Kigen

Open IoT SAFE Manifesto

Principles of open, zero-trust architecture serving enterprises and IoT Service Providers at the forefront of charting the secure connected future.

2021

Supercharging towards billions of secure and trusted IoT devices

Contents:

The essential concepts;

Zero-touch provisioning: Zero-touch provisioning is permitting fast configuration of new devices, and their enrolment to cloud services.

Transport Layer Security or TLS: Familiar with the padlock preceding the 'https://...' denoting that your browser activity is secure? That is due to a digital file used as a certificate to establish identity and trust between two parties on the internet. It's counterpart, Datagram Transport Layer Security or DTLS, is used for latency sensitive applications as its UDP based while TLS is TCP based. This means that DTLS is better suited to devices communicating across constrained (LPWAN) networks.

GSMA IoT SAFE: In order to bring well established authentication and verification models from mobile networks and (e)SIMs to ease network access for the diversity of IoT devices, the GSMA IoT SAFE sets the standard for robust, effective and scalable IoT security for OEMs and IoT service providers. IoT SAFE can be used to secure both TLS and DTLS communications.

Open IoT SAFE: Additional principles to GSMA IoT SAFE for open, zero-trust architecture that serve enterprises and IoT Service Providers to improve ease of integration to enterprise cloud instances whilst simplifying provisioning and enhancing end-to-end security.

Unlocking new frontiers with end-to-end security

At Kigen, we are proud to help technology pioneers who are driving breakthroughs for their customers and realizing their promises. Our teams and our partnerships are guided by a common maxim: “What if knowing your device is trustworthy and secure is as simple as switching it on?” What possibilities would trusted services bring to bear for industries and ultimately the billions of users who rely upon them?

We stand at a watershed moment for IoT. The thousands of businesses across six continents that our partners enable using our products, together with global IoT data and services, represent tremendous opportunities for our future. Yet, ‘global IoT’ is by no means a trivial exercise for businesses undertaking digital transformation to better serve their markets. For even the most resourceful of businesses, the manufacturing, securing, integration and operations of IoT goods and services presents challenges at every stage.

Launching a connected device that can be manufactured in one place, and deployed to simply work out of the box anywhere in the world, means that every OEM must develop capabilities that would traditionally rival an MVNO. As these lines blur, we need more ways to support device makers and solution providers accelerate to scale seamlessly.

Secure communications on the internet are built around Transport Layer Security (TLS) which provides end-to-end encryption and is usually denoted by a padlock in a browser. Often the credentials needed to establish this TLS layer are stored in insecure locations in IoT devices. Kigen’s response to simplifying global deployment starts with evolving the humble SIM, which has offered a secure, tamper-resistant store for network access credentials and become the de-facto standard for two factor authentication. eSIM, and it’s on system-on-chip integrated form-factor called iSIM, are the ideal identity stores that form a secure foundation for all connected devices. The eSIM is a significant improvement upon the SIM, as it forms a certificate-based security chain that begins at the production of the device, and is remotely manageable allowing provisioning or updating of both credentials and server certificate(s).

The complexity and fragmentation in present-day IoT are huge barriers to adoption. Device makers are operating in an ecosystem where there are many operating systems, chipsets, connectivity modules, clouds, plus many connectivity choices. There are infinite combinations of these elements which cause most devices to be custom-built for a given use-case, and this, in turn, is slowing down mass adoption.

So, what does an appropriate security solution look like, and how do we make our approach consistent and universal? How do we avoid the complexity of many-to-many integrations between ecosystem players to create a secure ecosystem?

To cut through all of this, Kigen is working on a holistic approach to instil trust from chip to cloud. Kigen’s goal in helping design such an approach has always been to extend the scalability of the solution by building upon the collaborative efforts already set in motion through the GSMA IoT SAFE programme. Taking some of the internet’s most robust and hardened protocols, our approach around Open IoT SAFE centres on the enterprise who needs smooth interoperability and a connectivity-agnostic approach with multi-vendor compatibility and growth for the future without compromise.

“Our hope is that with these principles and our connectivity-agnostic approach, we can ease your path to scale smart goods and digital services for a secure, connected future..”

Vincent Korstanje, CEO, Kigen.

An open architecture for securing Digital Transformation, at scale

In a 2020 GSMA intelligence survey of 2,873 global companies covering various geographies, industry verticals, roles, and company sizes, we discovered that 98% of IoT decision makers see data protection from device-to-cloud as important. Indeed, the confidentiality, integrity and reliability of data being collected is of paramount importance.

Enterprises haven't had ready access to a secure enclave in connected devices, where they can store their credentials used to protect their data from device-to-cloud. Enterprise data protection has been treated as less important than protecting the radio layer from eavesdropping, and from subscription fraud. This was because of the lack of an open standard that leverages readily available hardware, combined with the cost constraints that exist in the IoT space.

To summarise, enterprises want:

- Simple integration to existing systems or preferred vendors
- Consistent and universal availability
- Consistent secure communications with devices across Non-Cellular and Cellular IoT networks
- Tamper-resistant storage to protect their credentials
- Security that can cope with constrained LPWAN networks such as NB-IoT, LTE CAT-M and 5G NR Light once available
- Off-the-shelf devices that don't require complex key injection processes along the manufacturing or logistics chains
- Simple deployment, open protocols and solutions that are based upon open industry standards
- GSMA and security compliances

How can we remove the rigmarole of pre-loading credentials for a given cloud into a custom-built device at the point of manufacture and make the process of provisioning credentials into the IoT device as innovative as the solutions the IoT delivers? Do we really need an "IT department" in the manufacturing, supply, or logistics chains? A device is not just being onboarded to a given cloud, but to a given enterprise-account on that given cloud. This is so that the enterprise has the option to own and manage *their own* authentication and end-to-end encryption credentials.

So far, we have seen initiatives to combine network authentication and application security albeit, in a proprietary approach or requiring complex many-to-many integrations, creating many private systems. This has increased fragmentation and is therefore preventing scale. To further improve the ease of deployment of solutions building upon IoT SAFE, Kigen has conceived the Open IoT SAFE initiative by combining GSMA IoT SAFE with IETF Enrolment over Secure Transport (RFC 7030). By doing so, we're combining two important technical principles:

Firstly, exclusive use of the standard, (D)TLS-secured, IP channel to exchange with the cloud's on-boarding service over a secure interface thanks to credentials securely injected during device manufacturing.

This avoids interconnecting many clouds to numerous SIM or Secure Element trusted service or Over-the-air management platforms. This eliminates the resulting complexity and effort of integration by each party wishing to use the service.

And the second principle is the use of on-board key generation, meaning that we can generate operational, enterprise credentials, directly inside the device which remain in the secure, tamper-resistant element. Enterprises can then use these brand-new credentials, to secure future exchanges with *their own* account in their cloud of choice, utilising best in class security practices.

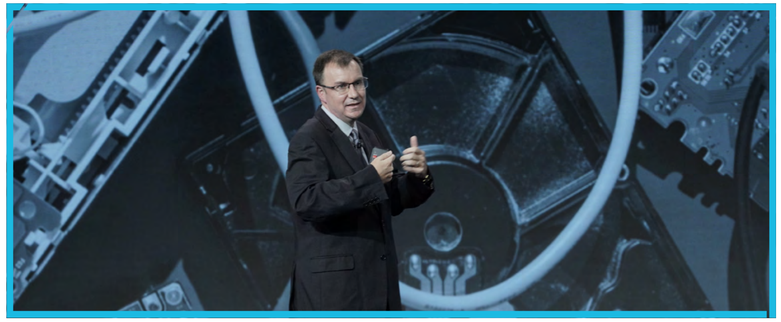
In combination, these result in:

- ANY device should be able to exchange
- ANY data across
- ANY network

And securely exchange that data with a given enterprise account on....

- ANY cloud

This is a future which we can all look forward to.



Paul Bradley, Director of Strategy and Innovation, Kigen.

> "It is vital for the trustworthiness of the Internet of Things (IoT) that we take a secure-by-design approach by properly protecting and processing the credentials used to secure data exchange between the IoT device and the cloud. Otherwise, enterprises will not be able to rely on the quality, accuracy or integrity of the data being collected, rendering it useless or even worse, dangerous."
>
> **Ian Pannell**, Chief Engineer, GSMA

Open IoT SAFE Manifesto

Benefits of open, zero-trust architecture serving enterprises and IoT Service Providers

Simple, unified **zero-touch provisioning**

Treating enterprise security credentials with the same level of security as mobile network credentials, by **leveraging tamper-resistant hardware**

Removing barriers to access hardware-based security to better protect credentials

Using open systems, based upon standards and without complex integration

What to do next?

Much like zero-touch provisioning, your next step should be frictionless. Here are some considerations to factor into your next steps:

1. Review your supply chain. We recommend you inject a root of trust into your devices as early as possible, even if it means an initial change to the supply chain. Work alongside security IP providers and their manufacturers to determine a best approach. Kigen's flexible approach ensures the manufacturing process accommodates changes at the cellular or device maker stage in the supply chain.

2. Rethink interoperability. The principles within Open IoT SAFE are not limited to cellular-connected devices but can also be implemented on any devices supporting a secure element and connected to the internet via Wi-Fi, Bluetooth, or any IP connection. Additionally, IoT system architects, device designers, and application developers do not need to select vendor-specific security solutions, or to implement ad-hoc mechanisms to secure device authentication and connection to an IoT cloud application. IoT SAFE ensures the security measures will be executed as a background, invisible task thanks to low level integration with major TLS stacks, rendering them IoT SAFE compatible.

3. Hardware choices for better data security. IoT devices typically have multiple TLS stacks. IoT application developers should follow best practices for storing credentials within tamper-resistant secure elements or eSIM/integrated SIM. Most modern mobile phones have eSIMs and secure elements, and spurred by Google's announcement of the **Android Ready SE Alliance**, the approach is gaining adoption across new use cases in smartwatches, smart home and automotive.

4. Leverage ecosystems. The Open IoT SAFE ecosystem is growing fast. We're already working with a broad range of module providers, integrators and middleware providers committed to interoperability and implementing support for the standard as part of Kigen's ecosystem. Speak to our teams of experts to find connectivity partners who are seamlessly enrolling and onboarding devices, helping businesses aiming for massive IoT.

10
Chipset and module providers

7
Integrators and middleware providers

3
Major clouds

50k
Enterprise customers

100m
Devices under management

We hope the approaches and thinking we put forward here can accelerate your success.
Interested in scaling your end-to-end secure IoT? Learn more or share further on **kigen.com/open-iot-safe**

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 (integrated) eSIM becomes the cornerstone of connected devices security. Our industry-leading SIM OS products enable over 2 billion SIMs. Our remote SIM provisioning and eSIM services drive this momentum further placing us amongst top 5 SIM vendors globally. Our 135 employees globally are guided by the vision of a world where every device can connect securely and reliably. For more information, go to **kigen.com** or speak to us on **@Kigen_Ltd** on Twitter and LinkedIn about **#futureofSIM**.

Kigen Ltd

linkedin.com/company/kigen

@Kigen_Ltd

kigen.com/contact/