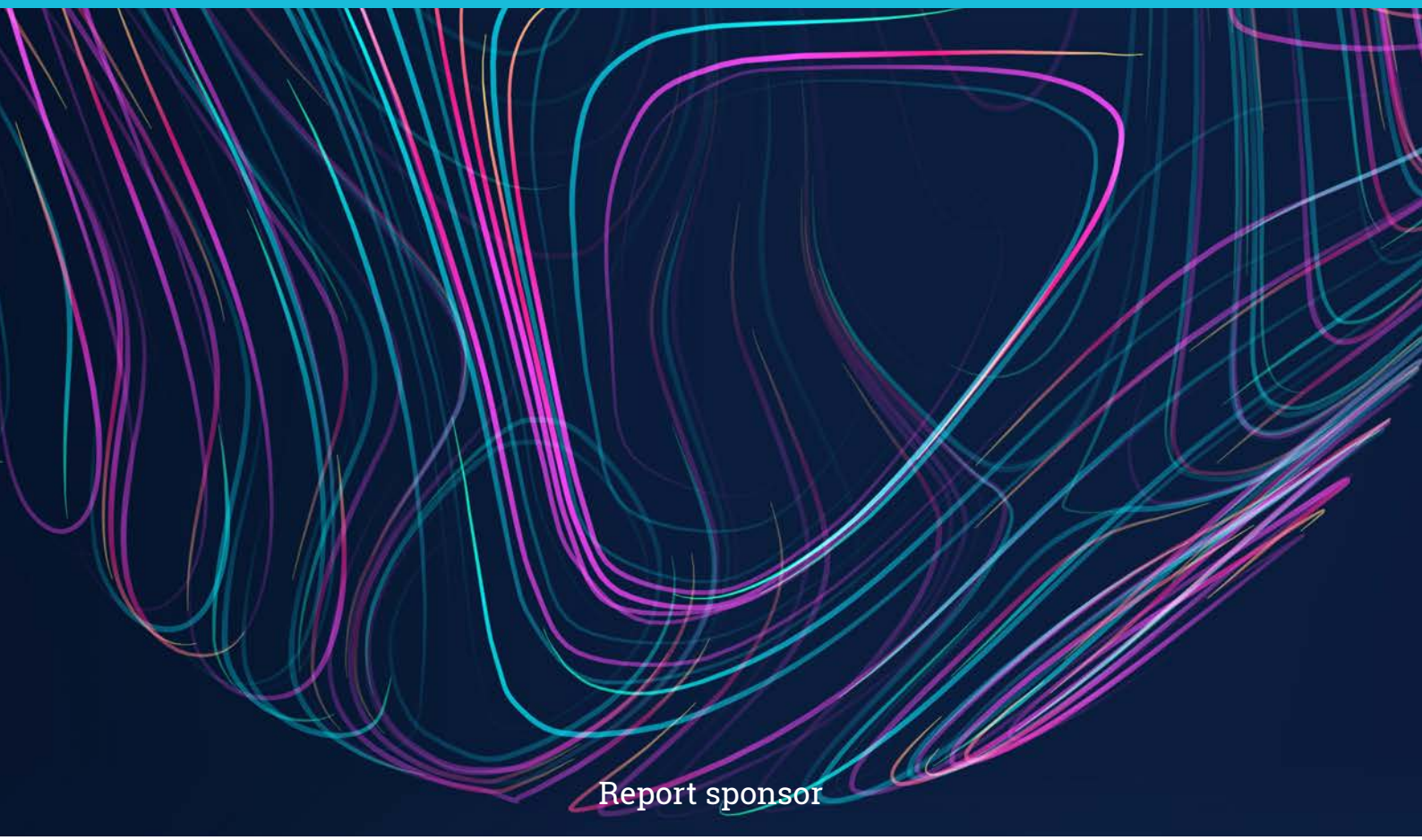
Best practice for delivering IoT connectivity



Report sponsor

BOSCH

Invented for life

Best practice for delivering IoT connectivity

The last decade has seen a rapid evolution in the way that IoT devices are connected and supported. In this light report Transforma Insights examines the key developments in delivering cellular-based IoT, how they translate (or should translate) into evolving demands from enterprises, and what connectivity providers, and others in the ecosystem, need to do to deliver them

The IoT connectivity space is going through a period of pronounced change. The tools used to deliver connectivity, the commercial models surrounding it, and the regulatory environment are undergoing a period of quite rapid evolution. In this section we identify some of the key critical changes that might affect how enterprise IoT solutions might be supported.

The first development relates to the arrival of a set of technologies that are optimised for more effectively supporting IoT. The most notable of these is probably the arrival of a set of low power wide area (LPWA) technologies that are designed to support relatively low bandwidth applications (less than 1Mbit/s, and often much less), coupled with low power consumption allowing devices to last for months or even years in the field, and a low price point. The most notable cellular additions here are narrowband-IoT (NB-IoT) and LTE-M. These technologies are the medium-term replacement for 2G and 3G networks, and with superior capabilities, that are being switched off around the world.

A number of other technologies have also become available that are also optimised for deployments in more constrained environments, i.e. where there is a lack of access to power, processing or connectivity. For instance, IoT optimised protocols such as message queueing telemetry transport (MQTT), constrained application protocol (CoAP) and Lightweight M2M (LwM2M) are increasingly widely used. Similarly, embedded operating systems such as Free RTOS, TinyOS or Zephyr, reduce the requirements for processing and memory on the device. ▶

One of the key facets of the arrival of the IoT optimised technologies noted above, is that they are also highly constrained, meaning that it's necessary to ensure that they are cross-optimised with each other to make sure that devices, connectivity, protocols and applications all work well together. This is one reason why we see hardware makers increasingly successful in bundling hardware and connectivity: one cross-optimised solution with a single vendor to deal with in the event of any problems.

The other major technology development is embedded SIM (eSIM). Until 2016 devices relied on removable SIM cards for authenticating devices. Since then eSIM (a ruggedised soldered chip) has become increasingly the norm, with integrated SIM (iSIM), which virtualises the SIM entirely as an element on another processor, to follow. With this change of form factor can the need to change the profile remotely, using a technique called Remote SIM Provisioning (RSP). Today there are two standards (known as M2M and consumer) with a third (IoT) being standardised currently. The availability of eSIM creates new dynamics in how connectivity can be provided and by whom. According to Transforma Insights, by 2032, 40% of new cellular IoT shipments will be eSIM-capable.

The advent of eSIM focuses attention on another major change ongoing in how IoT connectivity is delivered, particularly for multi-country IoT deployments.

Historically connectivity providers used roaming, either based on their own roaming agreements or those of partners. Alternatives included proprietary 'multi-IMSI' approaches. However, roaming has become less viable, partly due to regulation, and partly because host networks have been less willing to accept roaming IoT devices on their networks. The need to be conscious of regulatory issues of all types has also increased dramatically in recent years.

We should also note that the delivery of IoT connectivity is not immune from the growing importance of artificial intelligence. It has two major implications. Firstly it can be harnessed for more effectively delivering IoT connectivity services, for instance in analytics and optimisation. Secondly the requirement to embed AI within applications will have knock-on effects on the architecting of IoT solutions. Whereas historically the intelligence of an application might have resided on the customer's server or hosted in the cloud, increasingly the intelligence will be distributed so as to reduce the latency of the application and more efficiently manage data. This creates implications for edge computing, and the need to manage payloads at various points on the network whether that be at the edge device, the network edge, or in the cloud.

Turning to the more commercial aspects of IoT we also note a number of significant trends that influence how ▶

IoT connectivity is delivered. Most notably there is a clear dynamic of price erosion, manifest in what Transforma Insights refers to as '$1 IoT', whereby many devices may generate less than US$1 of revenue per year. This doesn't apply to all connections, but it is likely to apply to a large volume, particularly of the LPWA connections. This trend triggers connectivity providers to make numerous changes to their propositions to do two things: bolster revenue and reduce cost. In the former case this results in the addition of new services offerings, which in many cases are sorely in demand by enterprise customers that need more of a tailored service. In the latter case it drives a desire to be more 'hyperscale', delivering connectivity with low touch, highly scalable platforms and processes.

7 key requirements of enterprise IoT connectivity users

In general, enterprise demand for the features and functionality of their IoT connectivity solutions have always been quite consistent: secure, reliable, compliant, low cost connectivity that is easily managed and highly scalable. However, with increasing price pressures, more regulation, emerging technologies and new commercial dynamics, those needs are constantly in flux. This section provides an overview of the key requirements that Transforma Insights hears from enterprises regarding IoT connectivity, whether they are triggered by evolving changes in the industry, or not.

Reliability

The prime consideration above all others with IoT connectivity is: does it work? Network outages are unacceptable and enterprises need to give careful consideration to which mechanisms are being used by connectivity providers to support their deployments. This necessitates some potentially tough questions with providers over exactly how they plan to deliver connectivity services such as sponsored roaming, multi-IMSI, or eSIM localisation. Further to this, the cross-optimisation topic noted in the previous section should deliver more effective solutions with fewer faults, as well as simpler fault resolution, because the different elements of the solution have been developed with consideration of the capabilities and limitations of the others.

Reputation and brand

In the Transforma Insights Enterprise IoT connectivity survey published in November 2022, the number one factor influencing enterprises over vendor choice for IoT connectivity was "reputation/brand". The category combines a broad range of considerations, but there is little doubt that enterprises should give very careful consideration to whether a connectivity provider is a trusted long-term partner. Most enterprise IoT deployments will involve a long-term relationship that typically involves mission-critical applications. Enterprises should look at factors such as ownership ▶

structure and major backers, the use of standards, and established credentials with major adopters. Similarly the ability to back-out of a relationship if things go wrong, which would usually be associated with the use of eSIM.

Security

This topic has always been one of the top two considerations and concerns for IoT adopters. The security threats associated with IoT are growing: there are more use cases, with bigger scale and more mission-critical than ever before, making IoT an increasingly appealing target for bad actors. Even without that growing scale, the security landscape for IoT was already something of a headache with a complex array of stakeholders, a diverse set of devices, and a general lack of embedded security development skills. Add to this the fact that IoT is making more use of constrained devices with potentially less capability to support security features.

Coverage

With cellular IoT connectivity, there is no escaping network coverage as a significant consideration. However, the degree to which coverage is important will depend very much on the application. Some devices will be located in hard-to-reach places, while others will be constantly moving. The question for enterprises is: will I get the right coverage for the application at an appropriate price point. Some connectivity providers may be able to support connectivity over a single network in a market, and others using multiple networks. The use of eSIM for localisation may be the best approach. But in some cases the ability to roam onto multiple networks will give a superior experience. Cellular connectivity solutions are also increasingly integrating non-terrestrial networks (NTNs), i.e. via satellite, so these offerings may hold some potential.

Price

We have already mentioned that price for IoT connectivity is seeing some erosion. This will always be a prime consideration for enterprise customers. However, the most important thing to consider is: low price at what cost? A low headline rate often belies a service that is not delivered in a compliant way. Or where there will be subsequent overage charges once the real volume of data generated by the application becomes apparent.

Compliance

Regulations affecting IoT have expanded significantly in recent years. This has increased the degree to which enterprises need to be aware of compliance-related topics. This is particularly important for some countries that have more challenging regulatory regimes, e.g. Brazil for permanent mobile roaming, China for data sovereignty, Europe for data, or the US for device security and certification. ▶

Support

For most enterprises, IoT is not core business. As a result, it is normal for enterprises to require a high degree of hand-holding as they go through the process of developing and rolling out their IoT solutions. Most need an additional service layer on top of the technology building blocks which helps them to understand which are the most appropriate technologies for them to use, what the roadmap looks like, how to deploy them and more.

A checklist for what connectivity providers and others in the ecosystem need to deliver

The evolution in technology and commercial models, as well as changing demands from customers, as outlined in the sections above, should flow through into a refined set of capabilities from IoT connectivity providers, MNOs and MVNOs.

In this section we provide a checklist of some of the key facets of what those providers should deliver, both technical functions, such as features of a connectivity management platform, and services.

SIM management - The baseline functionality of IoT connectivity, involving managing the SIM, specifically activation, deactivation, suspension, APIs and some billing functions.

Abstraction - Many enterprise customers have multiple relationships with connectivity providers. They will want a single pane of glass to enterprise customers to manage all their connections.

Localisation - Supporting connectivity in any geography, either through eSIM subscription management or through some other viable alternative to provide compliant comprehensive coverage.

Analytics - A range of analytics and automation of connectivity functions based on network data, including related to network selection, security, anomaly detection, root-cause analysis, churn reduction, bill prediction and many more. This is likely to make increasing use of AI. To be fully optimised, this must be real-time.

Control - Complex global device deployments demand greater policy control and management of data flows. It is increasingly common practice for connectivity providers to operate their own core network and associated infrastructure for the purpose of providing greater transparency, more real-time capabilities and higher levels of security.

Compliance - Connectivity vendors need to be able to provides some level of guarantee to the enterprise about the end-to-end compliance of its deployment, for instance related to permanent roaming, data sovereignty or device security. ▶

A device-to-cloud (and edge) experience - IoT is about connecting devices to the cloud to enable (bidirectional) data flows. As a result, an IoT connectivity offering must incorporate serious considerations of (and features related to) delivering that full stack. This includes cloud connectors for seamless integration into AWS, Azure and others, orchestration of payloads, and the integration of hardware into the proposition.

Devices - Further to the device-to-cloud topic, IoT connectivity providers are increasingly adding in device-related capabilities, as a way to avoid the potential pitfalls of simply bolting on a connectivity provider to an already built device. Capabilities include hardware integration and optimisation, device management, troubleshooting, and warehousing and fulfilment.

Security - A range of capabilities including end-point, network (such as private APNs, network diagnostics and troubleshooting, device locking, device quarantining), transport (such as IoT SAFE and transport layer security), cloud/data, and application security. Additionally end-to-end security including secure-by-design, policy management, vendor compliance, and anomaly detection across the other layers.

Hyperscale platforms and processes - The price of connectivity is declining and in order to support that, particularly for low-cost LPWA connections, IoT connectivity providers need a set of capabilities and processes in place that can deliver connectivity in a low-cost scalable way. This includes cost-effective connectivity management platform with low touch onboarding of devices.

Speed and agility - Time to market is an increasingly important issue for enterprises deploying IoT. Operators will need to provide a connectivity solution that is deployable in a matter of weeks. Connectivity providers also need to be sure that they can react to changing market dynamics, including regulation, requiring new features, reports or technologies, delivered in a timely way.

SLAs - IoT is often deployed for mission-critical use cases. Enterprises will demand strict SLAs, particularly over up-time and fault resolution time. The ability to offer SLAs will depend largely on the CMP vendor's end-to-end control of the proposition.

Superior customer support - Comprehensive 24x7, follow the sun, support is a must-have for IoT connectivity providers. As is online self-care. Also customer success managers to act as the voice of the customer within the organisation, reflecting the fact that IoT is not a product-based transaction, but a managed service.

A customised/contextualised approach - IoT is not best delivered as an off-the-shelf product. All customer requirements are different and require some degree of customisation, or at least contextualisation, i.e. delivering a connectivity offering that is the most appropriate for the customer's circumstances. This requires enhanced pre-sales support and a consultative sales approach to really understand their needs.