UNLOCKING MNO & OEM OPPORTUNITIES WITH THE eSIM IoT SPECIFICATION

A KALEIDO WHITE PAPER SPONSORED BY

IDEMIA

www.idemia.com
www.kaleidointelligence.com

Kaleido Intelligence

IDEMIA

EXECUTIVE SUMMARY

eSIM for IoT use cases has had relatively low traction in the market relative to its potential: only around 30% of global Remote SIM Provisioning investments were directed towards M2M profile support in 2022. Meanwhile, only 31% of cellular IoT adopter enterprises have leveraged eSIM for IoT operations, as of April 2023.

In reaction to market demand, the GSMA has published key documents for the IoT eSIM specification during 2022 and 2023. The specification is designed to considerably reduce the technical burden associated with eSIM support and use across global deployments.

By employing lightweight communications protocol support in addition to the option of using efficiently-sized eSIM profiles (virtual SIM cards) delivered over-the-air, power-constrained devices can be more reliably addressed under the new specification, meaning that eSIM is now appropriate for all device types.

MNOs will be able to use existing investments into Consumer RSP infrastructure to support IoT specification eSIM use cases. Lower technical barriers mean that the path towards monetising eSIM for IoT use cases is less costly and time-consuming.

OEMs will be able to more easily realise a single SKU concept for device deployments globally via enhanced flexibility, and benefit from expanding connectivity coverage as more local connectivity services become available. Risks associated with cellular IoT connectivity are thus lowered.

EXECUTIVE SUMMARY

There is no simple migration path between eSIM's M2M and IoT specifications and no backwards compatibility between the two systems. Solution partners must strive to ensure that operations are made as seamless as possible where profile and subscription management is concerned.

Where device deployments require management of both M2M and IoT specification eSIMs, an orchestration layer capable of seamless management and application of business logic workflows across use cases via a single interface is crucial.

Well over a billion IoT devices will leverage eSIM connectivity by 2028. This level of scale means that Remote SIM Provisioning solutions must be positioned to address both high scale and high security requirements .

eSIM Background: Development, Challenges and the Path to IoT Specification

Introduction

GSMA-compliant eSIMs for IoT devices and applications have been on the market for several years and have helped underpin a vision for long-term flexibility in cellular IoT connectivity. Device lifecycles can span over a decade or more, necessitating a level of certainty regarding connectivity availability. In the meantime, pricing, connectivity performance, regulations, and the relationship with the connectivity provider may undergo changes during that lifecycle. With a significant proportion of IoT SIM cards being difficult to access (embedded/soldered into the device) or located remotely, the physical replacement of SIM cards to modify the connectivity service is costly and unfeasible when dealing with thousands of devices.

The M2M specification for eSIM was designed in response to this challenge, establishing an architecture alongside an interoperable eSIM profile format to provide an industry-standard solution for over-the-air (OTA) programmability for SIM cards. Customers using eSIM in this manner can alter the connectivity profile of the SIM card remotely, should there be a requirement to do so.

The success of eSIM in this context has been mixed. Although it has been successfully deployed in automotive use cases (a sector that played a pivotal role in driving eSIM development), widescale cross-vertical customer adoption has not yet emerged. On the supply side, it is notable that as of the end of 2022, roughly 70% of investments into eSIM Remote SIM Provisioning (RSP) among connectivity customers were directed towards consumer use cases (such as smartphones, tablets and laptops) as opposed to M2M/IoT use cases.

> Remote SIM Provisioning customer demand has been considerably higher for consumer use cases than for IoT, due to complexity in the M2M eSIM specification.

M2M Specification Challenges

The reality of the situation is that the architecture for M2M eSIM management is rather complex. Support for global eSIM connectivity across a diverse set of devices and service providers requires a significant level of technical expertise, time and cost to achieve. Unlike the Consumer specification for eSIM, which depends on a single component (the SM-DP+) for eSIM profile hosting, routing and delivery, the M2M specification relies on:

- The **SM-DP** for profile package generation and delivery.
- The **SM-SR** for communication with the end device, routing information of the finished profile package supplied to the SM-DP, and link to the operator's SMSC (for SMS communications).

One critical challenge here is that for all process flows within the eSIM M2M remote management process to function correctly, integrations between relevant SM-DP and SM-SR components must be established and tested before commands can be executed reliably. Further work is required to ensure that BSS (Business Support Systems) are correctly configured to establish billing processes as eSIM profiles are transferred from one operator to another.

Where OTA profile swaps are desired, but the necessary technical integrations and testing have not been conducted, customers can typically expect a significant cost in addition to several months of lead time before such a project can be fully executed. This in itself is a challenge, but when one considers the scale of the mobile ecosystem, the number of integrations required to establish connections between a large number of operators' RSP systems would take several years and cost a considerable sum of money. In essence, the nature of the architecture has made it difficult to scale eSIM infrastructure to support global operations across many different customers and devices.

> SM-SR and SM-DP infrastructure integrations require considerable time and cost, limiting global, seamless, over-the-air eSIM network switching.

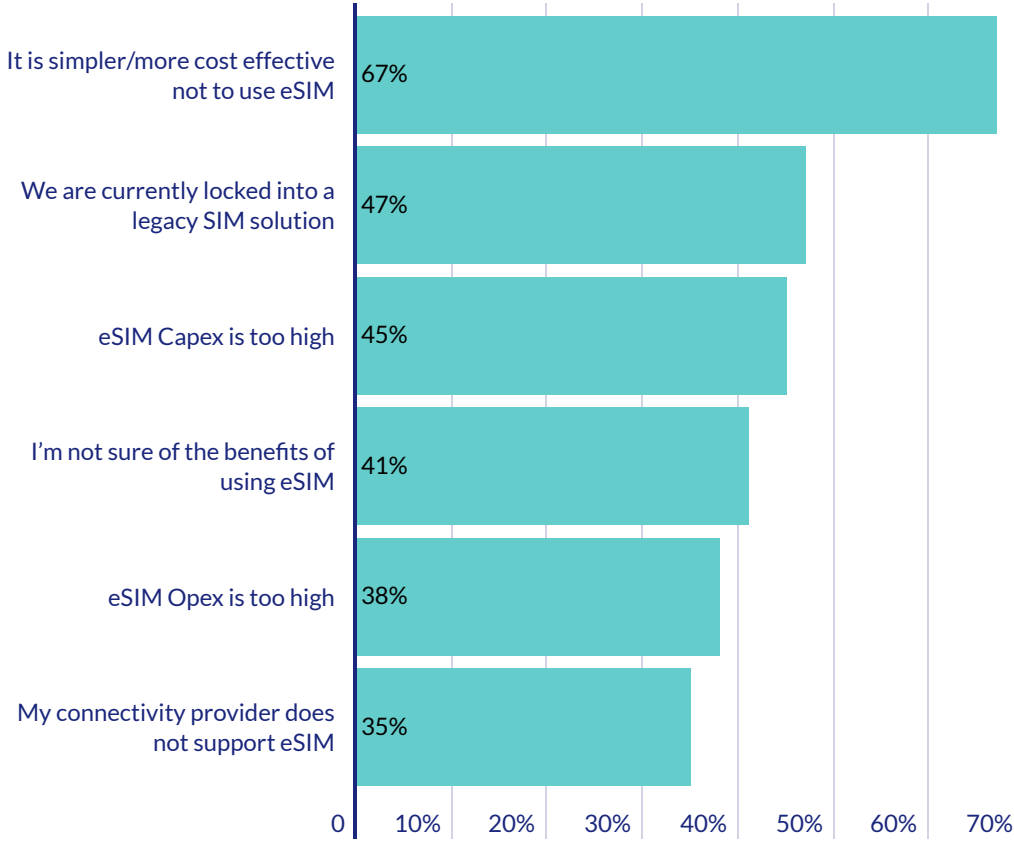
M2M Specification Challenges

IoT devices are often low-cost, relying on LPWAN (Low Power Wide Area Networks) technology such as NB-IoT or LTE-M. Such devices are either power- or battery-constrained and, therefore, require efficient use of available power.

The M2M specification requires that devices support SMS, BIP, TCP/IP or CAT_TP, which are not universally supported by constrained devices: this means that they may simply be unreachable by standard RSP architecture unless custom solutions are put in place. Naturally, this is not conducive to scalability.

Kaleido Intelligence Enterprise IoT Connectivity Survey April 2023:

'Why have you chosen not to use eUICC (eSIM)?'



Source: Kaleido Intelligence. N = 460

The Path to the IoT eSIM Specification

Within the context of the M2M specification, the industry has worked hard to enable the eSIM ecosystem for IoT devices. In the past, many customers experienced complexity in SIM logistics and commercial relationships where they wanted to service multiple markets, including those with regulatory restrictions related to roaming, such as Brazil and Turkey. For the most part, connectivity service providers have found solutions to this, often in the form of eSIM profiles tailored to address challenging markets. Similar approaches have been reflected on the infrastructure side through a growing list of regional and country-specific SAS-accredited data centres in order to enable eSIM at a global level.

Nonetheless, growth in eSIM adoption has been slower than was originally envisioned: despite interoperable eSIM profiles to facilitate connectivity network switching being available on the market since 2016, significant growth in active eSIM use in IoT devices did not occur until 2021. Indeed, it took over 5 years before over 100 million eSIM devices began using M2M RSP infrastructure, despite the overall cellular IoT ecosystem growing by 2 billion connections during the equivalent time period.

The industry has recognised the apparent complexity associated with eSIM when using the M2M specification, in addition to the challenges associated with being able to address the wide variety of devices present in the ecosystem. As a result, during 2022 and 2023, the GSMA has published the architectural and technical documents associated with a new specification – eSIM IoT specification - which aims to address these concerns. This will be examined in the next section.

The eSIM IoT Specification: Enabling Mass-Market eSIM in IoT Devices

Specification Outline

As outlined in the previous section, several technical challenges and associated costs have hindered eSIM scale and vertical adoption for IoT use cases.

To date, the architectural and technical elements of the IoT specification have been published by the GSMA. This means that customers interested in supporting deployments via the new specification can begin testing with relevant RSP service providers. Solution testing criteria, in addition to compliance elements of the specification, are yet to be published, with the industry expecting this to occur during 2024. Nonetheless, pre-compliant solution testing is currently underway, with several proof-of-concepts in place in preparation for market entry.

The IoT specification initiative essentially provides a system that is architecturally and functionally similar to the Consumer specification, albeit with key modifications to allow for the remote management of devices. From a high-level perspective, these changes have been designed to reduce the M2M specification's technical burden required to support eSIM, in addition to changes aimed at addressing IoT devices comprehensively (including constrained devices) rather than a subset of the ecosystem.

One of the critical changes made has been the removal of the SM-SR component, which the eIM (eSIM IoT Remote Manager) has replaced, while the SM-DP component has been replaced by the SM-DP+ used in the Consumer specification. These changes reduce the integration pain points described in the previous section. A further component, the IPA (IoT Profile Assistant), has also been introduced. The functionality of the eIM and the IPA are described below:

- **The eIM** has a dual role. Primarily, it is used as a management agent to instruct the IPA to execute eSIM profile management actions, such as ordering a profile download. For constrained devices, it can also act as a proxy to retrieve profiles from the SM-DP+ and pass to the IPA. The eIM used, as well as the SM-DP+ it connects to, can be changed at any point during the device lifecycle. The eIM has only to pass on the new SM-DP+ address to the IPA for it to connect to the new SM-DP+, directly or indirectly through eIM. An eIM switch is also simply achieved by reconfiguring it in the IPA.
- **The IPA** is used to handle on-device eSIM operations. It can either be deployed on the eSIM (IPAe) or on the device itself (IPAd). This entity is functionally similar to the Local Profile Assistant found on eSIM-enabled smartphones and tablets, albeit optimised for IoT operations. Deployed in the device (IPAd) will allow customers to utilise native device-level information, such as GNSS (Global Navigation Satellite Systems) or signal strength, to automate profile management actions. However, the numerous device types and operating systems available in the ecosystem make this a complex endeavour. The IPAe model will incorporate the IPA functionality on the eSIM itself and, as such, offers the smoothest path towards eSIM remote management capabilities.

Specification Outline

Importantly, the dependency on SMS in the communication process flow has been removed. New protocol support has been introduced in the form of DTLS, CoAP and UDP, while maintaining the capability to communicate via TLS, TCP/IP and HTTP. In this context, protocols such as LwM2M and MQTT can be utilised in device deployments where battery life and processing power are factors for consideration. Alongside the GSMA's specification work, in April 2023, the TCA (Trusted Connectivity Alliance) introduced its 'IoT Minimal Profile' as part of the eUICC Profile Package: Interoperable Format Technical Specification version 3.3. This reduces the size of the eSIM profile by approximately 400 bytes and, when coupled with the IoT eSIM specification architecture, helps ensure that remote management of eSIMs in constrained devices is made as efficient as possible.

Dependency on the SM-SR has been discarded, reducing integration complexity between infrastructure components. The combination of the eIM and IPA replaces it.

The eIM is introduced as an intermediary anchor point, communicating with the IPA and, if required, the SM-DP+. Its configuration towards any IPA or SM-DP+ is flexible at any point during the lifecycle.

The IPA is introduced to handle on-device eSIM operations and supports a flexible model of deployment in the eSIM, or in the device firmware itself. The IPA can be configured to connect to a new eIM or SM-DP+ if and when required.

While it has been pertinent to consider the technical improvements made to the specification, from a customer perspective, it is much more important to consider what this means for the ecosystem. Kaleido notes that 2 customer groups in particular, will benefit as the new specification begins to be commercialised.

Mobile Network Operator Opportunities

Earlier in this whitepaper, we observed how approximately 70% of investments into eSIM RSP solutions have been focused towards the Consumer ecosystem, which is primarily aimed at targeting devices such as smartphones, smartwatches, tablets and laptops, among others. On the one hand, this was to be expected: consumer devices, and smartphones in particular, represent the 'low-hanging fruit' of the overall eSIM ecosystem. The combination of market opportunity, in addition to market forces on the supply and demand side, has helped accelerate eSIM RSP adoption by incumbent MNOs (Mobile Network Operators). Meanwhile, complexity and potentially high customer costs have hampered the market for eSIM in IoT.

One immediate benefit derived from the IoT specification where MNOs are concerned is the fact that existing investments into Consumer RSP solutions, namely the SM-DP+ in addition to existing BSS integrations, can be repurposed as part of efforts to support IoT use cases.

This fundamentally makes the market simpler for MNOs to participate in: IoT profiles can be generated for use on existing SM-DP+ infrastructure, which in turn will increase profile availability and choice for OEMs (Original Equipment Manufacturers) wishing to connect devices across international markets.

> The potential for existing SM-DP+ infrastructure to be reused, in addition to lower technical barriers within the IoT specification allows for simpler market participation.

Mobile Network Operator Opportunities

In essence, the market opportunity will shift in significance away from only MNOs with investments into M2M RSP towards a much more open market where all MNOs with a desire to monetise eSIM profiles can do so if they wish. This increased participation will, in turn, encourage more enterprise customers to leverage eSIM, particularly as the pool of available eSIM profiles on the market increases. This will be driven by 2 critical factors identified in Kaleido's enterprise IoT connectivity survey outreach:

49% of cellular IoT adopters reported a lack of either Consumer or M2M profile support by MNOs

Source: Kaleido Intelligence Enterprise IoT Connectivity Survey April 2023. N = 460

65% of respondents stated restrictions surrounding permanent roaming represent a top challenge for scaling IoT up

Source: Kaleido Intelligence Enterprise IoT Connectivity Survey April 2023. N = 800

It is notable that an increasing number of enterprise IoT customers are aware of and concerned about regulation and commercial challenges related to cellular IoT connectivity. Over the past years, and particularly in the post-COVID-19 era, industry concern has grown over permanent roaming practices within IoT, which has led a number of regulators as well as incumbent MNOs to take steps to prevent permanent roaming at scale. Importantly, the risk of regulatory or commercial barriers preventing permanent roaming in the future is something that cannot easily be mitigated through traditional SIM solutions. eSIM has already been positioned as a solution to this problem, but its value is enhanced when end customers know that the market offers not only a standard mechanism to mitigate risk but also a broad choice of fallback options if the primary connectivity contract is eventually deemed unsuitable.

Market participation in the eSIM ecosystem for IoT use cases is critical in overcoming such perceptions and challenges. The knowledge that systems are in place to efficiently ensure long-term connectivity reliability will help position eSIM as a de facto solution for IoT connectivity, leading to increased adoption and revenue opportunities.

Original Equipment Manufacturer Opportunities

From the perspective of OEMs that require connectivity for their devices, the IoT specification for eSIM represents a significant milestone. This is most pertinent for OEMs that aim to develop towards, or already have a need for, the management of devices across a significant international footprint. Invariably, supporting truly global IoT connectivity requires that contractual and technical relationships are established with several connectivity service providers: the new eSIM specification does not entirely solve this challenge, but where eSIM and RSP are required across that international footprint, the new specification offers key benefits.

Under the M2M specification, the integrations between SM-DP and SM-SR components of the RSP infrastructure quickly become complex and time-consuming to scale up beyond a small number of connectivity service provider partners. Via the new specification, the SM-DP+ becomes the primary component for profile hosting and delivery, with the integration between the service provider's SM-DP+ and the IPA handled through the standard interface, used in Consumer RSP. The IPA can be configured to connect to different SM-DP+ servers during the device lifecycle, the process of connecting to various service providers' RSP infrastructure is now much lower in complexity.

Under the new specification, OEMs will now be afforded a considerably greater level of control and flexibility over operations. On the one hand, **all device types can now be addressed using eSIM, due to the wide variety of communications protocols supported in addition to the ability for the eIM to act as an intermediary for CoAP and TCP communications between the device and the RSP infrastructure. Additionally, the removal of SMS dependency, in addition to the introduction of more lightweight eSIM profiles for constrained devices, means that even NB-IoT devices can be addressed**. These factors are of significant importance, given the long lifecycle of IoT devices, where guarantees in regard to long-term connectivity support are required to ensure the financial viability of IoT projects.

Lower technical burden to connect to a wide number of connectivity service provider partners.

Lightweight protocol and profile support means that power-constrained devices can now be efficiently addressed.

More flexible provisioning process at any point in the device lifecycle helps realise a true single SKU concept.

Original Equipment Manufacturer Opportunities

Meanwhile, a key benefit of the specification is the newly simplified mechanism to enable connectivity provisioning of the eSIM. Manufacturers will no longer have to bind eSIMs to a specific connectivity provider during production due to the fact that the eIM link to an IPA, as well as the link between the IPA and SM-DP+, can be configured or modified at any stage of the device's lifecycle. Under the M2M specification, the 'single SKU for global deployments' concept was introduced for OEMs but was challenging to realise due to the need for SM-SR configuration at the point of production. **According to Kaleido's April 2023 survey of IoT enterprises, 40% of OEMs experience challenges and complexity related to eSIM provisioning at the point of manufacture.** In contrast, the IoT specification has the potential to finally realise the single SKU concept.

As the technical challenges of eSIM integration have significantly diminished, OEMs can now simply establish connections with a broader array of connectivity providers. This allows them to place a more substantial emphasis on defining commercial terms and selecting partners. **As the new specification becomes commercially available, OEMs' options and long-term flexibility regarding eSIM are therefore considerably enhanced.**

> The new specification realises new levels of control and flexibility for OEMs while the business case is shifted from a small subset of IoT devices to all devices.

Best Practices for Consideration

Introduction

The development and forthcoming commercialisation of the IoT specification for eSIM mark a substantial advancement for the market. Technical barriers have been lowered, making market participation more accessible for both service providers and customers. Simultaneously, flexibility in onboarding and long-term SIM management processes has seen significant enhancements. Nonetheless, the new solution does not come without challenges, and adopting the new specification is not simply a question of selecting a relevant partner and executing a go-to-market strategy. This section will aim to identify the key challenges associated with the new specification, bearing in mind the current state of the market and how the ecosystem is positioned.

There is no migration path from the M2M specification to the IoT specification

At the outset, it must be noted that there is no backwards compatibility or clear migration path between M2M and IoT eSIM platforms. The operating system (OS) on the eSIM must be compliant and certified for each type of RSP solution, with differences between Consumer, M2M and IoT OSs. Meanwhile, the architecture of the IoT specification is markedly different compared to the M2M specification. These factors ensure that existing deployments on M2M RSP infrastructure will remain isolated in terms of servers and underlying technical integrations and processes from deployments using the new IoT specification.

Immediate challenges come to mind when considering the fact that many customers have existing deployments on M2M RSP solutions but wish to leverage the IoT specification for new rollouts. Here, complexity may be increased if separate systems and backend integrations have to be configured and as device volumes increase, this management task becomes increasingly complex and costly for the customer.

While solution providers may have the ability to separate between M2M and IoT RSP-enabled eSIMs using tags or other mechanisms, this does not guarantee a seamless experience where management of the eSIMs is concerned. The 'single pane of glass' concept is important here in that the most advanced solutions will offer capabilities to shield end-users from M2M/IoT RSP targeting and workflow complexity. Solutions should be capable of configuring, deploying and updating eSIMs via a unified interface regardless of the specification set they conform to.

Business workflow processes may have pain points

The workflow process is a rather important aspect to consider, given the differences between eSIM specifications configurations that will be applicable to Consumer, M2M and IoT-compliant eSIMs. On the one hand, MNOs may not be aware with which specification the profiles that they make available to customers should conform to. Without this information, incorrect or incompatible profiles may be delivered to customers, resulting in loss of connectivity or unwanted device behaviour. On the other hand, OEMs may have developed specific business logic to execute various remote SIM management commands, depending on aspects such as location, connectivity agreements in place, etc.

How these types of challenges are addressed by any existing orchestration layer will be fundamental in smoothing the transition between M2M and IoT specification deployments. In the same way that it is important to leverage a single pane of glass management concept, leading orchestration layers should be capable of abstracting this complexity away from the end-user. The ability to detect specification conformity, adapt profiles according to specification and adapt workflows based on business logic are some of the main aspects that ultimately enable a more reliable and seamless solution service.

System security and scalability are important considerations

To date, many RSP solution deployments have been deployed via on-premises models that are by nature limited in their total performance capacity. Given the substantial increase expected in both smartphone as well as IoT eSIM connectivity and the pressure (in terms of system load) that this is anticipated to generate, it is important to ensure that the selected RSP solution is future-proofed and capable of delivering availability even during periods of very high demand.

In a similar fashion to how traditional IT systems and solutions have looked towards the cloud to enable elasticity and flexible on-demand capacity, this shift is also needed at the RSP level: where system loads reach hundreds or even thousands of transactions per second to manage eSIM profiles, reliability must be maximised in so far as is possible to ensure that OTA campaign failure rates are kept as low as possible which, in turn, maintains a customer experience level that is expected by the industry. In the IoT ecosystem, reliability is perhaps even more of an important factor, as the very notion of connectivity outage may mean revenue loss or damage to the brand.

One side-effect of cloud migration is, perhaps surprisingly, an improvement in the security of the overall solution. Data centres housing RSP servers are naturally security audited and accredited by the GSMA regardless of whether they are on-premises or cloud-based, which means that at a baseline level, both types of deployment are equally secure from physical and cybersecurity threats. Given the stringent requirements applied by the GSMA in terms of physical and system security for RSP solutions, the primary possible weakness in the context of security is Denial-of-Service (DoS): this is where hyperscale cloud providers that have partnered with RSP solution providers are likely to offer an

System security and scalability are important considerations

enhanced layer of defence: this is simply a natural evolution of years' worth of cloud solution building based on reliability and resilience. In the same vein, the cloud can offer additional reliability which may not be possible through on-premises deployments: geo-redundancy at regional or even local level ensures that, if one system should become unavailable, the geo-redundant solution will be in place to deliver service continuity.

Conclusions

Ensure your RSP partner is capable of addressing disparate eSIM specifications through a single pane of glass.

Bear in mind process workflows, business logic and appropriate profile provisioning for different eSIM specification types requires a suitable orchestration layer.

Ensure that as eSIM demand increases, RSP solution partners are capable of ensuring high availability and security for operations via cloud-based infrastructure deployments.

ABOUT IDEMIA

Since our founding, IDEMIA has been on a mission to unlock the world and make it safer through our cutting-edge identity technologies. Our technology leadership makes us the partner of choice for hundreds of governments and thousands of enterprises in over 180 countries, including some of the biggest and most influential brands in the world.

In applying our unique expertise in biometrics and cryptography, we enable our clients to unlock simpler and safer ways to pay, connect, access, identify, travel and protect public places – at scale and in total security.

At IDEMIA, we are proud to be trusted by 600+ governments, state & federal organizations and 2,300+ enterprise customers across the globe, who count on us to secure billions of essential interactions for payment, connectivity, access control, identity, travel, and public security every year.

ABOUT KALEIDO INTELLIGENCE

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: November 2023