ISSN 2634-9116

IoT Global Network

trending tech.

WILL eSIM ENABLE IoT SECURITY AT SCALE?

Vol. 3, No. 4

Report UK£99 but **FREE** for anyone that registers to Trending Tech: **www.trendingtech.io**

Trending Tech – your new inside track to the topics that **really** matter.

eSIMS RE-INVENT SECURE, TRUSTED CONNECTIVITY FOR A NEW GENERATION OF CONNECTED DEVICES

Embedded SIM is introducing a new environment in which IoT organisations can experience greater interoperability, improved security and more freedom to choose their connectivity provider. Standardisation, automated provisioning and a renewed focus on secure credentials are driving uptake in the enterprise and IoT markets and high volume adoption is now reality across many sectors, writes George Malim

Embedded SIM (eSIM) has emerged as a means to free consumers and connected devices from the constraints of the traditional, plastic subscriber identification module (SIM) card by enabling an eSIM or an integrated SIM (iSIM) to be embedded into a device at the point of manufacture and shipped globally. On arrival at the place where it will be used the device simply connects to the most suitable network operator in a process known as bootstrapping and the device is authorised to connect to the network, with the owner paying service charges.

This radically simplified process is an advantage for original equipment manufacturers (OEMs) because it enables them to streamline the production process and have just a single stock-keeping unit (SKU) designation for a global product rather than having multiple variants for different global markets. Users also benefit because they don't have to install SIM cards into devices when they arrive at the point of use. They also don't have to engage in complex vendor management processes nor do they have to commit to a single carrier for the life of the deployment. Instead, they have flexibility to choose the best coverage at the best price for each deployment.

In practice, it is still likely that large deployments will drive economies of scale by utilising connectivity from a single mobile network operator or group but having the flexibility to use the network of a rival where there is no or poor coverage is a substantial benefit.

Although introduced into the consumer sector over the last decade in a variety of smartphones such as devices from **Apple**, **Google** and **Samsung** and more recently the **Moto** Razr, the first eSIM-only model, smartphone deployments are set to account for almost 50% of eSIMs by 2025, according to **Counterpoint Research**. This suggests that large markets will co-exist in enterprise IT and IoT.

"IoT-based devices and modules have also seen a significant adoption of eSIM, driven by eSIM standardisation requirements for M2M/IoT devices," said Karan Dasaor, a senior analyst at the research firm. "The current eSIM adoption as well as activation rates in cellular B2B IoT are much higher than consumer IoT, as devices are often in difficult places to reach physically, making eSIM a must. The low revenue per connection also works against physical provisioning. LPWA technologies, such as LTE-M and narrowband IoT (NB-IoT) will be key drivers for cellular IoT devices at mass-market scale for things and assets which were never connected before."

Into the billions

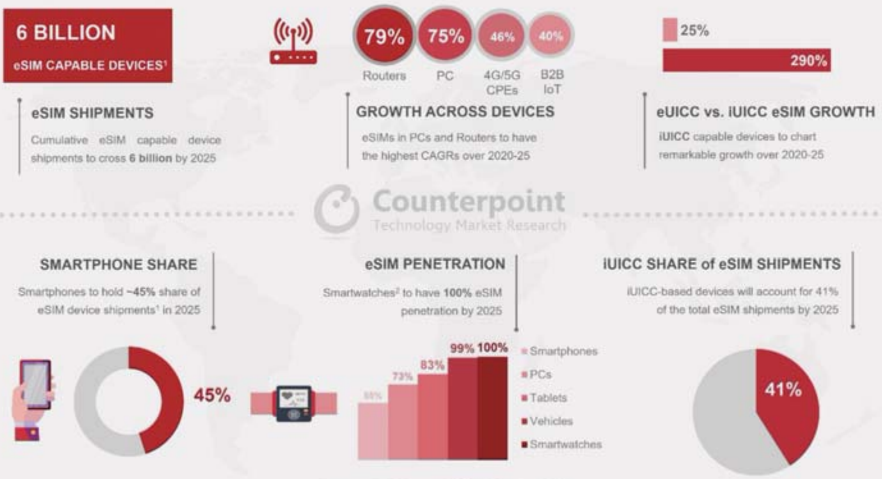
Counterpoint Research projects in **Figure 1** that six billion eSIM capable devices will have been shipped by 2025 with B2B IoT eSIM adoption having a 40% CAGR over the period 2020-2025. "**Microsoft**, **Intel** and **Qualcomm** have been focusing on always-connected PCs supporting natively integrated eSIM and LTE modems," added Dasaor. "Several LTE PCs have already been launched, with eSIM appearing in many SKUs. With 5G likely to reach the mass-market in the future, cellular connectivity will become a standard for laptops and those without it will slip towards a minority. We expect eSIM capable PCs and B2B IoT devices to exhibit CAGRs of 75% and 40% respectively over the next five years." ▶

Commenting on eSIM penetration, Counterpoint's research vice president Neil Shah said: "Smartwatch-makers have been increasingly adding cellular connectivity for varied use-cases, from health monitoring and safety tracking to making them standalone companion devices. eSIM is a natural fit here from the integrated form-factor, space-saving and ruggedised design perspectives. Apple, Samsung, **BBK**, **Huawei** and others have adopted eSIM for their cellular models."

"Emergency services as well as driving and vehicle condition monitoring via telematics have been the primary drivers for cellular connectivity modules and eSIM capabilities inside vehicles," he added. "The European eCall mandate, which requires all new cars be to be equipped with eCall technology from April 2018, has also continued to drive greater embedded connectivity. Over the next few years, the addition of connectivity to infotainment for content streaming, live HD maps and other use-cases will drive eSIM adoption. eSIM is expected to permeate into nearly 100% of the cellular connected smartwatches and vehicles by 2025."

These initiatives fuel interest and market acceptance of eSIM and embedded universal integrated circuit cards (eUICC) and are introducing greater awareness of iSIM and iUICC, as Shah explained: "Both eUICC, hardware-based eSIM, and iUICC, software integrated eSIM or iSIM, form-factors will co-exist and grow depending on the preference of mobile network operators and device and module makers. So far, eUICC has been the go-to standard for eSIM implementation. However, iUICC capable devices' growth is expected to outstrip eSIM devices' growth with the former growing at a CAGR of around 290% over the next five years. We expect the iUICC-based eSIM to become quite popular among Chinese smartphone brands, as they move from less secure trusted execution environment (TEE)-based virtual/soft SIM to a more robust iSIM solution. Players such as Apple and Samsung will also be looking to offer an option to replace hardware eSIM with iSIM if it meets GSMA's secure element specifications, as it is critical for operator-driven western markets."

Figure 1: Counterpoint Research's Key eSIM Insights Dashboard



Source: eSIM Forecast & Analysis, Dec 2020

Dasaor also highlighted, "If the iUICC is standardised in next two years or so, we should see rapid adoption and the segment providing tough competition to hardware-based eSIMs after 2026-27. The role of players such as Qualcomm and **Arm** will be crucial in driving this across smartphones. We also see a greater interest in iSIM solutions after 2021 in IoT as more module vendors and operators start supporting it formally. Overall, iUICC-based devices will account for 41% of the total eSIM capable device shipments by 2025."

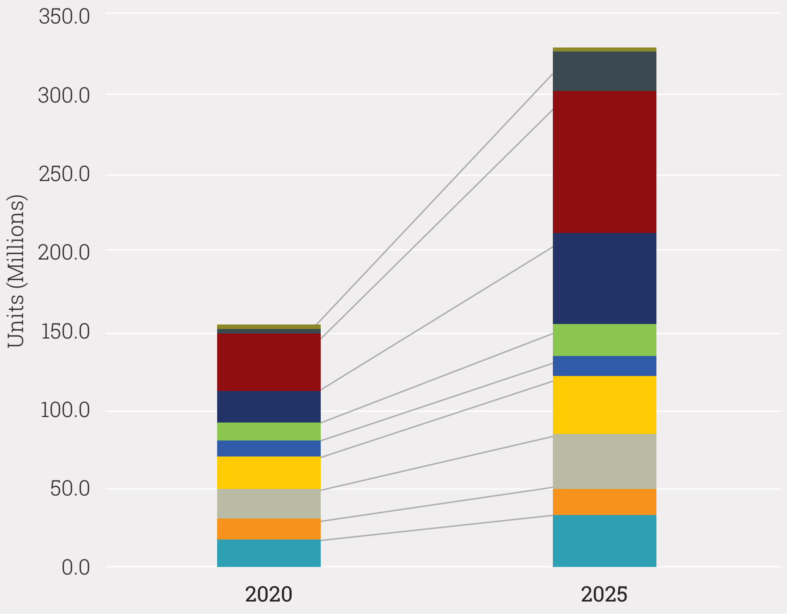
Awareness meets appetite

The increased awareness of eSIM and later iSIM is aligned with significant business needs for the technology. "The growing number of SIM-enabled devices in IoT projects presents a maintenance and management headache from an enterprise perspective; the need to change SIM cards in millions of IoT devices, is impractical and unrealistic," said Andrew Brown, the executive director of enterprise and IoT at **Strategy Analytics**. "eSIM offers a robust, scalable solution to the SIM card challenge especially for enterprises and is based on the open, vendor-neutral standard developed by the **GSMA**".

For those reasons, eSIM developments are now ramping-up and, following years of non-interoperable eUICCs, the industry now has clear standards and a broad ecosystem of partners, with more than 200 carriers supporting eSIM. "Over the last few years we have also seen growth in iSIM, which builds on eSIM functionality," added Brown. "While an eSIM is a dedicated chip soldered on to a board and attached to a device's processor, iSIM integrates the processor core and encryption in a system-on-chip (SoC). This is important for use cases which look for low cost, low power, and high levels of security in very small form factors. The growth in eSIM and iSIM is vital to driving seamless connectivity into as many devices as possible over the coming years." ▶

Figure 2: Total IoT eSIM sales by vertical industry (millions)

Source: Strategy Analytics, 2020



As **Figure 2** shows, Strategy Analytics forecasts that sales of eSIMs for IoT applications will grow to 326 million by 2025. One of the reasons for this projection, according to the firm is that eSIM offers the ability to change service provider profiles using remote SIM provisioning (RSP), without needing to physically change the SIM card itself, which is vital in enabling devices where it is either difficult or inefficient to access a physical SIM, for example hermetically sealed medical devices, vehicles, consumer electronic devices or a whole range of other IoT devices.

RSP also plays into IoT organisations' desire not only to have flexibility but to have greater control of connectivity and to be assured of security for their devices. Significant steps have been made in this respect with **GSMA** piloting development of the IoT SIM Applet For Secure End-2-End Communications (IoT SAFE), which aims to provide a standardized, globally accepted root of trust for IoT communications. Ensuring that eSIM includes a root of trust or secure element is therefore an increasingly important requirement and one which suppliers are responding to.

P.A.ID Strategies has launched its new 'Digital Secure Solutions: Credentials, Embedded + IoT Devices Market Intelligence Service' and found that the market for secure credentials and embedded hardware for connected devices increased in value by 15.4% in 2018 and is forecast to rapidly grow by a further 41% by 2022 as emerging applications in IoT implement security and digital credentials are introduced alongside existing smart cards.

IoT sectors, including automotive, industrial, ICT infrastructure, logistics and supply chain, object ID, smart home and consumer, and utilities will increasingly look to proven hardware-based secure solutions in order to meet regulatory, service provider and end-user requirements and concerns regarding security and data protection.

Secure credentials

Traditional credentials, such as smart cards, will continue to account for the majority of market volume although the ability to create, access and share digital credentials, plus securing connected devices, will drive adoption of higher value solutions. Demand is set to increase to 18.8 billion units in 2022 for a combination of authentication ICs, embedded secure elements (eSEs), embedded SIMs (eSIMs), hardware security modules (HSMs), secure microprocessors, smart card ICs, secure access modules (SAMs), trusted execution environments (TEEs) and trusted platform modules (TPMs).

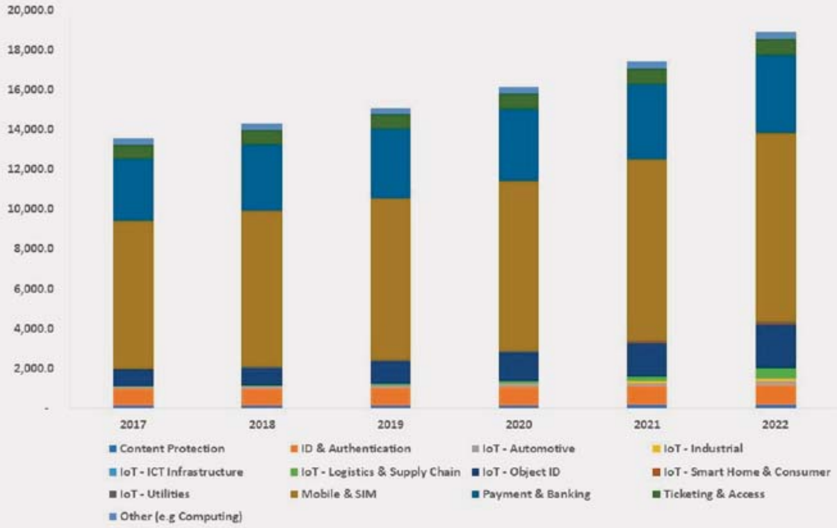
"Smart cards have been a proven and trusted solution for 20 years although adoption has been unsteady, even in established sectors such as banking and government," said John Devlin, a principal analyst at P.A.ID Strategies. "We expect that the same will happen in these new IoT applications; it will not be even and steady despite there being a recognised need to implement security."

Different industries will move at different paces and take different approaches, depending on the level of security their applications need. As **Figure 3** details mobile and SIM deployments will lead uptake for secure digital solutions with various subsectors of IoT accounting for significant activity, accelerating as offerings mature.

"Automotive has been the first to move, with deals being struck between OEMs with companies like **G+D Mobile Security**, **Infineon** and **Trustonic** for eSIMs, TPMs and TEEs to ensure cars remain safe and secure as they become more connected and autonomous," Devlin added. "Some sectors are more fragmented and will either take regulation or a major breach to move the market forward. Smart home and consumer devices are quick to market and do not always have security built in by design." ▶

Figure 3: Applications for digital secure solutions 2017-2022

Source: P.A.ID Strategies



Although it does not foresee the industrial and public sectors driving eSIM uptake, **Juniper Research** does see significant opportunities for the technology across industrial sectors. A recent study identified the oil and gas, manufacturing and logistics sectors as three key areas in which eSIM adoption will ramp up. The firm's research suggests that the development of rugged form factors will position vendors well to capitalise on the market, as eSIM installations in these verticals grow from 28 million units in 2021 to 116 million by 2025.

Research author, Scarlett Woodford, said: "Ensuring convenience for the end user must remain the top priority for eSIM management platform providers. To do so, they must provide a level of service comparable to that found with traditional SIM deployments."

Even so, the firm believes the consumer sector will account for 94% of global eSIM installations by 2025 and anticipates that established adoption of eSIM frameworks from consumer device vendors, such as Apple and Google, will accelerate the growth of eSIMs in consumer devices ahead of the industrial and public sectors. The bulk of eSIMs will be installed in connected devices and these will increase from 1.2 billion in 2021, to 3.4 billion in 2025; representing a growth of 180%.

The research found that global eSIM deployments across all consumer verticals will increase by 170% over the next four years, with widespread adoption reliant on backing from network operators. Juniper Research therefore has urged device manufacturers to place pressure on operators to support eSIM frameworks and accelerate market maturation.

However, fragmentation of hardware vendors in the cellular IoT device market will require each vertical to adopt a combination of wireless technologies, hardware and management tools. In turn, it predicts that specialist vendors will emerge that provide robust eSIM form factors for industrial environments. These, alongside eSIM and iSIM providers that adopt secure practices and enable the new SIM to become a root of trust will empower IoT – as well as other sectors – with secure and flexible means to connect their devices with less friction and more choice than ever before.