eSIM's secure element underpins data integrity for the mass-scale, AI-enabled next generation of cellular IoT

The mass-market success of cellular IoT has been delayed partly by the constraints of utilising cellular networks that were designed to support the communications of consumers rather than the connectivity needs of connected devices, sensors and vehicles. Now though, a new wave of cellular networks designed with IoT mind are coming to market addressing high energy-efficiency use cases with optimised cellular connectivity. This provides greater choice for organisations deploying cellular IoT devices but also keeps them and their data protected thanks to the continuation of carrier-grade security provision for new networks and for enabling technologies, such as embedded SIM.

With the security stakes rising as AI-enabled services start to emerge, even heavier reliance is being placed on assured device identity and data integrity Vincent Korstanje, the chief executive of Kigen, tells George Malim

George Malim: 2024 looks to be the year that cellular IoT growth accelerates rapidly, beyond the dominance of the automotive industry and into a wide variety of industries. What do you see becoming mass-market in cellular IoT this year?

Vincent Korstanje: Indeed, as we embark on 2024, the early indicators are very promising – something industry experts and analysts have been forecasting. At **Kigen**, we champion the original equipment manufacturers (OEM) and device makers, which gives us the pulse of the adoption of cellular IoT – and momentum, especially driven by eSIM, is tremendous. There are multiple mass-market industries already, but I think the change is that the cellular IoT sector is now ready to support an industry that can come in and add hundreds of millions of connections. All of that won't happen overnight but I can see NB-IoT and Cat-1 bis helping customers to break into mass markets quickly.

The move into connecting shipping labels and smart trackers is already underway and accelerating. This is due to the desire by shipping giants to have real-time visibility or nationwide transformation programmes such as the AIS-140 regulation for passenger safety in India, all amounting to applications in logistics to be a mass growth area.

Also, devices like smart meters are moving to cellular connectivity in huge numbers. This type of deployment has become more attractive where cellular IoT is far more effective than other technologies such as when assets are remote and costly to access in large numbers, and IoT has quick payback.

We're also seeing use cases such as the monitoring of industrial or domestic solar power generation becoming increasingly popular. When you are considering connected assets that are integral to national infrastructure, securing connectivity is essential for the outcomes – in this case, optimised production. Across many connected campuses, airports and other sites, we see micromobility drive growth: particularly, think delivery robots! We share a case study later in this issue, on how private and public networks support a vast range of connected services in such environments. ▶

GM: How do you see Kigen's role in OEMs to achieve mass market success?

VK: I think there's a fundamental shift happening because of embedded SIM (eSIM). eSIM is changing the IoT industry because the OEM can determine connectivity when the device is either constructed or shipped. This means that in contrast to changing the SIM at the point of deployment and adding connectivity later, the eSIM enables connectivity decisions to happen earlier. That can be good and bad, depending on the deployment type.

It's good because the eSIM enables a smaller form factor within the device, which allows greater design flexibility and, of course, a smaller overall size and weight. This is appealing for OEMs. If you consider a smart meter maker looking to create a product for the world, moving to soldered eSIM enables more straightforward sourcing: they don't have to negotiate separate connectivity from different operators, each with their own minimum order quantity and requirements. Plus, the embedded hardware and the connectivity ▶

A connectivity profile is often something that can be set at that last stage of manufacture

profile make a unique stock-keeping unit (SKU), which would need to be maintained for each. This can be cumbersome and not suited to production setups for scaled manufacturing.

A connectivity profile is often something that can be set at that last stage of manufacture. So, instead of having 20 or 30 versions, you can achieve just-in-time provisioning of the right connectivity profile on the manufacturing line itself, which enables the device to bind with a cellular network before the smart meter is shipped into the field.

Of course, the final deployment is not the only time a device needs to connect. For example, an eSIM might contain secure elements from a German manufacturer such as **Infineon**; in another scenario, it could be **Samsung** in South Korea. Their module is selected from **Murata** in Japan, so the secure elements must be shipped to Japan, and then the module is sent to the ODM or OEM in Taiwan. In these three stages, the product is tested – so once in Germany, Japan and Taiwan. It may then be sent back to Europe or the US, where it is deployed into a tracker on a car, which might move between borders.

There might be four, five or six times an eSIM needs to connect in different regions during the manufacturing to deployment process, and that's something that secure in-factory provisioning can help with to ensure connectivity works for the whole supply chain. At Kigen, we hear positive feedback from our OEM customers on our focus to bring this critical missing piece in eSIM adoption at the mega scale.

Vincent Korstanje
Kigen

GM: Power consumption is still a critical part of the cost vs lifespan vs form factor equation that every device has to go through. How can battery life be conserved and maximised from manufacturing onwards?

VK: Power efficiency and optimisation have been a mainstay of innovation in IoT device design. This affects cost majorly across the overall lifespan – the total cost of ownership, and hence is a critical requirement. For example, in metering, the devices are designed for low data rates and with very low power NB-IoT connectivity but need to operate effectively for a minimum period of ten years on a single battery charge. So, simply downloading a new connectivity profile, which can reduce useable life when the device is in the field might not be in your best interest. This risk can be minimised by installing device profiles in the factory before it ships and can be enabled in the field. Enabling a profile is a much smaller operation that doesn't involve radio as much, so power consumption is much lower.

GM: Cellular connectivity is not the only option for IoT deployments. Why do you expect volumes to grow substantially?

VK: There are several dynamics to consider. Cellular technologies used to be confined to 2G, 3G, 4G and 5G – where available – but now, the range encompasses a wider variety of low power wide area network (LPWAN) options, developed with IoT use cases in mind. These are a much better fit for cost, power, and network performance with IoT use cases than adaptations of cellular network technologies initially developed for consumer communications.

Increasingly now, there is an appropriate cellular technology for each IoT deployment, and the choice extends from made-for-IoT technologies such as narrowband-IoT and 5G RedCap to IoT-appropriate offerings such as LTE Cat1 bis. Of course, there are also standard LTE, LTE-Advanced, 5G standalone, and non-standalone to consider as 2G and 3G networks sunset. These options mean there is less need to over-specify cellular performance, and cost can be controlled.

These in combination with the Kigen secure OS products for eSIM and iSIM, you start achieving energy-efficiency with the benefits of robust security in a similar ballpark as other connectivity options. With a radio chip now coming down to perhaps US$7 or US$8 the comparison to a Wi-Fi chip at US$5 is narrowing. A washing machine company could install its own cellular chip to communicate data, assuming data protection compliance, without needing the customer's Wi-Fi connectivity. The business case for IoT is also now well established, so whether you are considering a connected product line of washing machines, one of the world's largest solar power generation plants, or a connected airport – cellular is far more in consideration than ever before due to the cost being on par.

Further, the cellular market has changed a lot, and it is no longer in isolation. It's likely that water ▶

eSIMs are a really good security asset that can be used for other things, such as verifying device identity, and to sign data coming off any IoT device. In the world of AI, security is a must

meters that use NB-IoT, for example, will also link to non-terrestrial networks (NTNs) to gain satellite connectivity in areas where there is no coverage.

And with eSIM technology, it is getting much simpler for OEMs as we just talked about. This year we see the SGP.31/32 specifications formalise, which has created great excitement and demand from OEMs. Traditionally, cellular product development timelines were far longer, the time needed to invest in contracts and certification of your module or SoC. Kigen has taken this unique position in the market to bring semiconductor, module, and chipset vendors and connectivity partners to build a more agile, faster path to market. Now, OEMs can come to Kigen and request to access eSIM and iSIM with their chosen MNO profile such as **AT&T**, and then work directly with their major operator and transfer their subscriptions to their existing operator relationship. This ecosystem approach creates shared value (which we continue to build on from our origin in **Arm Holdings**), and also contributes to greater confidence from OEMs that are new to cellular, growing the overall sector.

So all of these put together bring new options to market with great flexibility and, in turn, help to drive the volume substantially.

GM: How do you see the arrival of SGP.32-ready devices helping increase flexibility and broaden the appeal of cellular IoT?

VK: What's important about SGP.32 is that it starts to bring the consumer specification's ease for IoT deployments. That's interesting because the old M2M specification has several challenges, one of which is the management of devices had to be done in a GSMA-certified location. This would typically be restricted to the site of a SIM supplier or by the mobile network operator. Secondly, although interoperability between the players was there in theory, it wasn't working in practice for OEMs. A lot of effort was required to make it work well. So, the new eSIM specifications have aimed to solve specific, real-world challenges.

SGP.32 has the potential to enhance interoperability – so more devices work on more cellular networks, and with more third-party technologies. It's about the ability to take control of your devices and make sure they have the right connectivity provider for your use case. That might be an e-scooter provider doing a new deal in Paris and choosing to move its scooters over to **Orange** connectivity or it could be that a device realises it's going into the desert and it needs to switch to satellite connectivity. With SGP.32, the market will be able to manage fleets of connected vehicles in a more streamlined way to optimise their connectivity. We anticipate this would be a positive development to broaden the appeal and are focused on creating easy transitions for OEMs – with our first solution with SGP.32-ready features announced with **TEAL** in January 2024. We are always eager to learn from customers what we can do, for them to be future-ready.

GM: Having management control and the secure element are two key steps to ensuring the performance of connected devices. That is essential to enable use cases that demand data is monitored and that are used to fuel artificial intelligence, machine learning and greater automation. How important is the ability to assure data integrity becoming?

VK: The integrity of the data is indeed a foundation for the future. AI is garnering a lot of OEM attention because generative AI is shaking up the world. At some point, it will run out of data to take in because the English language – and other languages – are only so big. Fundamentally, that means at some point quite soon, AI will need to take in new data and data from new use cases becomes particularly interesting.

AI is currently summarising papers but at some point, it will be advising us then it will be assisting us. If you think about connected cars, it is already assisting us. Then, it will take decisions and for that, it really needs data that we can be sure nobody has tampered with. Where does that data come from? Initially, it comes from reading the internet, but soon it comes from those sensors such as smart meters out in the grid or vehicle sensors.

Those sensor networks and sensor data better be secure, which is why secure element enabled eSIMs and iSIMs are so important. eSIMs are a really good security asset that can be used for other things, such as verifying device identity, and to sign data coming off any IoT device. In the world of AI, security is a must. There is a lot of hype and concern around the fast evolving potential of AI and so it can be daunting to know where to start. To help companies, I have penned an approach which I hope will assist anyone looking at making most of greater automation, machine learning and AI.

With eSIM in cellular IoT, we are designing that security into use cases to ensure the device identity is trusted and also that the integrity of the data it communicates is assured. That's a compelling advantage for the use cases of the very near future - whether they are AI-enabled or not. ■

www.kigen.com

eSIM services on private networks redefine connected mobility

IoT Now highlights how 5G IoT technology is playing a role in creating new opportunities for connectivity providers, device manufacturers and enterprises in 2024. Kigen shares how security and trust unlock next-generation experiences and what's important to know now

Embedded SIMs (eSIMs) can support cost-savings with further advantages in managing device fleets across enterprise devices. By bringing the improved ease and experience of connectivity profile distribution of Consumer eSIM to IoT, the new specification in SGP.32 also supports other services that redefine secure connectivity. Take the example of connected aviation.

- 190 million passengers will travel internationally through Beijing's new Daxing International Airport, within the 40 day Lunar New Year Spring Festival[1]
- 500% predicted growth for the travel eSIM retail market between 2023 and 2028 as leisure and business travellers embrace eSIM travel plans[2]

The challenge

Large airports serving regional flight hubs are small cities. For example, Charles De Gaulle airport in Paris employs more than 230,000 professionals, who may use connected services to improve the traveller experience, such as passenger hospitality or transit of cargo and people, while maintaining ambitious goals for the airport to be more sustainable and more innovative.

Connected assets
Sensors, enabled by secure network connectivity, deployed on physical assets to collect and transmit usage and location data for real-time scheduling and dynamic coordination across authorities, tenants and passenger services.

Connected operations
Replacing obsolete siloed technologies, airports are expanding the use of autonomous vehicles and robots in airports. These in turn depend heavily on the availability of secure, eSIM-secured low-latency networks.

Maximising security
There is a need to separate operational and passenger usage and traffic among networks, essential for security, safety and privacy reasons.

Planning for the future
Airport operators require complete visibility and control over their wireless infrastructure – from planning and deployment to operations and upgrades.

The solution

Private networks with **Kigen**'s extensive ecosystem of leading connectivity providers, with Kigen's Remote SIM Provisioning secure services and enablement suite, simplify digitalisation for an airport that never rests. Combining and augmenting an increasing number of innovative connected services and devices with added intelligence, all supported by security in multiple forms, 5G IoT is helping shape the future of aviation.

The connected airport is a far more familiar scenario than other connected functional arenas such as campuses, stadiums, oil and gas fields or mining sites, which also benefit from this solution.

www.kigen.com

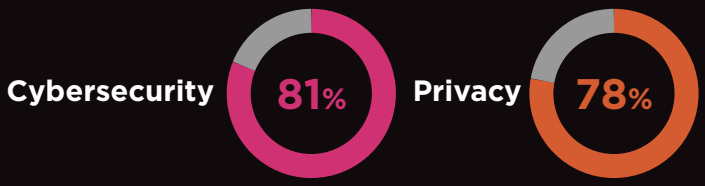
[1] Ministry of Transport and Tourism of China, Jan 2024
[2] Kaleido Intelligence Research, Oct 2023

SPONSORED CASE STUDY

Are AI ecosystems agents of disruption?

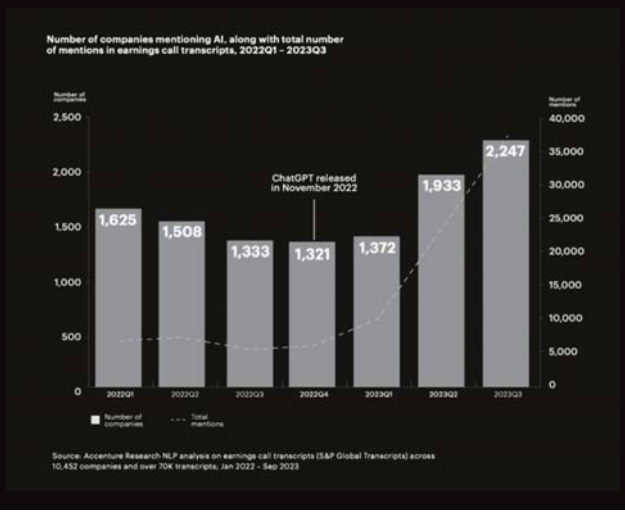
When ChatGPT directed global attention to the transformative potential of artificial intelligence (AI), it marked a pivotal moment in technology history: It moved AI from the minds of a few thousand scientists to 100 million people and 50 languages. That rate of growth and proliferation of technology is one we have never seen before. There is much speculation and debate on how it will impact the future of practically every industry. Navigating this hype with some pragmatic steps to win with AI is possible, writes Vincent Korstanje, the CEO of Kigen

Top-of-mind Gen AI concerns for IT leaders



Can AI have your attention

The number of mentions of AI in earnings call transcripts has increased by 6x since the release of ChatGPT in November 2022.



- 97% of global executives agree AI foundation models will enable connections across data types, revolutionising where and how AI is used in their own organisations[1]
- 6x increase in the mentions of AI in earnings call transcripts since the release of ChatGPT in November 2022[2]

The large language models (LLMs) behind ChatGPT, Bard and others mark a significant turning point for machine intelligence with two key developments:

1. AI finally grasped the intent and language complexity that is fundamental to human communication – for the first time, machines can express answers, bring up context and can be independently generative.
2. Using the vast amount of training data in rich text, video, lyrics and image formats, AI can now adapt to wide range of tasks, and can be repurposed or reused in various forms.

The ability of these LLMs to follow instructions, perform high-level reasoning, and generate code, will overturn the enterprise data, analytics and app marketplace: This is a disruptive opportunity for device makers.

LLMs are built and trained on huge amounts of data – ChatGPT, for example, was trained on a massive corpus of text data, around 570GB of datasets[3], including web pages, books and other sources. It will exhaust the available written text and articles at some point in the foreseeable future and will have to rely on verifiable real-life data. Sensor-driven data is essential for this and would be the most potent way to sense, verify and add to the integrity of the data that AI inferences are based on.

At **Kigen**, we have been talking about machine learning applications applications for several years[4], and the fact that LLMs can now be run on readily available computing platforms such as Raspberry Pi is encouraging. As AI capabilities propel forward, we may see them co-exist and collaborate through ecosystems to offer personalised user experiences. In this interlinked context, where AI agents aid or take actions on behalf of users, it is paramount that the data exchanges are secure — all the way from on-device sensors, processors and cloud — wherever that may be appropriately used.

On-device AI is another fast-emerging development – Increased compute power, more efficient hardware, and robust software, as well as an explosion in sensor data from the Internet of Things — are enabling AI to process data on devices that have direct user contact rather than piping everything to the cloud, which can carry privacy and security risks. Such on-device AI capabilities open new ways to personalise experiences.

However, according to a **KPMG** survey[5], cybersecurity and privacy remain top of mind concerns around AI for IT leaders. So, how do you move forward? The answer is start with what you can control: invest in secure-by-design sensors and IoT devices and integrate security end-to-end. One simple implementation of this that spans from the most constrained and simplest sensor to any edge device and cloud is Kigen's IoTSAFE based on GSMA standards.

The greatest risk associated with using GenAI is a loss of data confidentiality and integrity from inputting sensitive data into the AI system or using unverified outputs from it. For OEMs looking to be leaders in this space, integrating security into their sensors, devices and through the tech stack is a must.

In the age of AI, security is not just a feature, it is a necessity.

www.kigen.com

[1] Accenture Technology Vision 2023
[2] Accenture research NLP analysis on earnings call transcript (S&P Global transcripts) across 10,452 companies and over 70k transcripts Jan 2022-Sep 2023
[3] Aparna Iyer, analyticsindiamag.com, 2022
[4] https://kigen.com/resources/watch-now/isim-and-ml-iot-edge/
[5] KPMG survey, 2023

SPONSORED ARTICLE

360° VIEW OF YOUR ASSETS WITH eSIM

On the fast track

As the industry's unrivalled forerunner in power-efficient IoT, Kigen secure eSIM OS and Remote SIM Provisioning Solutions empower you to serve the growth in next billion connections. Scale with ease and monetise IoT faster.

- *Solutions compliant to GSMA SGP.31/.32*
- *Highest quality LPWAN and NTN connectivity ecosystem*
- *Late-stage device provisioning in the factory*
- *Chip-to-cloud security for trusted data services*

Kigen invites you to discover what's possible together, with eSIM.

For more, visit kigen.com/esim

Kigen

Let's meet

#FutureofSIM