Can we realise the promise of IoT, and tame the complexity? Yes, says Eseye

Massive IoT is on a long journey that is yet to reach its destination. Early deployments have barely scratched the surface of the opportunity and we're still waiting for tens of billions of IoT connections and more importantly the value they create to arrive. Excess complexity, weak standardisation, geographical fragmentation, and different technologies have all played their parts in slowing adoption but simple access to connectivity has been among the leading drag factors to IoT's progress.

This is changing with the introduction of eUICC-enabled embedded SIMs (eSIM) but there is still too much inconsistency, lack of flexibility and poor management visibility and control when it comes to IoT connectivity. What's needed is a universal platform for managing IoT connections that is mobile network operator agnostic and can be applied across all the networks devices use, Nick Earle, the chief executive of Eseye, tells IoT Now managing editor George Malim ▸

SPONSORED INTERVIEW

There are more than 800 mobile network operators (MNOs) and all have the same business model of offering a proprietary SIM that locks you in to a contract with them

Nick Earle
Eseye

George Malim: Everyone understands that the predictions of there being tens of billions of IoT connected devices by now were overcooked but even so, the potential of IoT and massive IoT in particular hasn't been met. What has been the hold up?

Nick Earle: First, there is a complete lack of interoperability. There are more than 800 mobile network operators (MNOs) and all have the same business model of offering a proprietary SIM that locks you in to a contract with them. They connect you to their network and if your device is out of their coverage zone they choose and manage the roaming partner.

The problem with this is that under this model no operator, no matter what size they are, can offer anything like 100% global coverage for IoT devices. There are always geographical coverage gaps ranging from 20%-40% depending on the country. And when a roaming profile – an international mobile subscriber identity (IMSI) - is used there is no cast iron guarantee that a network will always be available. This is because roaming quotas between operators are set in advance and often inadvertently exceeded, in which case permanent roaming can be limited or made unavailable. And finally, permanent roaming is prohibited by the regulator in many countries.

What this means is that if you want to embed global connectivity capability in your IoT devices, you must use multiple MNO SIM cards and patch coverage together yourself. This creates huge overheads in manufacturing and supply chain logistics. If you want to embed a SIM card in a device you either have to ship cards from the MNO in the country of deployment to the factory or manufacture without any SIM in the device, and deal with the local SIM installation logistics at the point of deployment.

By adopting a global embedded UICC enabled eSIM, you can solve one component of the puzzle. A single global product with a single stock-keeping unit (SKU) number that can bootstrap to the optimum available network automatically when deployed.

GM: Does eSIM solve the complex management challenges that are stifling IoT growth?

NE: On its own, no. eSIMs are not consumer SIMs, they need specific hardware capabilities and firmware settings to enable effective communication between the modem and the SIM, power management and IMSI rotation. Customers don't have these skills – they need their IoT partner to solve these issues for them upfront before they deploy and have challenges.

In addition, many MVNOs say 'we use eUICC enabled eSIMs now so we can do global IoT' but the provision of global connectivity is more than just switching between roaming contracts, providing a single management dashboard and consolidated billing. Your IoT partner needs its own SM-SR (the switch that controls the remote SIM provisioning) that can work across any MNO as well as an SM-DP (the list of IMSIs you can switch to) and in most MVNO solutions this functionality is not owned by them as it is resident in each MNO. So, if that global single SKU is reliant on four MNOs to ensure complete coverage, you could then be in a situation where each has its own platform, pricing, application programme interfaces (APIs) and support systems which the user has to glue together. This doesn't provide what enterprises need for their IoT projects – they want it to just work, not to have to act as if they are an MVNO or systems integrator. We believe 80% of market adoption hasn't happened yet because agnostic operator interoperability and a true single global platform management capability has not yet been enabled.

GM: How will the IoT industry eliminate the crazy and enable the massive IoT opportunity to become reality?

NE: We've approached this by asking our customers: if you had a blank piece of paper, what capabilities would you ask for to help simplify IoT deployments?

When we do this, they consistently say it comes down to enabling them to use one eSIM to connect any device anywhere with maximised choice of network localisation, not just roaming. They want the ability to switch networks based on their rules; not the operators and all devices, new and legacy, to be managed via a single platform which gives the choice to either buy data from the IoT partner or directly from any operator. On top ▶

We also have the Eseye AnyNet Federation which now has 16 MNO members with more being added

of this they want a single set of APIs to create new managed services to allow them to create new customer experiences.

The only way to achieve this is to design the architecture and the solution specifically to solve these IoT problems. That's what we've done at Eseye, and we call this 'IoT that works'.

GM: That's easily said but how is Eseye able to provide this level of simplicity to your IoT customers?

NE: A few years ago we bought a specialist IoT hardware design company, DataFlex. This has become a hugely important part of our value proposition as we are able to either design a device for an edge router to meet a specific use case, or analyse a customer's existing device to identify the firmware changes that need to be made to enable full eUICC functionality and global deployment capability. We own the problem, so the customer doesn't have to.

To solve the management issue, we have built the **Infinity IoT Platform**. A full stack of cloud-based capabilities encompassing the access layer, network layer, BSS & OSS, RSP (rules-based remote SIM provisioning via our own SM-SR and SM-DP), device management, API enabled analytics and a security and policy engine. This enables the capability for a device to rotate between operator IMSIs either from up to 10 pre-loaded IMSIs or through an over-the-air (OTA) transfer from our cloud platform.

And we enhance these mobile virtual network enabler (MVNE) type capabilities with device design, testing and certification professional services to help our customers with the complete IoT lifecycle – from idea to implementation. The functionality is truly global as it is native to **AWS** and runs across our 20 data centres, enabling local breakout using our own private cloud-based, software-defined network. Furthermore, all data is encrypted with access point name (APN) access and does not terminate on the public internet.

We also have the **Eseye AnyNet Federation** which now has 16 MNO members with more being added. It's like the **Star Alliance** airline model but for IoT and gives us a great localisation footprint across the globe. What this means is that our platform rules engine can switch the device connection between networks OTA, across all of these operators and localise the connection when doing so. When this happens, we avoid roaming and so protect our customers from the risk that a single operator plus a pre-determined list of roaming options can present. We like to think of ourselves not as an MVNO but as a VMNO – i.e. a virtual mobile network operator delivering 100% global connectivity via an abstracted, operator-agnostic software capability based on cloud federated network orchestration.

GM: What other features does the new platform offer to help IoT service providers manage their devices?

NE: Enhanced security. It's great that eSIM makes the SIM agnostic to the operator but an eUICC-enabled IMSI change means that when the device moves from operator A to operator B the IP address also changes. So if your application uses fixed IP addresses you can lose device visibility. And if you have implemented your security via **Vodafone**, for example, but the device rotates to **Three**, for example, you have to implement another security solution integration. ▶

Our single MPLS network architecture for all connections allows developers to extend connectivity to all eSIM devices. For example, we have signed a deal with **Armis**, the leading agentless IoT security company, to extend security to the edge via an API to our network. Without this capability they'd have to do multiple MNO integrations.

Another compelling aspect is that Infinity has the capability to not only manage Eseye SIMs but legacy SIMs as well. What this means is a single platform solution for all customers' devices - not yet another platform.

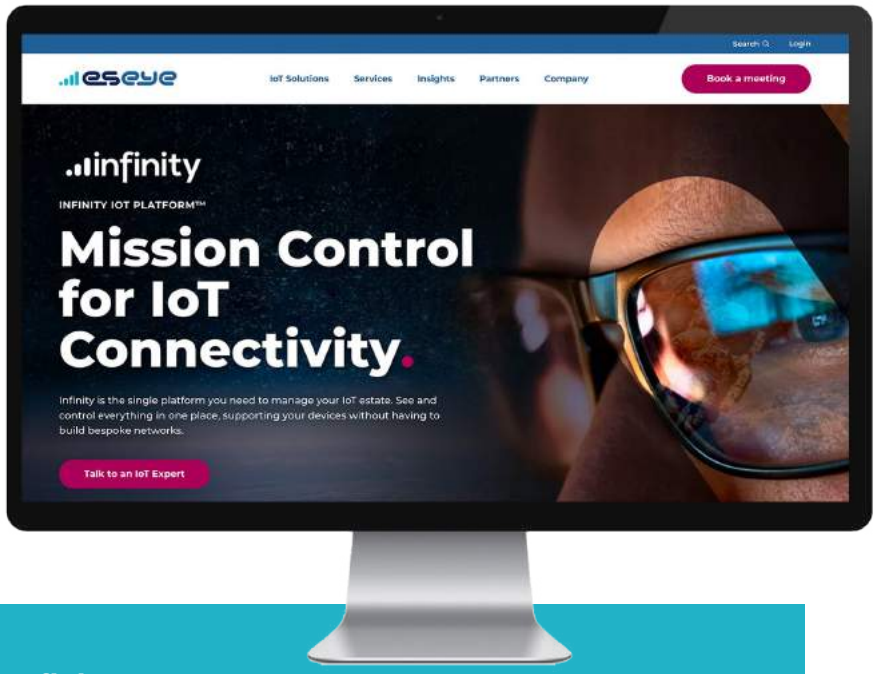
GM: What's Eseye's business model for the platform?

NE: A key feature is BYOC – bring your own contract. For example, if customers have a great data rate from **Verizon** for the US, then they can use that contract, and if they need connectivity in remote locations like Brazil or Turkey, for example, they can buy that data from us. In both cases we manage it all through one platform for which they pay a small fee per device, per month. This has resonated very strongly not just with the initial large enterprise customers who see it as a best of both worlds option, but also with the MNOs who want to maintain their relationship and revenue with the customer in their key markets.

We also offer the ability to manage private LTE and 5G networks across our platform. This allows seamless switching across both public and private networks, which opens further dimensions for large enterprise deployments and customer choice. This is going to be hugely important as devices move seamlessly between private and public deployments. It will be the MNO switching problem on steroids.

We also offer the ability to manage private LTE and 5G networks across our platform

www.eseye.com/infinity



How IoT service providers are using Infinity

The Infinity IoT Platform is being used by many large enterprises as they grapple with the challenges of managing their global IoT device estates. Most want to simplify management while enhancing flexibility, control, and security. Some companies take Infinity directly from Eseye, but others take white-labelled versions of the solution from providers such as **TELUS** under the TELUS Global Connect brand.

The platform is currently in use by **Amazon** for its Lockers and Key for Business (KFB), the business version of the Ring doorbell, devices. In the case of Lockers, they have implemented a globally dispersed network of physical drop boxes being enabled by Eseye. Similarly, KFB devices are being used by Amazon Prime drivers to gain automated access for parcel drop offs around the world. Infinity is utilised to ensure global, reliable connectivity so they can put a Locker on any street corner in the world or a Key for Business device into any door or gate and it just works – first time and with 100% connectivity.

Shell Recharge Solutions has long been an Eseye customer but also utilised another operator SIM card in the European chargers. With the Bring Your Own Contract offer; Shell is free to contract directly other MNOs as necessary while deploying a single Eseye SIM across all its charging points and in so doing gain visibility and management of all its devices from a single platform - Infinity.