roaming. Both industry regulators and mobile network operators are increasingly taking a hostile stance towards permanent roaming, increasing the risk of unwanted physical SIM swaps and associated costs.

Embedded SIMs, in the form of eSIM and iSIM, offer long-term solutions to issues raised by legacy SIM solutions. These SIMs are remotely programmable over-the-air, and allow customers to remotely change network operator profile and localise the connection, if regulatory concerns or commercial terms for roaming become unfavourable.

Multi-IMSI functions in a similar manner as eSIM network operator profile switching, allowing roaming connectivity partners to be changed over-the-air and allowing the connection to be localised in some instances. Built on top of eSIM, multi-IMSI capability mitigates many of the technical and legal pain points associated with the current eSIM specification.

Choosing the right provider to support the end-to-end lifecycle of a device at low risk is essential considering the lifespan of connected IoT devices often spans over a decade. Lock-in effects, commercial risk, and support for connectivity and device issues must be considered if a large-scale project is to be successful.

Market Background: Cellular IoT Connectivity Challenges

Since 1991, cellular connectivity has been facilitated by the now ubiquitous SIM card. While the SIM card provides a reliable, secure method for authenticating devices on the network, its original design was based on a removable smart card form factor which required users to purchase and insert new cards if they wished to change connectivity provider. This is because traditional SIM cards only store network profile access credentials for a single operator on the card. By and large, this business model continues today, although alternative solutions are now rapidly gaining traction.

In the consumer market, this type of model does not present a significant level of disruption, given the well-established retail presence of mobile operators and the fact that most consumers are only concerned with managing connectivity of a single device. The situation is rather different in the IoT world however, as device fleets managed by a single entity can frequently number in the tens, or hundreds of thousands. **Due to the length of time that IoT devices are in the field, there are often good reasons to wish to change connectivity provider during the lifecycle: commercial terms may become unfavourable, the regulatory environment may change, performance or support may be lacking, for example.**

As such, the idea of physically changing SIM cards in IoT devices across large device fleets raises the potential for enormous unwanted business expense due to truck roll and servicing costs.

Physical , single-profile SIM cards can lead to significant business costs if the connectivity provider needs to be changed

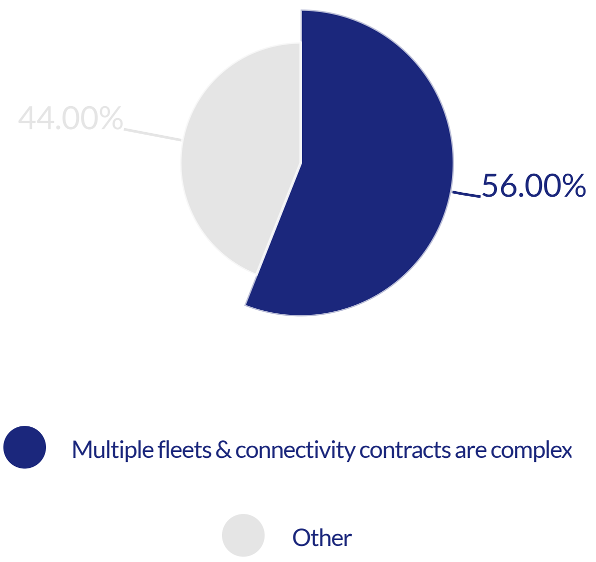
These costs are exacerbated when devices are in remote, hard-to-reach areas. Given the typical small, incremental margins that are offered by each individual IoT device, the costs associated with changing connectivity provider through physical SIM swaps often mean an effective lock-in with the provider, as it is simply not economically feasible to move to a preferred operator.

Moreover, because IoT devices may have certain requirements in terms of durability; the ability to resist temperature extremes, dust, or the need to guarantee read and write operations for several years; SIM cards - which are by specification only consumer grade - are not always a desirable option. In response to this, the MFF2 form factor was developed. MFF2 represents an embedded SIM solution, where the SIM is soldered to the module board during manufacturing (making it non-removable, but therefore more secure than a removable card), in addition to having qualities such as temperature resistance and higher read/write cycle capabilities. **The fact that MFF2 SIMs are soldered means that IoT customers faced even greater expenses should they wish to change connectivity provider when only a single network profile is stored on the card.**

The traditional business model behind cellular connectivity has posed additional challenges to the market. While the consumer retail model is almost entirely focused on direct sales through domestic channels, the IoT ecosystem is rather more fragmented.

In many instances, end-customers are forced to insert SIM cards into thousands of shipped devices, while in others, colour-coded SIM cards may be used according to the country or region that the device is expected to be shipped to and operated in. Naturally, this creates many operational headaches and unnecessary cost overheads in deploying anything over a very small number of devices, not to mention the fact that deployment under this type of model would require several contracts with different connectivity providers to support operations in each country. **In a recent Kaleido Intelligence survey responded to by 759 enterprises, the need to engage with multiple connectivity providers for IoT was viewed as a major challenge by 56% of respondents.**

Survey response to: What do you perceive to be the main challenges where cellular IoT connectivity is concerned?



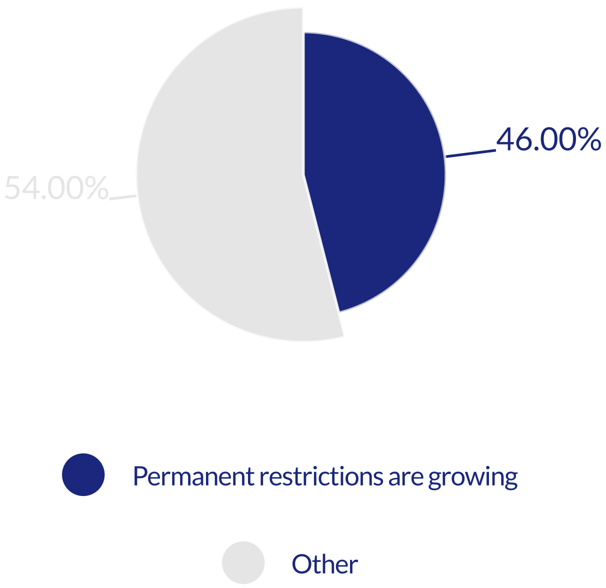
More recently, one of the answers to this challenge has been the concept of the global roaming SIM, where a single connectivity provider with a large global footprint is relied upon to enable connectivity through roaming agreements wherever devices are shipped to. Nevertheless, this model is dependent on the provider of the global roaming SIM having secured favourable commercial rates for whichever country the device operates in, in addition to having the capability to offer consistent performance levels and service support on the international stage.

Although this is now beginning to change, roaming agreements have been developed on the basis of predictable patterns associated with consumer and business travel. Most IoT devices are static in nature, and can vary considerably in the types of data that they transmit across the network. This means that traffic consumption patterns are no longer predictable for any operator accepting IoT roaming connections, while usage in any given country is likely to exceed the short timeframes associated with tourism and business travel, leading to the concept of 'permanent roaming.'

Today, **permanent roaming is a topic of considerable concern among IoT customers and connectivity service providers.** Across the globe, regulators are examining the impact of permanently roaming IoT connections and, in some cases, taking direct action. For example, Brazil, Turkey, and China have regulatory measures in place that prevent permanent roaming. The perceived potential impacts on network performance and the commercial mismatch of supporting IoT connectivity for inbound roaming rather than via retail contracts (domestic connectivity sales) means that many

MNOs, such as in the US, Australia and Canada, means that additional pushback against permanent roaming is increasing from network operators. **In Kaleido's survey, 46% of cellular IoT adopters raised significant concerns over permanent roaming.**

Survey response to: What do you perceive to be the main challenges where cellular IoT connectivity is concerned?



Ultimately, traditional approaches to cellular IoT connectivity have given rise to several compromises that mean scaling IoT volume has been unnecessarily constrained:

- Single operator profile removable or soldered SIM cards effectively lock customers into a commercial relationship with the connectivity provider whose network access credentials are stored on the SIM card. Cost overheads associated with physically changing SIM cards can far outweigh the benefits that are afforded by IoT data connectivity.
- Regulatory authorities as well as MNOs are actively taking increasingly hostile stances towards roaming IoT devices that remain in the visited mobile network for longer than 90 consecutive days; a practice known as permanent roaming. Due to the longevity of IoT projects, which can span several years or even decades, the prospect of regulatory or MNO action against permanent roaming gives rise to inherent risk for connectivity availability.
- Where permanent roaming is prohibited or where roaming is undesirable, local connectivity solutions must be procured instead. Typically, this has involved the need for multiple commercial connectivity relationships and software integrations with each provider to manage internationally distributed device fleets. This model also causes challenges in terms of the logistics of ensuring correctly provisioned SIM cards are present in devices themselves.

> ***Legacy approaches to cellular IoT connectivity have disrupted the ecosystem’s ability to scale in addition to raising concerns over future-proofing, flexibility and performance.***

The Embedded SIM: Opportunity Analysis

The industry has recognised the challenges associated with single-profile physical or soldered SIM cards and has since developed alternative solutions in the form of the GSMA's embedded SIM (eSIM) specification and integrated SIM (iSIM). In contrast to traditional MFF2 solutions, eSIM refers to the secure framework developed to allow SIM operator credentials to be downloaded, activated or deleted over-the-air (OTA) without having to physically change any hardware, rather than the form factor itself. Indeed, eSIM can take any SIM form-factor. iSIM on the other hand is a SIM-on-chip solution where the SIM is integrated with the SoC, obviating the need for any additional SIM hardware.

eSIM: programmable OTA & capable of switching network profiles. Delivered in any form factor.

iSIM: same capabilities as eSIM, delivered as a SoC-integrated form factor, saving cost and space.

Today, while many iSIMs on the market are programmable OTA in similar fashion to eSIM, they are not yet certified as fully compliant with GSMA eSIM requirements in terms of chip security. Nevertheless, several chipset suppliers expect to release security-compliant silicon over the coming 18-24 months and, as a result, GSMA-compliant iSIM should be viewed as an alternative eSIM form factor offering the same flexibility, albeit with a lower bill-of-materials in addition to space and power consumption savings.

eSIM and iSIM represent a transformative step forward in the structure of the connectivity market for cellular IoT. Where operator lock-in was effectively guaranteed for the reasons described in the earlier section, the software architecture designed as part of the eSIM specification is explicitly designed to overcome this, by virtue of being able to switch network operator profiles through OTA commands. **Physical SIM swaps are no longer required, leading to the potential for cost overhead reduction. Because any compliant operator profile can be used on the SIM, roaming can be avoided should a local profile be activated, thus avoiding permanent roaming risk. Additionally, local connectivity will likely reduce connectivity costs, as well as offer improved device quality-of-service (QoS) and quality-of-experience (QoE) due to lower latency and, in some cases, improved support.**

Although the programmable capabilities of eSIM and iSIM represent a theoretical connectivity utopia, they remain an imperfect solution when the GSMA OTA network profile switching capability is deployed on its own. In the first instance, many MNOs are only now making their profiles available to connectivity providers on the market and, in most cases, will not share their profiles with other MNOs due to perceived competition. The absence of a 'profile library' available through a single provider means that end-customers are forced to entirely switch connectivity management platforms when activating a new operator profile, which is technically and legally challenging. This process can often take months to achieve, at great expense. IoT MVNOs often have access to several MNO profiles for use on their platform, which reduces this challenge, although no connectivity provider has come close to a library of profiles for every single country market in the world.

Presently, **many of the drawbacks associated with technical and legal challenges associated with eSIM profile switching can be mitigated by coupling eSIM or iSIM technology with alternative solutions.** These come in the form of multi-International Mobile Subscriber Identity (IMSI) capability, whereby on-SIM or network-based algorithms optimise the active IMSI in use on the SIM depending on desired business conditions. In a practical sense, this can work similarly to eSIM profile switching: end-customers may be able to use a locally-issued IMSI to avoid roaming, while modern multi-IMSI implementations allow IMSIs stored on the SIM card to be updated dynamically OTA. This type of switching involves none of the technical and legal barriers associated with eSIM profile switching, and none of the operational expenses associated with eSIM OTA management platform use (whereby OTA commands that are executed are chargeable by the platform manager).

Nonetheless, multi-IMSI does not conform to any industry specification, and is thus considered proprietary. **eSIM and iSIM thus become an important addition to multi-IMSI to ensure that any lock-in effects are avoided.** When necessary, ownership of the connectivity management can be transferred to a new provider using OTA eSIM or iSIM capabilities.

In the legacy SIM environment, contracts are agreed with connectivity providers and SIMs are inserted in the device production facility or after they are shipped to their destination. As we have observed, this comes with significant barriers from an operational standpoint. In the case of eSIMs, a 'bootstrap' model has been developed, whereby an initial, bootstrap profile is loaded in-factory to ensure that when the device is switched on, it can connect to a network in order to select an appropriate profile to use on the eSIM, or to download a new one for use. Due to the nature of iSIM, this process must take place during the production of the SoC itself, and may introduce complications where the provider of the hardware module must outsource connectivity. That said, several module OEMs either resell connectivity through a partner, or are connectivity providers themselves, in order to overcome this in-factory SIM 'personalisation' process challenge.
As we have described above, programmable embedded SIMs can offer significant advantages over legacy SIM solutions. These come in the form of:

- Commercial benefits. Physical SIM swaps are no longer necessary, which can considerably reduce unforeseen costs associated with changing to a new connectivity provider. OTA profile swaps through an IoT MVNO with a library of several eSIM profiles available for use offer the most cost-efficient and seamless route for new connectivity profile associations, with only the cost of OTA command executions chargeable.

- Where OTA profile switching requires changing to a new management platform, costs increase due to required software integrations, legal agreements and business process changes; however, these remain lower than physical SIM swap costs in the case of larger device fleets. The GSMA is currently in the process of introducing a new eSIM specification that will dramatically reduce the technical and legal challenges associated with the latter profile swap example, making eSIM or iSIM a long-term cost-effective solution for all types of device fleets.

- Low risk. eSIM and iSIM dramatically reduce the risks associated with permanent roaming and other regulatory concerns over the lifetime of the device due to OTA capability to switch to a local operator profile. This ensures that devices do not run the risk of being disabled from accessing the mobile network in any given country, often at short notice, and guarantees that customers can safely deploy devices in the field for a decade or more.

- Flexibility. Costs and performance can be optimised through eSIM or iSIM solutions in a manner that is not possible with legacy SIM solutions. Profile selection can be determined at any point in time to leverage favourable commercial rates, or gain local connectivity access to reduce latency. These benefits are augmented if multi-IMSI capability is used alongside eSIM, as similar benefits can be realised without the cost overheads associated with eSIM profile switching.

While these advantages may apply to almost any segment in IoT, from a cost-benefit and longevity perspective, eSIM or iSIM and embedded connectivity can be particularly beneficial to certain market verticals. Examples of these are examined below.

Telematics

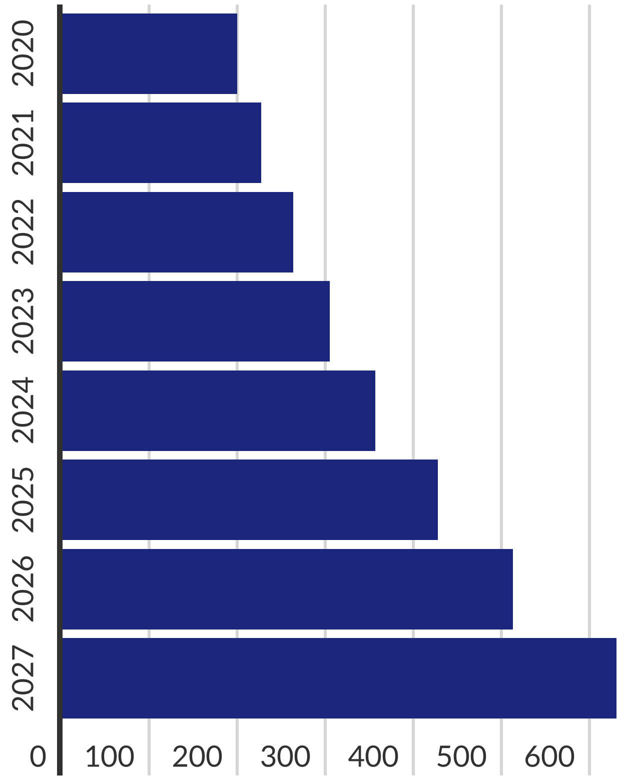
Vehicle telematics solutions have been developed in response to fleet owner demands for vehicle tracking, maintenance and diagnostics information, safety solutions, shared mobility services and insurance services, among others. OEMs supplying telematics solutions to customers frequently sell products on a regional or global basis, and demand that the end-user QoE is consistent no matter where the unit is delivered.

- In the case of combustion engine or electric vehicle (EV) deployments, the expected lifetime of operation for the vehicle and its associated telematics capabilities will run, on average, between 10 and 15 years before the vehicle is retired. Therefore, connectivity must be guaranteed for the entire lifecycle of the telematics solution.

- Meanwhile, road vibrations, temperature extremes and security requirements frequently mean that consumer grade plug-in SIM solutions will not be feasible from a durability perspective.

- Micromobility deployments, involving devices such as electric micro scooters for example, are typically space constrained, making the legacy physical SIM and associated SIM tray a non-optimal design solution.

Cellular IoT Telematics Connections in Millions, 2020-2027



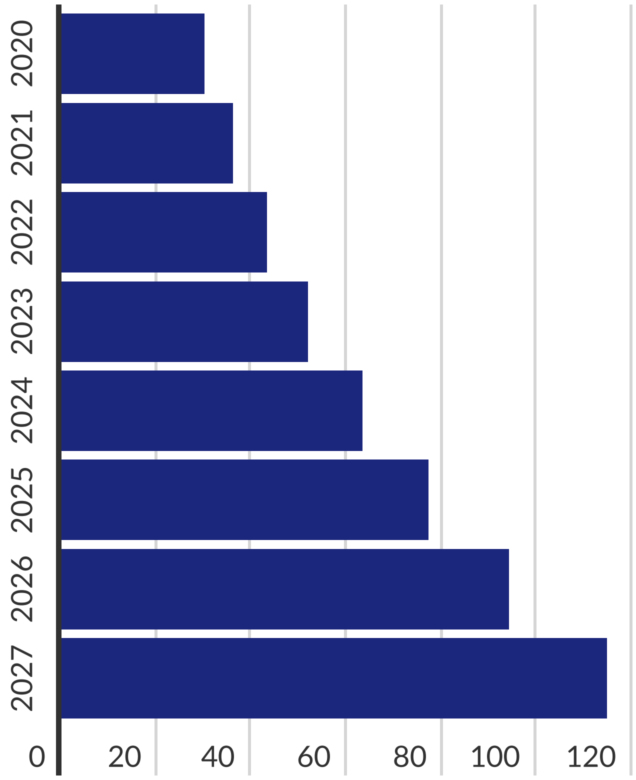
Source: Kaleido Intelligence

Healthcare

A range of use cases apply to the connected healthcare sector, which has been boosted by the onset of the COVID-19 pandemic. Digitisation efforts are accelerating in the sector to enable use cases such as remote patient monitoring, tracking of medical equipment and staff within hospitals and care facilities, connected sanitation assets, connected pacemakers in addition to pop up care facilities and telehealth videoconferencing solutions.

- Body-worn devices to monitor patients are typically space-constrained and sometimes battery-powered, making the iSIM's small form factor and lower power draw an ideal solution for connectivity.
- End-to-end security is paramount in this sector, given the sensitivity of data involved. Embedded SIMs offer a tamper-proof solution to ensuring that devices are not misused, while on-SIM applets such as IoT SAFE can be leveraged to mutually authenticate device and connected cloud services to guarantee the integrity and confidentiality of data exchanges.
- Connectivity reliability is essential for healthcare applications in order to prevent any unforeseen incidents. This means that the connectivity solution must be as flexible as possible to ensure that performance meets requirements as needed, and that uptime is maximised throughout the device lifecycle.

Cellular IoT Healthcare Connections in Millions, 2020-2027



Source: Kaleido Intelligence

EV Charging

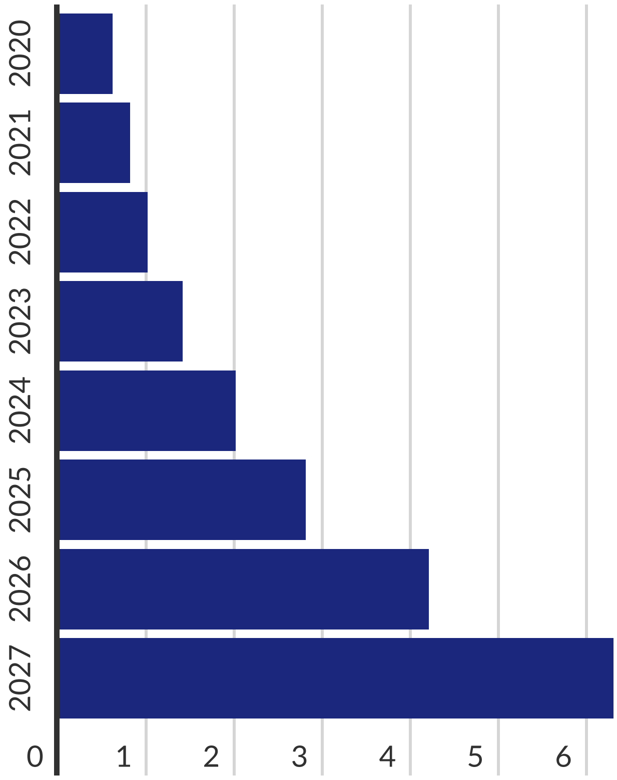
With nearly all automotive OEMs now having developed a future roadmap based on Electric Vehicle (EV) powertrains, infrastructure to support vehicle charging is essential. This infrastructure must be smart from the ground up, by ensuring that appropriate billing is applied, that maintenance teams are alerted in timely fashion when a unit requires servicing, and for ensuring that new services such as dynamic pricing models and smart charging algorithms based on real-time energy grid loads can be introduced in future. The expense of rolling out this type of infrastructure at high volume means that units must be software upgradeable using secure connectivity and platforms to meet future demand requirements.

- Cellular technology is undoubtedly the most reliable connectivity solution for these types of devices, given the wireless capability and flexibility to meet various bandwidth needs. Many EV charging infrastructure suppliers ship units across an international footprint, and thus require minimal complexity where dealing with their connectivity is concerned. This means that a provider must be capable of comprehensively addressing international connectivity needs.

- Charging stations are likely to be in the field for at least 10 years or more. They must therefore not be at risk of permanent roaming restrictions, while the changing nature of the EV charging ecosystem means that units must be capable of being upgraded from a firmware and application perspective throughout the lifecycle.

- The fact that these units are typically placed in publicly accessible locations means that they must be as secure as possible. Here, embedded SIM solutions offer tamper-proofing to avoid device misuse.

Cellular IoT EV Charging Station Connections in Millions, 2020-2027



Source: Kaleido Intelligence

Best Practices & Strategic Recommendations

While this whitepaper has demonstrated how programmable embedded SIM solutions can offer commercial and performance flexibility, high security in addition to guarantees against commercial or regulatory risk, the ecosystem continues to experience challenges.

From a hardware perspective, eSIM and iSIM are not simply plug-and-play solutions. These must be tested with other connectivity components, such as the modem, to ensure interoperability, while additionally ensuring that OTA commands are correctly executed across a range of different mobile networks. This is not a simple process, and remains a significant burden on the industry. While iSIM may be a preferred form factor in many cases due to materials cost savings, device space savings and a lower power draw, the more complex nature of SIM personalisation, which must be delivered at the chip production stage, will require that iSIM remote management platform vendors maintain strong relationships with accredited chipset providers to ensure a high level of security.

By selecting cellular modules from a supplier that has pre-integrated and tested the hardware, customers can avoid the pain points associated with embedded SIM testing and configuration. In most cases, these suppliers will have tested units to ensure compatibility across a large number of mobile networks, ensuring that global deployments do not run into problems wherever they might be shipped to.

As discussed earlier, the OTA profile switching capabilities of GSMA-compliant eSIM and iSIM solutions come at a cost to the end-user. Each OTA command typically incurs a charge of several tens of cents, which means that swapping a device fleet entirely to a new connectivity provider can e a costly affair. These costs are increased if the eSIM or iSIM remote management platform instance of the connectivity provider is not integrated with the newly selected connectivity provider's own eSIM or iSIM remote subscription management platform and will thus require integrations and business process changes that can take several months and thousands of dollars to complete. The GSMA's forthcoming IoT specification for eSIM and iSIM is expected to be completed at the end of 2022, with compliant solutions on the market during the following year or 2024. This will dramatically reduce the cost burden associated with remote subscription management platform changes, as the new architecture is not reliant on integrations between two instances. Moreover, it is likely that new cost structures for OTA command execution will emerge, away from ad-hoc transactional charging, and possibly towards bundled or subscription models that will enable long-term cost projections.

Relatively few connectivity providers on the market have undergone the necessary investment to ensure that eSIM or iSIM profiles beyond their own can be used over their connectivity management platform. Selecting a partner that not only owns their own eSIM or iSIM remote subscription management platform instance is critical here, in addition to gaining assurances that the partner can deliver local connectivity in countries where roaming is challenging or high performance is required; either through eSIM profile availability or multi-IMSI capability; in order to reduce the total cost of ownership of the solution.

Support for IoT connectivity is critical in all cases, and without necessary software integrations in place between connectivity supplier partners, there is a risk that device visibility is lost, or that poor support is offered by one of the partners. This is particularly impactful in roaming scenarios, where inbound roaming connectivity partners may view the roaming devices as a lower priority compared to their domestic connections. Additionally, issues can and do occur with devices themselves that may result in a loss of data transmit uptime or loss of data quality. Here, device expertise will be required in order to gain swift resolution to any outstanding problems and ensure that functionality is restored.

Many connectivity providers either do not have a mobile core network dedicated to IoT connectivity, or simply resell others' connectivity agreements. In both cases, support levels will be diminished due to a lower level of optimisation capability, or poor visibility over the device fleet when these are in roaming scenarios. Selecting an innovative connectivity partner that has a dedicated IoT core network integrated with several other operator partners will ensure a high level of international connectivity support. Additionally, in a best-case scenario, the connectivity provider will have in-house device expertise, which will help streamline device issue resolution processes, and maximise the time that devices remain online throughout their lifecycle.

Review: Critical Vendor Credentials

Telit has a long history as a leading cellular module vendor, and has the additional capability of providing global IoT connectivity and private network solutions for customers. The fact that it has direct expertise in hardware sales and development has allowed it to leverage several differentiation points that set it apart from other non-MNO connectivity providers. Telit has recently become a full MVNO, launching Telit NExT with support from leading technology providers, to deliver globally distributed core network infrastructure.

Ownership of IoT core network infrastructure allows Telit to have full control over connections under management in domestic as well as roaming scenarios. Core network integrations with partners enable it to offer a superior level of connectivity support to customers, owing to full visibility of device fleet activity and error diagnosis.

The company can boast that it was the first to the market for iSIM approximately 4 years ago, which enables it to deliver cellular module solutions based on the smaller form-factor of the technology combined with a soft-SIM profile. Given the size of its module operations (million of shipments per year), this provides the company with significant reach and scale and will likely see its connectivity offering grow significantly in the coming years. Connectivity is normally offered to its module customers, although Telit module ownership is not mandatory.

Customers benefit from a more streamlined service where issues are concerned, given the company's ability to determine where issues on the SIM, network, and device arise. This aids in reducing the number of touchpoints that customers must pass through to resolve problems.

Telit supports eSIM connectivity, in addition to iSIM , with the company having successfully deployed a viable iSIM offering based on collaboration between Telit R&D and IDEMIA. Presently, multi-IMSI is combined with eUICC technology, to support global coverage and cost optimisation.

By deploying eSIM or iSIM supported with multi-IMSI capability, customers can benefit from the ability to deploy devices via a 'one product, one lifecycle' concept. Permanent roaming restrictions can be avoided due to the flexibility of the solution, while allowing customers to optimise costs and network performance through eSIM profile switching or IMSI switching. Additionally, lock-in effects are avoided through the company's eSIM offering.

About the Authors

Before IoT, There Was Telit. We are a pioneer and leading enabler of global Internet of Things (IoT). We offer products for companies that rely on mission-critical connectivity and enterprise-grade performance. Our secure modules, IoT connectivity plans, and software and platforms enable end-to-end IoT deployments. Our products can be used separately or bundled as an integrated solution to reduce time to market and cost.

Our IoT connectivity services optimize your cost throughout your deployment's life cycle.
We provide:

- Global IoT data plans
- IoT connectivity management tools
- SIMs and embedded SIM
- Value-added services

Not all connectivity solutions are created equal. We offer a robust IoT connectivity management tool and resource collection to get your IoT deployment to market.

For more information, please visit telit.com

Kaleido Intelligence is a specialist consulting and market research firm with a proven track record delivering telecom research at the highest level. Kaleido Intelligence is the only research company addressing mobile roaming in its entirety. Our Mobile Roaming & Connectivity research service covers industry leading market intelligence and publications on Wholesale & Retail Roaming, eSIMs, 5G Roaming, IPX, Private Networks, IoT MVNOs, IoT Roaming and Roaming Analytics & Fraud. Research is led by expert analysts, each with significant experience delivering roaming insights that matter.
For more information on this market study or if you have further requirements, please contact:
info@kaleidointelligence.com

Publication Date: 28th June 2022

©Kaleido Intelligence. Kaleido aims to provide accurate information. The information provided here is designed to enable helpful data and insights on the subjects discussed. References to companies are provided for informational purposes only and Kaleido does not endorse any operator, vendor or service included in this research and market study. While information and content of this publication is believed to be accurate at the date of publication, neither Kaleido Intelligence nor any person engaged or employed by Kaleido Intelligence accepts any liability for any errors, omissions or any loss or damage caused or alleged to be caused directly or indirectly by what is contained in or left out of this publication. This white paper consists of the opinions of Kaleido and should not be construed as statements of fact. It contains forward-looking statements and market forecasts that have been developed based on current information and assumptions. These are subject to market factors such as, not limited to, unforeseen social, political, technological and economic factors beyond the control of Kaleido Intelligence.