ISSN 2634-9116

IoT Global Network

trending IoT 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.

SPONSORED BY
Kigen

Kigen

Kigen
MOST PROMISING TECHNOLOGY SOLUTION COMPANIES FOR TELECOM INDUSTRY 2021

Future Digital Awards

Gold Winner
IoT Security Innovation of the Year
Technology & Innovation Awards 2020

The future belongs to those **re-thinking the possibilities**

Security is the foundation of trust in our digital society. At Kigen, we are making eSIM and integrated SIM (iSIM) the cornerstone of security.

Take advantage of future-proof, flexible, hassle free eSIM and iSIM technology.

- Compact and code-efficient OS across SIM, eSIM and iSIM
- GSMA accredited remote SIM provisioning server solutions
- Extensive ecosystem of innovation and full range of services to support your success
- Green Transportation

For more information, visit kigen.com/solutions

Recognised as "Best IoT Security Innovation of the Year 2020" by FDA Awards.
Recognised by CIO Review as the Most Promising Technology Company for Telecoms in 2021.

Secure eSIM

Editor's introduction

Report

IoT Security

eSIM Developments

About Kigen: At Kigen, we are making the future of securing connectivity simple. As simple as can be. Together with our partners and customers, we are unlocking new opportunities as eSIM and the integrated SIM (iSIM) become the cornerstone of connected devices security. Our industry-leading SIM OS products enable over two billion SIMs. Our remote SIM provisioning and eSIM services drive this momentum further placing us amongst top 5 SIM vendors globally. Our global teams are guided by the vision of a world where every device can connect securely and reliably. For more information, go to kigen.com or tune into our **#futureofSIM** conversations on **@Kigen_Ltd** on Twitter and LinkedIn.

IoT Global Network Trending Tech covers technological & business developments for businesses. © Copyright WKM Ltd. All rights reserved. No part of this publication may be copied, stored, published or in any way reproduced without the prior written consent of the Publisher.

ISSN 2634-9116

Managing editor:
George Malim
Tel: +44 (0) 1225 319566
g.malim@wkm-global.com

Editorial director & publisher:
Jeremy Cowan
Tel: +44 (0) 1420 588638
j.cowan@wkm-global.com

Digital services director:
Nathalie Millar
Tel: +44 (0) 1732 808690
n.millar@wkm-global.com

Business development:
Cherisse Jameson
Tel: +44 7950 279368
c.jameson@wkm-global.com

Designer:
Jason Appleby
Ark Design Consultancy Ltd
Tel: +44 (0) 1787 881623

Published by:
WeKnow Media Ltd.
Suite 138, 80 Churchill Square,
Kings Hill, West Malling, Kent
ME19 4YU, UK
Tel: +44 (0) 1732 807410

CRIME NEVER SLEEPS AND NEITHER DOES IoT

New technologies always bring new risks and often an expanded threat surface so has eSIM done enough with the latest IoT SAFE initiative and moves to enable it as a secure element, asks George Malim?

George Malim
Tech Trends

It isn't news that IoT is threatened by cybercrime and that security is at the forefront of the minds of organisations that are deploying IoT devices and services. Secure approaches are multi-layered and extend from analytical software to security in the network and in the device. Software, policies, processes and analytics are all applied to create a trusted environment and the connection itself must also be secure.

When it comes to embedded SIMs (eSIM), the integral security of the traditional plastic SIM is partly eroded by the programmability, over-the-air update capability and the ability to make changes that are inherent to eSIMs. Traditional SIMs' security weakness was largely at the factory at the point of programming and through cloning or hacking. However, for most consumer devices installing spyware is a much more simple approach for the unscrupulous.

Only part of IoT will be focused on consumer devices and eSIM and integrated SIM (iSIM) should be viewed distinctly from smartphone SIMs of the future, even though these will be embedded too. At the same time the threat surface is expanding rapidly. **Nokia**'s 2020 Threat Intelligence Report, for example, uncovered that IoT devices made up approximately 33% of infected devices, up from 16% in 2019. The 2020 report findings are based on data aggregated from monitoring network ►

IoT Global Network
trendingiltech.

traffic on more than 150 million devices globally where Nokia's NetGuard Endpoint Security product is deployed. Also, the 2019 Threat Intelligence Report identified that 78% of total detected malware activity was due to IoT botnets.

This illustrates the scale of the IoT security challenge and it is one that substantial investment and attention is being devoted to as vendors and developers adopt secure by design practices. Research from analyst firm **IoT Analytics** has revealed that companies increased their spending on IoT security in 2020 by 40.3%. The firm attributes this surge in spending to the high-profile security attacks that have been widely reported. IoT cybersecurity incidents that were visible in the media, such as hacks of **Amazon**'s Ring cameras in late 2019, led to increased awareness of the need for better protection of IoT devices.

The firm has also found that 83% of information technology professionals implemented stronger cyber hygiene among employees during the pandemic and plan to continue prioritising the subject after COVID-19.

Further insight has been provided by recent **GSMA Intelligence** research which has revealed that enterprises are showing a growing appreciation of the role of IoT security in their digital transformation strategies. The report on enterprises' views of IoT security finds that 85% changed their security practices as a result of their IoT deployments. A significant number of these companies (61%) have done so to use their IoT security position as a unique selling point.

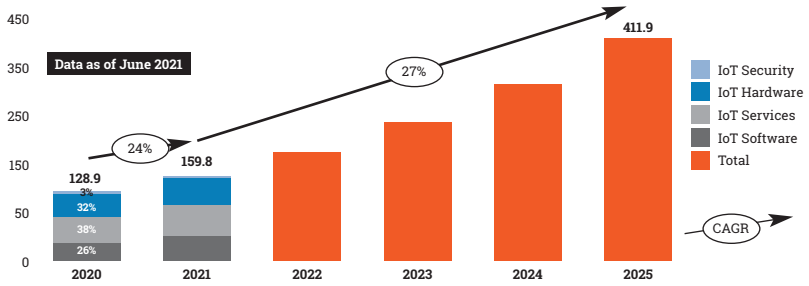
These indicators demonstrate the increased focus on securing IoT and also explain why significant effort has been devoted to securing eSIMs and GSMA has played an important role with its IoT Security Guidelines. These recommend utilising a root of trust or a hardware secure element to protect IoT data communications.

This has been formalised in the IoT SAFE initiative, which is detailed in this issue's analyst report, starting on page 6. IoT SAFE stands for stands for IoT SIM Applet For Secure End-2-End Communication and enables IoT device makers and service providers to utilise the SIM as a robust, scalable and standardised root of trust.

The SIM is well-suited to function as the hardware root of trust in an IoT device as it has advanced security and cryptographic features and is a fully standardised secure element, enabling interoperability across different vendors and consistent use by IoT device makers. IoT SAFE uses the SIM as a miniature

Figure 1: IoT Enterprise Spending 2020-2025

Global Spending on Enterprise IoT Technologies, in $B



Note: IoT Analytics defines IoT as a network of internet-enabled physical objects. Objects that become internet-enabled (IoT devices) typically interact via embedded systems and some form of network communications

crypto-safe inside the device to establish a secure transport layer security (TLS) session with a corresponding application cloud/server. It is compatible with all SIM form factors including embedded and integrated SIMs and also provides a common application programme interface (API) for the highly secure SIM to be used as a hardware root of trust by IoT devices.

In this way, IoT SAFE takes the most widely used end-to-end security protocol – TLS – and protects the credentials used to put it in place inside the device on the SIM, eSIM or secure element. Essentially, IoT SAFE enables the SIM to be used to be utilised as a root of trust, protecting both mobile network operators and the IoT devices they connect from cybercrime.

Additional benefits come in the form of seamless cloud connection with a zero-touch provisioning flow which allows massive scale cellular IoT connectivity because processes can be automated. IoT SAFE works in the same way regardless of the category of cellular communication involved and on any IP-connected devices that feature an eSIM or secure element.

Encouragingly, IoT SAFE is an example in which the whole ecosystem of IoT has come together. It encompasses chipset designers, module providers, eSIM and SIM providers, connectivity providers, software developers and IoT cloud service providers, all of which are already supporting IoT SAFE in their offerings.

An industry-wide initiative such as this provides a standardised method by which IoT device security can be enhanced and the connection itself protected. This should alleviate concerns and help to enable the hyperscale roll-outs of the next few years. Cyber crime never sleeps but, in this case, the IoT ecosystem has been putting in the hours to protect future development for all.

Research from analyst firm IoT Analytics has revealed that companies increased their spending on IoT security in 2020 by 40.3%

Matt Hatton
Transforma Insights

IoT Global Network
trendingiltech.
WHITEPAPER

The decisive opportunity for MNOs to be guardians of trust: Simplify IoT with eSIM

As well as reducing the cost and complexity of deploying IoT, embedded SIM can become the root of trust to deliver critical IoT applications relying on rich edge-to-cloud deployments, writes Matt Hatton, the founding partner of Transforma Insights ▸

SPONSORED REPORT

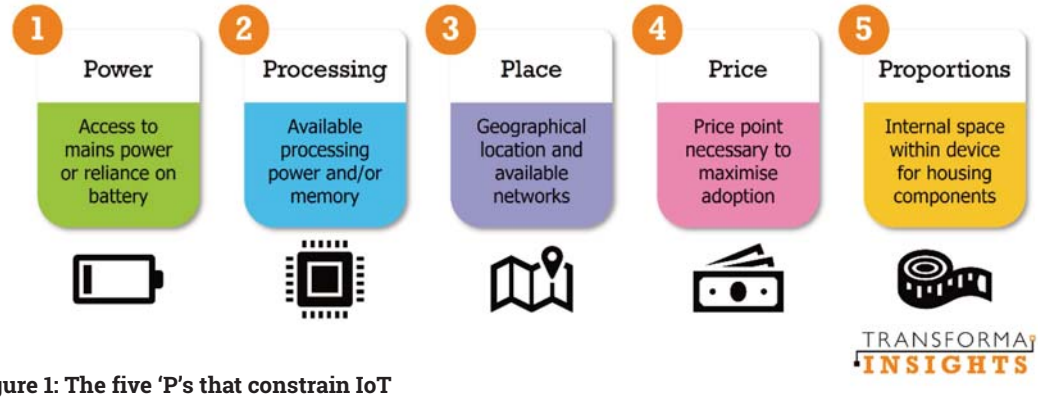


Figure 1: The five 'P's that constrain IoT
Source: Transforma Insights, 2021

Transforma Insights forecasts that by 2030 there will be 27.8 billion connected IoT devices, of which almost five billion will be connected using cellular technologies. Such market forecasts represent our best estimate of how the market will evolve. However, in such a fast-moving space, with rapidly changing technologies and business models, there are many potential developments that could accelerate, slow or alter the nature of the market evolution. Two contrasting developments define the state of IoT today: richer functionality and constrained environments. The balance between them will define the extent to which the market might exceed, or fall short of, those forecasts.

IoT's richer functionality and greater constraints

Firstly, we see increasingly rich functionality and capability aimed at deriving huge amounts of value from connected devices. Cloud and edge computing, machine learning, mobile private networks and 5G are just a few examples of richer functionality being applied to IoT. Furthermore, it is becoming increasingly evident that enterprises are using IoT for more critical systems, with the consequent requirement for more sophisticated features and capabilities, not to mention more robust security.

At the same time, an almost contradictory trend is occurring. IoT technologies are being rapidly refined to support applications deployed in highly constrained environments. Large volumes of connections must cope with limitations on, for instance, access to power, physical and cost limitations on componentry, and geographical remoteness limiting availability of networks. We refer to these constraints as the five Ps: power, processing, place, price and proportions.

The key to overcoming these constraints is in delivering what we at Transforma Insights term Thin IoT. This consists of, across each of five layers (device hardware, device software, networking, middleware, and edge computing and machine learning) an optimum set of technologies for supporting IoT in constrained environments. These include system-on-chip, chip-on-board, embedded operating systems such as TinyOS and RIOT, networking technologies such as message queuing telemetry transport (MQTT), constrained application protocol (CoAP), and low power wide area (LPWA) technologies, thin middleware, and data processing techniques such as tiny machine learning (TinyML). ►

Putting these two trends together places a strong requirement on the market to deliver cost- and energy-efficient solutions which are also capable of taking advantage of all the latest new technologies in order to deliver the optimum capabilities for the enterprise. One key technology which can greatly support both of these sets of demands, particularly as applied to cellular-based IoT, is embedded SIM (eSIM), all wrapped up with inherent trust.

eSIM/iSIM as a trusted enabler for IoT growth

The physical machine form factor (MFF2) embedded SIM has been available since 2016 and the ability for remote SIM provisioning (RSP) for several years before that, finally being standardised in 2016. Since then, the integrated SIM (iSIM) arrived in 2018 moving the SIM functionality to a secure location on silicon along with the application processor and radio, all implemented on the same system-on-a-chip hardware.

The new form factors mean cheaper, smaller and lower-powered devices, helping to address many of the constraints on IoT. Use of MFF2 chips is cheaper than the removable alternative, meaning the bill of materials will be directly reduced. Using iSIM will even further reduce the cost. Similarly, with a smaller footprint they also allow for smaller, lighter, devices with lower manufacturing and shipping costs – as well as probably a more appealing form factor, which might be important for some use cases. There are supply chain savings associated with being able to put the IoT device into field without needing to switch out the physical SIM card. The eSIM/iSIM will also have a longer lifespan, both because of being more robust – particularly in harsh environments of extreme temperatures and/or vibration – and also due to never needing to be swapped out. We should note, of course, that there is a cost associated with subscription management, but this is very modest in comparison to the cost savings that can be made.

The MFF2 devices, and iSIM even more so, also require lower power, for instance being able to awaken from power saving mode (PSM) to enact eSIM provisioning. For IoT solutions working in highly constrained environments, this can provide a significant benefit. It should be noted, however, that applications that are highly price- and power-sensitive may opt for narrowband IoT (NB-IoT) as the enabling technology, attracted by lower module costs, longer battery life and – probably – lower data charges. However, this can be incompatible with using remote SIM provisioning since it often relies on SMS, which isn't supported in lots of NB-IoT networks and devices. Mobile network operators (MNOs) should prioritise resolving this issue through the device management platform.

Embedded SIM is not just about cost and power savings, of course. It is also critical for enabling the richer set of IoT capabilities and the deeper integration of IoT into enterprise processes. As ▶

enterprises increasingly entrust their business-critical systems to IoT, two issues at which eSIM excels become increasingly important: security and device-to-cloud integration.

Cloud and edge computing are increasingly common features of IoT deployments. The migration of applications to the cloud has been happening for the last decade and will continue for the next. This has driven increasing interest from cloud hyperscalers, particularly **AWS** and **Microsoft**, in IoT. The moving of application logic to edge devices and the network edge to reduce latency and give more autonomy had created an increasingly complex environment where application logic, data and processing sit in multiple places, be it in the cloud data centre, the network edge, the gateway or the edge device itself. This complexity necessitates much greater consideration of how transport is secured end-to-end, from device to cloud server. Through the recent IoT SAFE initiative, the SIM can help to provide increased end-to-end security when connecting IoT devices to cloud services.

A further benefit of eSIM is its ability to future-proof technology choices in radio access networks. Today there is a patchwork of different technologies available, with NB-IoT, LTE-M and 5G being rolled out and 2G and 3G networks being gradually switched off. Remote subscription management significantly reduces the exposure to network sunsetting, by allowing connections to be switched across to alternative available ► networks.

What is IoT SAFE?

The IoT SIM Applet For secure End-to-end communication (IoT SAFE) is a mechanism for ensuring end-to-end security for IoT data flows, from chip to cloud. It establishes the SIM card as a hardware Root of Trust, a source that can always be trusted, storing private keys and certificates in a secure element (SE) that can be used to authenticate the end device and provide credentials for the IoT application. The SIM is the optimum place for this hardware root of trust. It is fully standardised, interoperable and highly secure. The SIM establishes a datagram transport layer security (DTLS) session with the other end point – typically a cloud server.

Transport layer security (TLS) refers to end-to-end security for data communication between end-points. A subset of that, which applies particularly to IoT, is DTLS, which specifies requirements related to data sent in a connectionless way so the sending device need not wait for the receiving device to be ready, will not seek confirmation that the packets have been received, and data packets need not be guaranteed delivery in a particular sequence or at a particular time. Most IoT applications rely on datagram-based technologies such as user datagram protocol (UDP). As a result of being connectionless, UDP is a lighter protocol requiring much less network resources and less processing on the device. Therefore, it is much better for constrained IoT devices.

Essentially, IoT SAFE is about applying to end-to-end transport of data a similarly high level of security that SIM brought to network access. Rather than just authenticating the SIM onto the network, this authenticates the IoT application into the cloud.

For more information visit: **https://www.gsma.com/iot/iot-safe/**

The arrival of eSIM and iSIM provides a valuable tool for addressing the challenges of the constraints under which IoT must work, at the same time as providing tools to better secure the much-needed device-to-cloud data stream.

Become guardians of trust in IoT

MNOs haven't been very active in embracing eSIM. Partly this is because of the relative immaturity of the systems, particularly anything more than simple initial bootstrapping and localisation of a device. Most of their reticence, though, stems from the complexity of implementing the system. It's quite straightforward to deploy the eSIM technology via the embedded universal integrated circuit card (eUICC), subscription manager data preparation (SM-DP) and subscription manager secure routing (SM-SR), although integrating with other MNO SM-SRs is a minor logistical hurdle. What is less simple is to manage the impact that eSIM has on other commercial and operational elements such as billing, customer care, inventory, device lifecycle management, legal, network planning and numerous other systems. The other reason for reticence is competitive: there is a persisting concern that allowing the switching of devices off the network is a competitive threat. Despite the MNOs' reservations, there is no escaping the fact that the future of cellular IoT is eSIM, and eventually iSIM. The cost and energy savings associated with using the technologies, as well as the increased redundancy provided by being able to switch operators, will mean that IoT adopters will demand eSIM/iSIM and MNOs and MVNOs will need to meet that demand. As cloud providers accelerate the expansion of their IoT capabilities, they will also demand the end-to-end security which is supported by IoT SAFE. There are also further benefits to MNOs in pushing the cost of SIM cards onto the hardware value chain.

MNOs have the opportunity to place a secure hardware element that they control into the device from day one and establish that as a root-of-trust for many aspects of the IoT application. This will deliver an additional layer of capability within cellular communications. It will also, through the standardised and interoperable transport layer security, provide the MNO with an additional critical role in supporting the deployment of high value secure IoT. If MNOs were reticent about eSIM, the ability to establish themselves as the guardians of trust in the IoT should make them think again.

What is critical for MNOs is to move relatively fast and in collaboration with fellow operators. Historically, there are many examples of ►

technologies where the operators should have been able to establish a strong position only for delayed and over-complicated solutions such as mobile payments or unified communications to be supplanted by more nimble alternatives such as **Apple Pay** or **Slack**. The track record of the mobile industry in inserting itself into vital growth areas is not particularly good. With eSIM and the hardware root-of-trust there is the opportunity to do so, particular where the MNO can exert influence over the hardware value chain to embed the functionality as early in the manufacturing process as possible.

Balance functionality with simplification

The key to accelerating the adoption of IoT is in balancing functionality with simplification. IoT solutions have always involved a lot of (sometimes literally) moving parts. Few technology disciplines have to deal with such a diverse range of technology fields, spanning hardware, software and connectivity. Over the last decade or so many developments have helped to simplify the process of deploying IoT; the platformisation of the software space being one good example. In other areas, things have become more complex, not least in the provision of wide area connectivity where a single dominant technology – general packet radio system (GPRS) – has given way to many including: GPRS, LTE, NB-IoT, LTE-M, 5G, LoRa, **Sigfox** and others. Beyond that, the arrival of edge computing and machine learning adds a further layer of complexity. Delivering IoT is a constant battle against complexity while at the same time harnessing the amazing technology tools that are available.

Initially, eSIM and iSIM may seem like further complications in how IoT is delivered. The reality is, however, that for adopters they represent a significant simplification, future-proofing vendor selection and streamlining supply chains. The use of the SIM as a root-of-trust also simplifies the inevitable requirement to integrate IoT data into cloud environments. Having that root-of-trust capability embedded in the device from day one removes one more complexity burden. The other big advantage with IoT SAFE is in the zero-touch provisioning to cloud services, again simplifying the process of integrating IoT.

MNOs can, with the benefit of eSIM, enhance the functionality delivered to customers of cellular IoT solutions, while at the same time simplifying adoption.

Report sponsor

Kigen

HOW TO SECURE IoT IN A 5G WORLD:

New approaches for innovation

5G promises to be a unified connectivity fabric that will connect virtually everything across our homes and businesses. This new generation of connectivity presents both opportunities and challenges for designing trusted services across diverse Internet of Things (IoT) requirements. Vincent Korstanje, the chief executive of Kigen, considers what is needed for a rich roadmap of system innovations across high reliability, device connectivity and cost. The bottom line is; security needs to be built in from the start

Cellular IoT's ubiquitous connectivity is a key draw for engineering innovations across fast-growing markets such as infrastructure for more intelligent transport, smart consumer services, smart city devices and connected health. The adoption of 5G is going to accelerate the deployment of these connected devices significantly. But as with most disruptive new technology waves, 5G brings its own challenges that require designers to consider how they support new radio bands while balancing not making IoT device design too complex. Increasingly, the devices in question are low power, long-lived in field, low cost, afford low levels of physical access, and are deployed across further and remote locations.

Cellular IoT has long been the choice of secure, large-scale and resilient deployments due to the robust subscriber identity module (SIM) that authenticates a device. As our devices shrink, and as remote devices must endure a wider range of environmental conditions, securing the device's identity requires new and broader solutions.
Every connected device will need to be updated at some point throughout its lifespan. One of the advantages of IoT devices is that they can receive software/firmware updates over the air (OTA). That said, the ability to only allow authorised updates is critical to ensuring the integrity of the device and code running on it.

Scale is both IoT's most significant opportunity and hurdle. Manufacturers need to consider how they will manage and secure the device throughout an extended lifecycle – in the case of cars and even consumer devices this includes an after-sales business model to support the ability to repair, replace owners or decommission securely to be more sustainable.

Take advantage of the evolution of SIM

Embedded SIM (eSIM) technology is still a hardware-based SIM, but this elegant, robust and scalable technology is soldered permanently into the device and was designed to address some of the challenges impeding true scalability in ▶

SPONSORED ARTICLE

Vincent Korstanje
Kigen

cellular IoT. eSIM allows devices to be deployed anywhere with existing cellular coverage; operator profiles or network providers can be updated over the air, based on standards that offer a frictionless experience for device manufacturers and service operators.

But there's more: an integrated SIM (iSIM) takes all the benefits of standards-compliant eSIM and embeds them into the device's permanent hardware array by combining the SIM with the system-on-a-chip (SOC) architecture and cellular modem. Fusing the secure locations into the chipset itself offers a low-footprint and introduces extra layers of security through a hardware-based secure enclave – a dedicated processor for security operations – that maintains the integrity of all cryptographic and key managed operations.

Security and scale go hand in hand

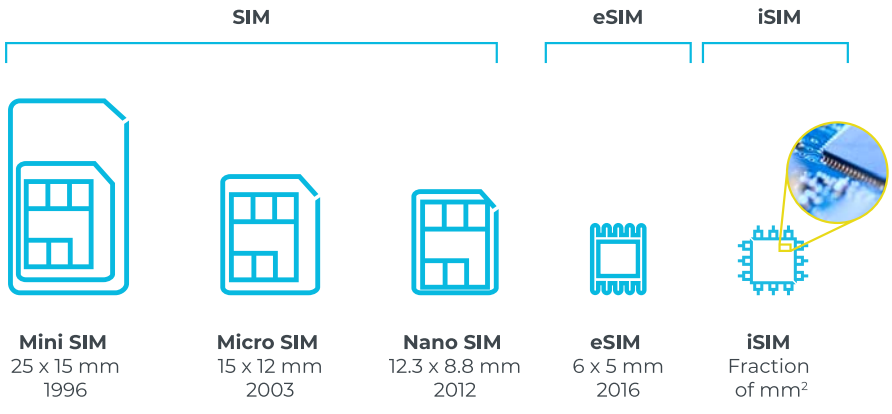
As the number of devices ramps up, the IoT attack vector will grow exponentially, and security cannot be an afterthought. IoT continues to move closer to core processes, and businesses should ensure that both devices – the endpoint itself – and data exchange, in technical terms, the chip-to-cloud security, have strong identity and trust foundations.

To achieve scale, businesses need simpler ways of manufacturing whilst being able to keep the robust security benefits derived from SIM capabilities. The fastest growth of eSIM and iSIM deployments is coming from markets that have not traditionally operated at the same cost points as cellular or smartphone industry. Markets such as fleet management of e-bikes or e-scooters or connected health wearables did not exist in their current capabilities a few years ago.

Within these, businesses need simplification of both the bill of materials and that of the supply chain. iSIM fundamentally changes the way device makers can access cellular capabilities for devices that could not be served before. iSIM offers the highest protection for subscription credentials and isolates processing in a secure enclave. An additional authentication layer serves as a root of trust for secure communications while reducing the bill of materials.

One of the often-overlooked elements of security design is how trust is granted to a device and managed throughout its lifecycle. While trust is relatively easy to manage within a trust manufacturing environment, it is much more difficult once that device leaves the factory floor.

The **GSMA** standard IoT SIM Applet For Secure End-2-End Communication (IoT-SAFE) iSIM supports the entire secure chip-to-cloud IoT infrastructure. A collaborative next step to this standard is the Open IoT SAFE principles, that allow a re-think of interoperability in order to deliver the promise of zero-touch provisioning. Using the most trusted internet protocols and iSIMs to authenticate both connectivity and application credentials for any data being exchanged with any cloud represents an opportunity for telecoms operators to win customer trust across any connection.



Evolution of the SIM

New opportunities

eSIM and iSIM are solutions to existing problems, but they also open up new opportunities for the broader innovations. Artificial intelligence (AI) and machine learning (ML) have an increasingly important role to play in the IoT. The **Economist Intelligence Unit** reported in 2020 that 90% of companies with extensive IoT deployments link their real-time data gathering with their AI planning. Companies with mature deployments can justify the traditionally high cost of incorporating AI and ML, as they had a demonstrable return on investment (ROI) from an existing deployment.

Luckily, that barrier to entry is being lowered today and we're seeing the cost of utilising these tools falling, broadening the types of diversity of devices that can be intelligent nodes across low-power wide area networks working together with mainstream 5G networks. Massive IoT will support the mainstay applications that we have come to envision 5G with such as cellular-to-vehicle-to-everything (C-V2X).

The opportunities presented by cellular IoT, underpinned by 5G are abundant. Herein is represented an unprecedented opportunity for collaboration across manufacturing, engineering, commerce and technology providers to ensure the 5G digital economy has security as it's cornerstone.

www.kigen.com

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." ▶

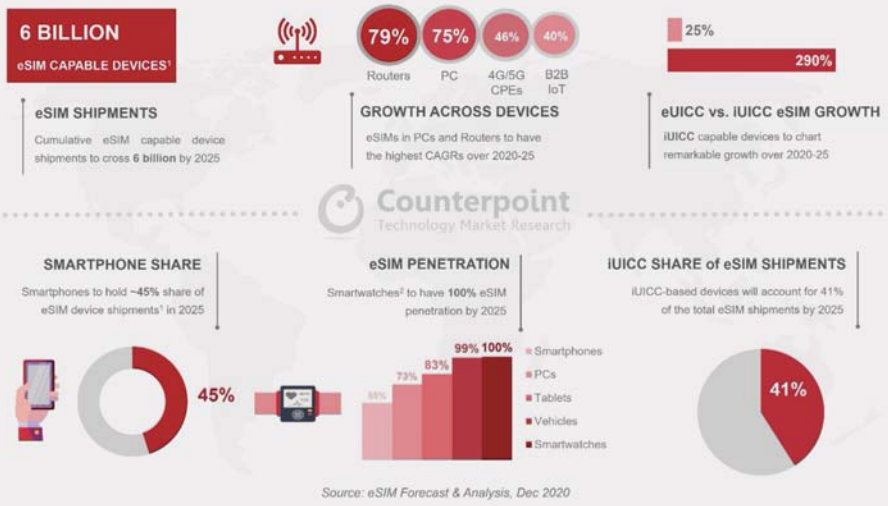
Commenting on eSIM penetration, Counterpoint's research vice president Neil Shah said: "Smartwatch-makers have been increasingly adding cellular connectivity for varied use-cases, from health monitoring and safety tracking to making them standalone companion devices. eSIM is a natural fit here from the 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."

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."

Figure 1: Counterpoint Research's Key eSIM Insights Dashboard



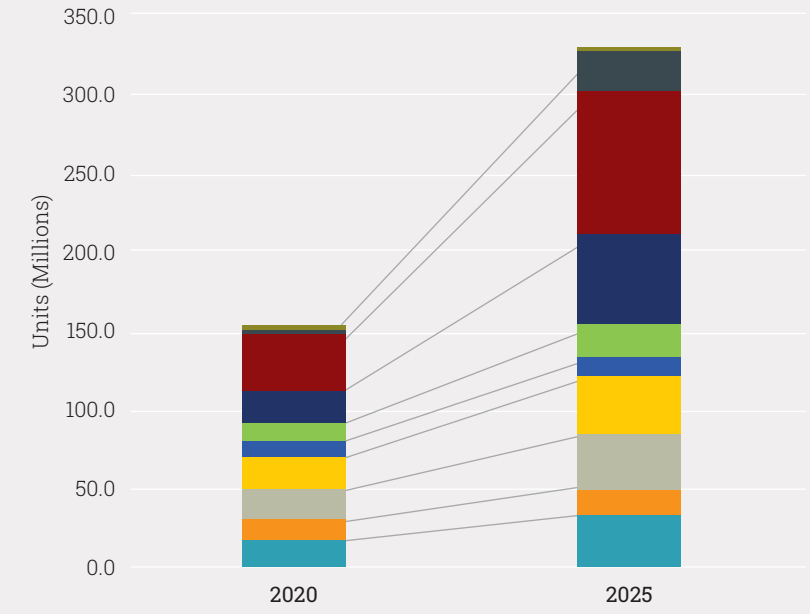
Awareness meets appetite

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

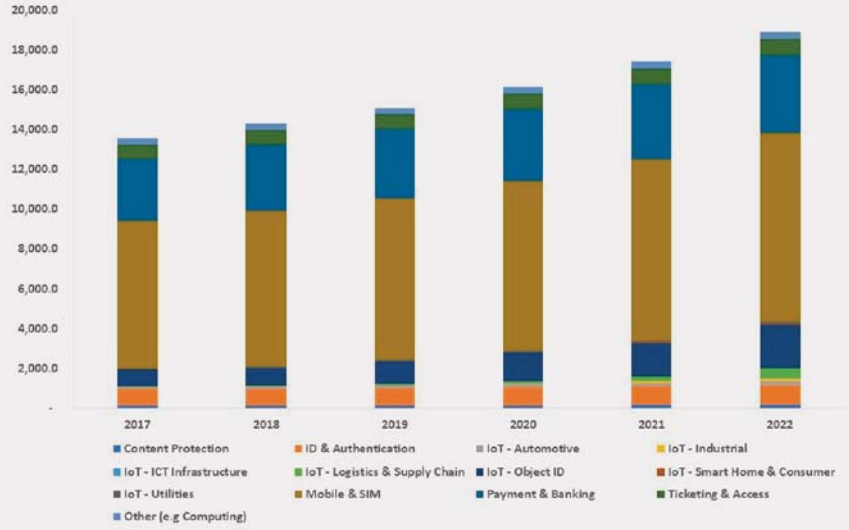
Traditional credentials, such as smart cards, will continue to account for the majority of market volume although the ability to create, access and share digital credentials, plus securing connected devices, will drive adoption of higher value solutions. Demand is set to increase to 18.8 billion units 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.

Kigen

Supercharging towards secure and trusted IoT

The present day IoT is complicated and fragmented. **We can do better.**

Kigen's Open IoT SAFE Manifesto guides enterprises, Telcos and connectivity service providers to supercharge open, end-to-end IoT security for any data cloud.

Download your copy:
kigen.com/open-iot-safe-manifesto