Ovum
TMT intelligence | informa

eSIM Solutions Drive New Opportunities for Global IoT Services

February 2019

Publication Date: February 8, 2019

Author: Alexandra Rehak, Isabel Freire

Summary

In brief

Mobile connectivity is a key element of many Internet of Things (IoT) solution deployments. Enterprises looking to benefit from the IoT need connectivity for devices that move around within cities, within countries, or across borders. IoT use cases requiring mobility – or global "always-on" connected functionality – include connected cars and other types of vehicles, tracking and monitoring of moving assets, and consumer wearables that need to function seamlessly as the wearer travels.

In addition, manufacturers are increasingly interested in delivering smart devices that may be shipped to and activated in many different global markets, for both industrial and consumer use. In some cases, manufacturers or their enterprise customers may themselves wish to act as IoT service providers[1], bundling in connectivity with the devices to establish a more ongoing, service-based relationship with the customers they sell to.

To support these requirements, enterprises and the IoT connectivity providers who serve them must be able to deliver reliable, flexible global connectivity. But delivering a seamless global IoT connectivity solution presents challenges. These include:

- eliminating coverage gaps for mobile IoT devices
- ensuring manufactured IoT devices can be provisioned quickly and easily across multiple geographies
- being able to support multiple connectivity technology options flexibly and securely, to meet the requirements of varying IoT use cases
- delivering the right service at the best price – which may require swapping out one underlying connectivity provider for another
- ensuring security requirements can be fully and reliably supported by the chosen IoT network and solution design

From a technology standpoint, many IoT deployments will require a variety of connectivity options and a level of global coverage that cannot presently be supported by most standalone mobile network operators. Some devices may need to connect to many different networks, depending on coverage and availability in certain geographic regions, requirements for improved indoor or underground coverage, or the need to fill gaps or transfer data using the lowest-cost solution.

Delivering IoT services at the right price is also a key concern for enterprises and IoT service providers, and locking in to a single mobile connectivity provider who is delivering global coverage via roaming agreements may not be the best way to achieve this. Industry alliances for global connectivity

[1] We use the term "enterprise" to refer to an end-user enterprise deploying IoT solutions or manufacturing and distributing connected devices; "IoT service provider" to refer to any entity providing IoT end-to-end solutions including connectivity, whether as an MVNO or using its own network assets; and "mobile network operator" or "operator" to refer to a network connectivity provider (which may also be an IoT service provider).

have sprung up to address these requirements, but may not always be able to support mobile IoT solutions at appropriate cost, with the most suitable technologies, and/or in the right locations. In addition, ensuring the security of IoT connectivity, devices, and data is of paramount concern for enterprises, but not all technologies or solutions for global connectivity provide the same capabilities in this regard.

Solutions such as remotely configurable embedded SIMs (eSIMs[2]) open up new possibilities that allow improved mobility and cost-effectiveness for IoT connectivity, as well as the assurance of tried-and-tested cellular-standard security, for IoT service providers and device manufacturers considering their connectivity options.

A partner that offers eSIMs and can aggregate and manage operator relationships using a single unified IoT platform can ease the way for enterprises looking to develop and deploy smart connected solutions and devices, and for the service providers that support them.

Extending reach by working with an eSIM partner allows IoT service providers to address enterprise demand for a broader IoT footprint, which can allow easy activation of new devices for international markets, and a fast path to scalability for new IoT offerings. Moreover, choosing an eSIM solution allows operators and service providers to offer a smoother customer experience, and to reduce capex and time to market for their own services, and for the IoT end customers they serve.

Key issues explored in this paper

- **Mobile connectivity is a key element of many IoT deployments. Delivering this at global scale seamlessly, flexibly, and securely is an ongoing challenge for enterprises and IoT service providers.**
- **Enterprises and service providers may need a variety of connectivity choices to support different types of mobile IoT devices and solutions, and are looking for solutions that enable this without introducing too much complexity.**
- **Cost and security are key concerns for enterprises looking to roll out IoT deployments, and for manufacturers developing IoT devices. Solutions that offer assurances of delivering best-priced connectivity, along with strong levels of security, are a good fit for many IoT use cases.**
- **Different technology options for IoT device connectivity are available in the market. Among these, mobile connectivity with eSIMs offers a set of capabilities that will be highly attractive to many end-user enterprises looking for the simplest option to support their IoT wide area connectivity requirements.**

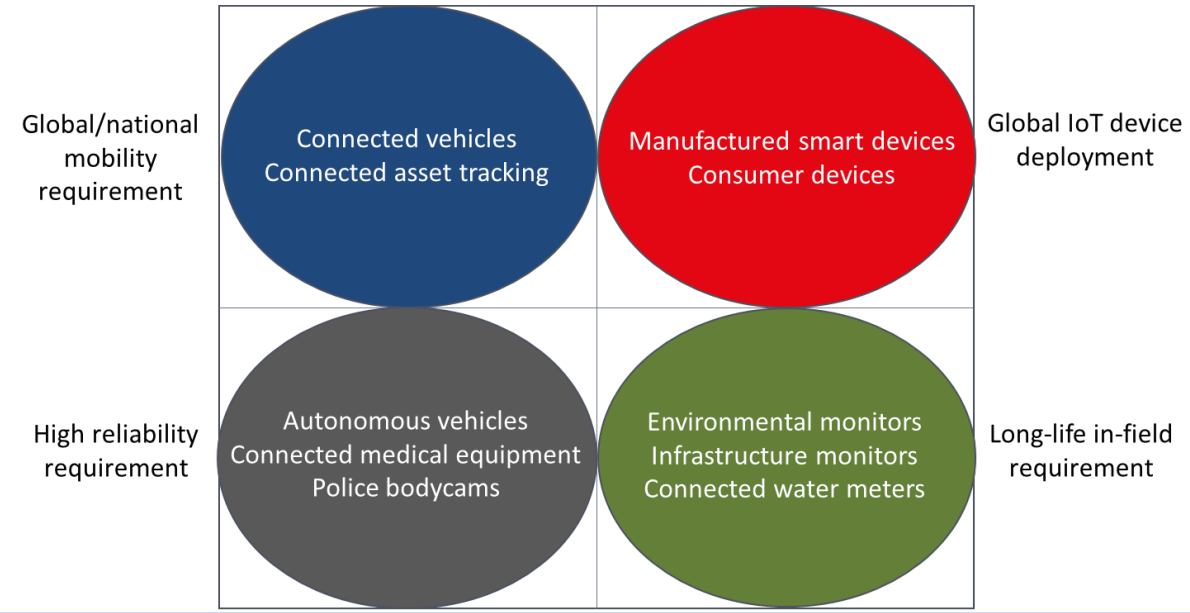
[2] Throughout this paper, the term “eSIM” is used to refer to eSIM/eUICC technology.

Many IoT use cases require seamless, flexible global mobile connectivity

As the IoT evolves, and connected devices and use cases proliferate, more and more organizations are adopting digital services. Meeting end-customer **expectations around service availability and delivery**, and doing so **in a flexible manner**, are key elements for success.

To meet these requirements, operators and service providers must be able to deliver seamless, wide-ranging mobile IoT connectivity. This is a key enabling element for many types of IoT deployments, particularly those requiring cross-border and national mobility, and those requiring global deployment. As highlighted in Figure 1, IoT use cases themselves are highly diverse, and the ways in which they drive demand for mobile IoT connectivity vary as well (note these drivers are not mutually exclusive).

Figure 1: IoT use cases and connectivity requirement drivers



Source: Ovum

Global/national mobility requirement

In the top left circle, Figure 1 shows examples of IoT use cases requiring seamless mobile connectivity services to support **IoT devices that actively move across borders, and nationally across wide areas within countries or even cities**. Transport, fleet management, logistics and supply chain, and the automotive industry all require both national and global mobile connectivity. New use cases are emerging within cities as well – for example, connected bicycles and scooters, mobility services, and public security.

The impact of IoT connectivity dropping out as a device or vehicle is moving can create a poor customer experience. More critically, data may be lost, or latency may be unacceptably high. In some cases, such gaps can have catastrophic impact – for example, if a connected vehicle is temporarily unable to communicate with a cloud-based mapping function, or with a sensor indicating the presence or speed of another vehicle. Connected vehicles, drones, and connected trackers (such as those on shipping containers and packages) all require seamless mobile connectivity to deliver the required

level of service as they move through the environment. IoT data must be collected and analyzed consistently no matter where the connected device goes, in order to enable insights, processes, and actions to be driven effectively.

Global IoT device deployment

A second demand driver for global IoT connectivity is linked to the growing **requirement for "instant-on" IoT connectivity for manufactured devices being shipped worldwide**. Manufacturers across all industries are looking to IoT-enable the goods and components they manufacture, for a multitude of benefits. For the end user, these can include improved and constant data about device status, performance and maintenance requirements, activities, and environment. For the manufacturer itself, this information can provide a valuable source of detail about the device's usage and performance that can feed into future manufacturing processes, and can also be used to enhance the customer relationship. In some cases, the device provider may also wish to become an IoT service provider, offering the customer an ongoing bundled-in service relationship to provide the connectivity, platform, and related applications for the device.

Such requirements are not limited to devices for use in industrial IoT settings. The B2B2C market is also driving demand for broad, reliable mobility for connected IoT devices, to support an active lifestyle. Consumer devices like smart watches, wearable fitness devices, and child and pet trackers are now mainstream. As these markets grow, speeding up time to market becomes increasingly important, and a single connectivity solution that applies across all instances of a particular product regardless of where it is shipped and sold can help achieve this. Further, in many cases, smart device manufacturers are looking to establish an ongoing service relationship with the consumer purchasing the device, requiring them to ensure ongoing provisioning of reliable connectivity as part of this.

But making this type of instant out-of-the-box connectivity and ongoing service relationship work wherever the device is shipped can be a headache for manufacturers, who may not have the resources or interest to manage multiple "localization" efforts for all markets they ship to, or to establish permanent roaming agreements (which are in any case not permitted in some markets).

High reliability requirement for mission-critical devices

A third IoT connectivity demand driver is the need for **full and reliable coverage for IoT devices that are generally stationary or move within a limited area, but that need constant highly reliable connectivity**. Examples include remote or body-worn video cameras for public security monitoring, connected medical equipment (which may move around a hospital), fully autonomous transport, and precision manufacturing-type applications that need computer vision. Supporting high reliability for these mission-critical devices requires absolutely seamless network coverage across all areas of a city or even a building. This may be difficult to achieve through use of a single-operator mobile network, which may have coverage gaps or points of failure.

Long-life "in-the-field" connected devices

Finally, certain types of IoT devices will have a particular connectivity challenge due to their **expected length of time "in the field."** This may range from 8–10 years for devices used for applications ranging from remote monitoring (at the low end), all the way up to embedded SIMs in connected cars, which will be on the road for an average of 10–11 years in most countries. The chance of network

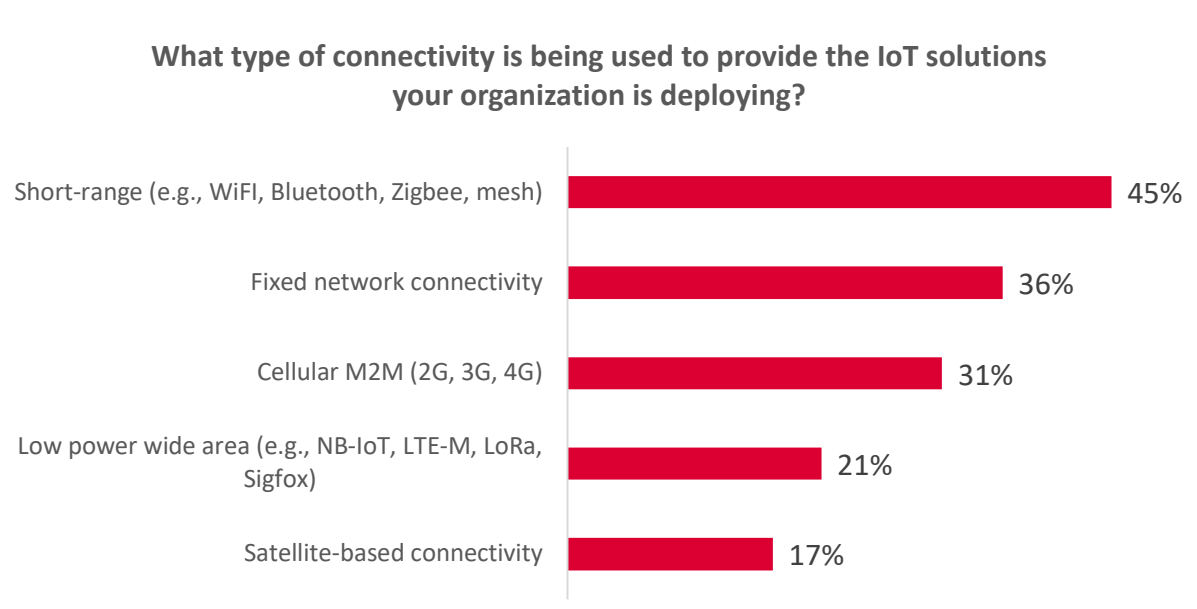
coverage and pricing changing during this extended lifespan is high, and enabling the flexibility for the IoT device to change to a different connectivity provider simply and easily would be a significant advantage.

Enabling multiple connectivity technologies is key to helping enterprises succeed with IoT

Delivering global, reliable connectivity is not the only challenge facing enterprises looking to deploy IoT solutions, and device manufacturers targeting the IoT market. As IoT deployments scale and the variety of IoT applications grows, enterprises are utilizing a wide array of connectivity technology options, both wireless and fixed, to support their IoT initiatives.

Findings from over 1,300 enterprises in 14 countries that responded to Ovum's recent IoT Enterprise Survey (see Figure 2) clearly illustrate this diversity. Enterprises may be deploying IoT using cellular machine to machine (M2M) connectivity (2G, 3G, 4G, and eventually 5G); short-range wireless options such as WiFi, Zigbee, and Bluetooth LE; traditional fixed network connections; low power wide area network technologies (e.g., NB-IoT, LTE-M, Sigfox, and LoRa); and even satellite. All of these technologies are in use for IoT, and many organizations are using several of them at once, or using different varieties in different locations.

Figure 2: Enterprises are using a variety of connectivity technologies for IoT deployments



Source: Ovum IoT Enterprise Survey 2017–18, n=1,343 enterprises already deploying IoT solutions or contracted to do so. Note: For the purpose of the above analysis, NB-IoT and LTE-M are considered part of the low power wide area (LPWA) network technology family; they are also **cellular-based** IoT connectivity technologies, which use licensed spectrum, as opposed to LoRa and Sigfox, which are *not* cellular-based and use unlicensed spectrum.

In an increasingly mobile and interconnected IoT ecosystem, the diversity of connectivity technologies can present a significant challenge for both enterprises and IoT service providers. Supporting multiple

technologies is a key requirement to deliver the best IoT solution for customers, at the most appropriate price point. Flexible mobile connectivity solutions such as eSIMs can offer a simple way to address this, as discussed in more detail below.

Cost and security are also important considerations for enterprise IoT solutions

Ovum's recent survey of enterprises deploying IoT solutions highlights the importance of cost and security as challenges to deploying and scaling up IoT solutions successfully (see Figure 3). To help customers succeed, IoT service providers (including device manufacturers looking to move into services by bundling connectivity with their devices) are seeking ways to access the lowest-cost connectivity for IoT deployments, while still providing an excellent customer experience.

The dynamic and emerging nature of the IoT market means new networks are being deployed at a rapid pace, and pricing strategies may also change rapidly. The flexibility to take advantage of these developments, and to manage that process via a platform enabling remote changes of underlying connectivity provider, offers a significant advantage both to IoT service providers and to their enterprise customers, who can benefit from the lower costs being passed on. eSIM solutions, together with the operator relationships enabled by a remote SIM provisioning (RSP) provider, offer a simple way to enable such flexibility.

Figure 3: Security and cost are most widely cited IoT challenges for enterprises deploying IoT

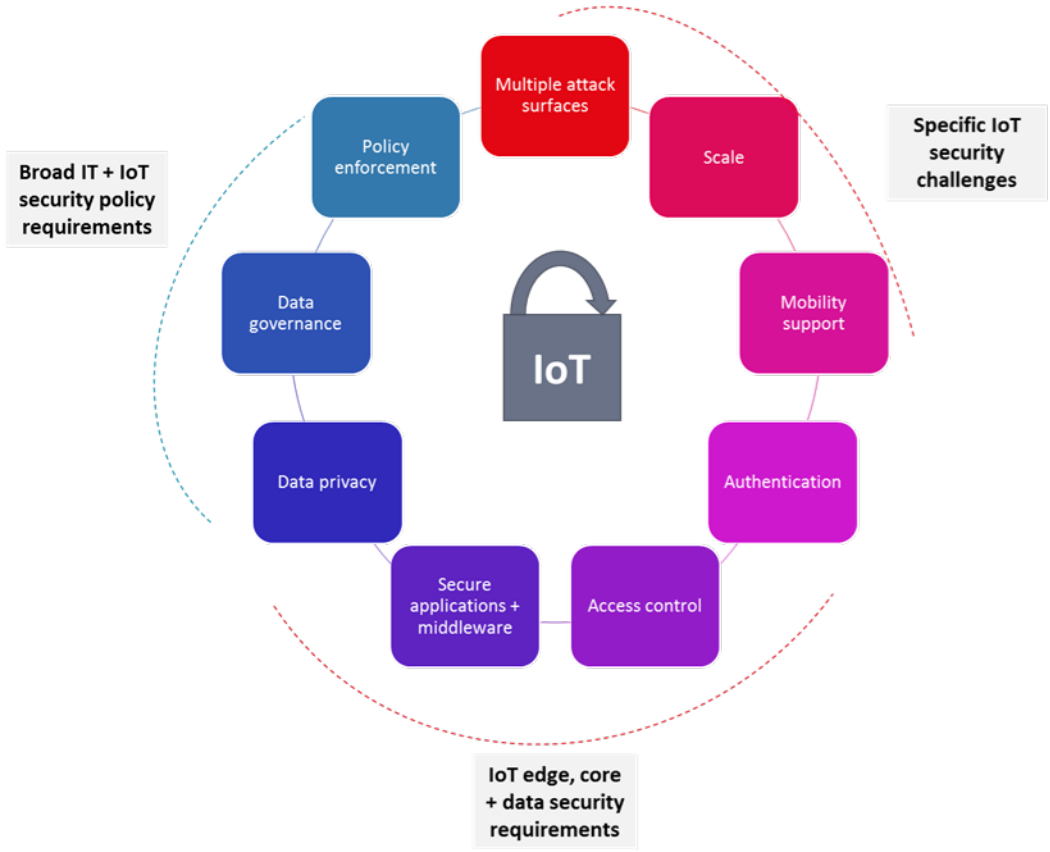
Source: Ovum IoT Enterprise Survey 2017–18, n=1,343. Note: Figures indicate % of enterprises deploying IoT who chose these responses as one of their "top 3 challenges." Respondents could select multiple options.

The security of IoT devices, and the networks and cloud services that enable them, is also of paramount importance for enterprises, OEMs, and IoT operators and service providers. Security comes up as a "top-3" challenge for nearly half of enterprises deploying IoT solutions, according to Ovum's recent survey.

IoT security exploits such as 2016's Dyn attack by the Mirai botnet show that more attention needs to be paid to making the IoT safe, especially given the pace and scale of growth. Similar to enterprise IT generally, IoT security must be applied across three domains: edge security, core security, and data security. Protection, identification, and data encryption are all key IoT security requirements.

However, several factors make IoT security especially challenging (see Figure 4). The IoT presents multiple "attack surfaces" for data, network, device, and application security breaches. The massive scale of the IoT, the complexity and diversity of IoT networks, the requirement to enable machine (not human) control of devices and processes, and the need to deliver this security at low cost and on a long-term basis for IoT devices that may remain in the field for many years – all make IoT security particularly complex. Manufacturers of IoT devices, and enterprises deploying IoT solutions or services should look to build in security from day one. Standardized solutions are a key enabler for this.

Figure 4: IoT security requirements and challenges



Source: Ovum

Another factor impacting IoT security is the requirement for mobility. Some IoT devices, such as sensors in smart buildings or forests, will be static. Others, such as engine control units (ECUs) in motor vehicles, will be mostly on the move while in operation. In security terms, device mobility raises the issue of changing IP addresses, whereas devices that do not move can retain a single address.

eSIMs offer a number of technical characteristics that support IoT security. Several mechanisms offered by eSIMs can be used to safeguard and secure IoT and mobile devices and infrastructure. Link encryption between the device and the mobile network is an inherent part of the eSIM standard. Operators and service providers may want to take advantage of end-to-end application encryption features that are also available.

eSIMs also offer physical security benefits that are relevant for IoT devices. Since they are incorporated into the device, they are less easily tampered with compared to traditional SIMs, as well as having less risk of falling out of the device.

In addition to the physical security characteristics of eSIMs, some eSIM providers offer additional security services that are particularly relevant for the IoT, such as configuring and applying behavior rules on devices to control who and what can communicate with a device. This provides a simple means by which enterprises can implement deeper security controls for their eSIM-enabled IoT devices.

Exploring mobile connectivity options for IoT devices

An enterprise that deploys IoT solutions needs to choose the connectivity option that makes the most sense for its business. Considerations include the specific IoT use case scenario being deployed, its cost and security requirements, and any need for flexibility in provisioning connectivity.

Traditional SIM solutions

Traditional cellular SIM cards are historically most suited to those IoT service providers and end customers that have a contract with one operator, and are likely to continue using that operator for IoT connectivity going forward. They offer the benefit of being portable to newer devices without losing the user's data.

Traditional SIM cards were designed to be easily physically removed from a connected cellular device, to enable the core service information to be ported from one device to another. They are not designed for over-the-air (OTA) provisioning and downloading of new profiles and updates – switching connectivity providers requires a roaming agreement, or a change in the physical SIM for the device.

However, the logistics of physically placing and then provisioning SIM cards in IoT devices can be cumbersome. Devices may be in hard-to-reach or remote areas (e.g., underground, on an oil rig), and replacing the physical SIM may also be impractical as IoT deployments scale up.

These challenges are compounded when the enterprise or IoT service provider needs to deploy and manage their connected devices globally. Multiple operator and roaming agreements are likely to be needed, and devices may require a different SIM in different markets. Global SIMs are on offer from many providers, including major mobile operators. However, roaming data charges can be expensive and unpredictable. Permanent roaming solutions present issues in some markets for regulatory reasons, on top of any concerns about commercial terms. Using a single network operator also leaves the IoT device vulnerable to potential coverage gaps or network faults, as well as locking the device into the operator providing the SIM from a service provision and pricing perspective.

Multi-IMSI

Multi-IMSI solutions combine International Mobile Subscriber Identities (IMSIs) from multiple operators on a single SIM. The IMSI is a unique number used to authenticate the device in which it is placed, on a cellular network. Multi-IMSI SIMs may support as few as two or as many as several hundred such IMSIs, with each being from a different global operator. The home country or network of the multi-IMSI SIM can be changed remotely, allowing it to effectively be "at home" in multiple markets, from a

tariffing point of view, and eliminating some of the inconvenience of having to physically access an IoT device to change the SIM or network.

Such solutions have been available for several years, and can make sense for IoT device deployments that require broader coverage or global roaming, as a means of avoiding high roaming data charges. They are supported by many IoT SIM providers, service providers, and alliances (e.g., Gemalto, Eseye, Cubic Telecom, Telna), with the focus usually on enabling global roaming for connected devices.

One significant disadvantage of multi-IMSI solutions is that they are not standardized – there are multiple varieties of multi-IMSI network architectures and IMSI selection logic approaches. This lack of standardization can impede the scalability of IoT devices and deployments, and also means security issues are likelier to crop up. The fact that the IMSIs are set up through operator agreements at the time of deployment also means these solutions are not necessarily “future-proof.”

eSIM

With an eSIM, the SIM is specifically architected to enable provisioning of the device on a network, and switching networks, digitally. The actual physical SIM does not need to be removed from the device – provisioning, updates, and new profiles can all be delivered over-the-air (OTA).

IoT devices that utilize eSIMs typically incorporate a remotely programmable internal SIM card that gives them the ability to transmit data via multiple operator networks. This allows the IoT service provider to easily shift connectivity providers, if the IoT device needs to use a new network to provide IoT connectivity – because it has changed geographic location, because the new network delivers improved coverage, or because the new network offers more attractive pricing for connectivity. An eSIM, provisioned via a mobile service provider that serves as a data aggregator, offers the ability for the device to change networks remotely using a standardized technology approach. This can be done without swapping out the physical SIM (as would be required with a traditional SIM), and without establishing new operator contracts or IMSIs.

New or relevant operator profiles are downloaded OTA to the device and set up via the eSIM, extending the effective footprint and connectivity options of the device. The mobile service provider or data aggregator provides the eSIM remote provisioning capability to activate the new profile. The fact that this activity is SIM-based ensures a guaranteed level of security, inherent in the SIM and cellular network architecture. Such solutions are offered both by start-up IoT providers, and by a growing number of established wholesale or aggregator players; examples include iBASIS, Sierra Wireless, Tata Communications, Stream, and 1oT.

Manufacturers can utilize the same compliant eSIM industry-wide. Standardization is crucial: both for ease of communications, integration and development; and because the number of compliance regulations is growing across the entire IoT and associated mobile and connectivity sectors. The GSMA’s Embedded SIM Specification provides a single, de facto standard mechanism for the remote provisioning and management of machine to machine (M2M) connections by operators for use on their networks. It provides a common approach and consistent user experience. Standardization also facilitates scalability, an important benefit as enterprises look to connect more and more devices. This in turn can speed time to market for new IoT devices.

Case Study – How Uros uses eSIMs to offer a global end-to-end IoT proposition

Uros, a Finnish telecom services company, offers an excellent illustration of how eSIMs and global connectivity solutions can be powerful enabling tools for IoT service provision. Uros, which was founded in 2011, delivers turnkey connectivity solutions for global enterprises in the following areas:

- 4G Mobile WiFi (MiFi) devices and global mobile broadband service, for consumers and businesses
- embedded global data application and services for OEMs' mobile devices
- global connectivity, remote connectivity management, and smart process management and optimization for industrial IoT use cases.

Uros offers device connectivity worldwide via its patented 4G Goodspeed mobile hotspots, its global roaming IoT platform, roaming applications, and Goodspeed SIM cards. Uros' cloud-hosted IoT platform steers and monitors connected devices as they move across the world connecting to different mobile networks.

Uros' customers include rental car agencies, airport kiosk service resellers, and other types of enterprises looking to connect their devices or to manufacture connected devices, as well as OEM smartphone handset vendors. The service provider also sells its services directly to consumers, in the form of MiFi devices which can be used worldwide.

Specifically for IoT, Uros is targeting the industrial IoT and smart cities markets, and has identified municipal water, pulp and paper, food and beverage, and metal and mining as vertical sectors which would particularly benefit from its solutions. Target use cases include process optimization, remote monitoring, liquid quality control, and wireless global connectivity for all types of real-time sensor data collection and processing. The proposition is to provide an easy-to-use end-to-end IoT solution, including support for global deployment and mobility requirements, to enterprise end users. In order to do this, as well as to support its broader global connectivity services, Uros needed support for its eSIM offering and platform.

Wholesale provider iBASIS, one of the world's largest international carriers, is supporting Uros by enabling its global mobile connectivity offering using standards-based eSIM technology. iBASIS provides Uros with white-labeled eSIMs, an API-controlled eSIM platform, and connectivity to mobile network operators. The iBASIS-enabled Uros solution now covers over 120 countries, and enables local IoT device connectivity via 2G, 3G, 4G, LTE-M, and NB-IoT.

Uros is bringing its eSIM solutions to the IoT market to address issues such as high data costs associated with roaming scenarios, and coverage gaps in rural and remote areas which may not be well-covered by standalone mobile operators. Its goal is to deliver seamless global connectivity through a variety of connectivity options via eSIM, to enable different types of IoT use cases. Uros has chosen eSIMs for its IoT offering because of the technology's ability to easily and flexibly support these core requirements, and because using a standardized eSIM solution provides inherently robust security.

Conclusions and recommendations

IoT demand in both the consumer and enterprise sectors is ramping up. Global, flexible mobile connectivity is an important enabler of IoT use cases for many enterprises, as well as B2B and B2B2C IoT device manufacturers.

Delivering truly seamless global IoT connectivity solutions is challenging from both the technology perspective and the business perspective. Coverage gaps, security concerns, technology complexity, and limitations to industry standard alliances and partnerships have presented obstacles to delivering mobile, globally viable IoT solutions. Enterprise customers need such solutions to be easily deployable at scale, at appropriate cost, and in the right locations.

eSIM solutions, delivered through a global mobile connectivity provider, can be an effective way to enable IoT deployments and devices quickly, simply, and in a future-proof way:

- eSIMs can enable mobile operators, IoT service providers, and enterprises to deliver global connectivity for IoT devices - while avoiding cumbersome contract negotiations with MNOs. This can speed time to market for their solutions and devices.
- eSIMs also simplify global deployment logistics. A single programmable eSIM can be embedded into all of a manufacturer's connected products, which can then be shipped to any market in which the eSIM has a "home" agreement with the mobile operator. This, in turn, eliminates the need to utilize permanent roaming.
- The ability to dynamically swap network connectivity providers as needed, via OTA profile downloads and provisioning, and to deliver OTA updates, can allow for the most beneficial pricing. It can also improve IoT device performance reliability and longevity.
- The standardization of the eSIM technology supports both scalability and security, and can work with multiple IoT technology options.

Along with these benefits, eSIM use can provide benefits from a customer experience perspective, in that the operator or service provider can help "future-proof" customer connectivity needs via the eSIM's remote programming capabilities. These capabilities also allow the customer or IoT service provider to select and set priorities for the IoT device based on specific needs or priorities (e.g., low cost, highest speed, greatest coverage).

In considering eSIM solution adoption, enterprises, device manufacturers, and IoT service providers may find it beneficial to partner with a connectivity provider that has a proven track record in IoT and established relationships with global operators. Benefits include the ability to hand off the technology challenges of integrating with multiple IoT networks; the ability to provide connectivity in different jurisdictions without the capex for new infrastructure or resources required to create new operator agreements; and a clear guarantee of the security and regulatory compliance of devices, applications, and networks.

It is important to note that the eSIM market is still in early stages. The standard specification was first released in 2016, and the market is not yet mature. While many mobile network operators now support eSIMs from both a technical and a business point of view, and some offer them directly, others are moving more slowly, either because of the technical complexity involved or because of a desire to retain as much IoT revenue and customer ownership as possible via traditional SIM

relationships. But the technology is now standardized, and multiple global connectivity providers – both start-ups and established players – are moving to offer eSIM-based IoT connectivity solutions. Enterprises and IoT service providers can expect to benefit from eSIM capabilities in the near future.

Appendix

Author

Alexandra Rehak, Practice Head, IoT

alexandra.rehak@ovum.com

Isabel Freire, Principal Analyst, IoT

isabel.freire@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum
TMT intelligence | informa

CONTACT US

www.ovum.com
analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo