ZARIOT
CONNECTED. PROTECTED.

The @ Company

Kigen

Flipping the Internet of Things

Using the power of the SIM for data privacy in IoT

End to End Encryption for Cellular IoT Devices

Simple, Efficient Privacy & Security for the Holistic IoT Solution

Who?

For IoT device manufacturers, solution owners, and systems integrators, who need a futureproof solution, data security, and privacy compliance; and want simple, scalable, provisioning. The ZARIOT/@ Company solution provides the answer using SIM-based, end-to-end encryption from device to application, and beyond, to users, management platforms, legitimate 3rd parties, and more.

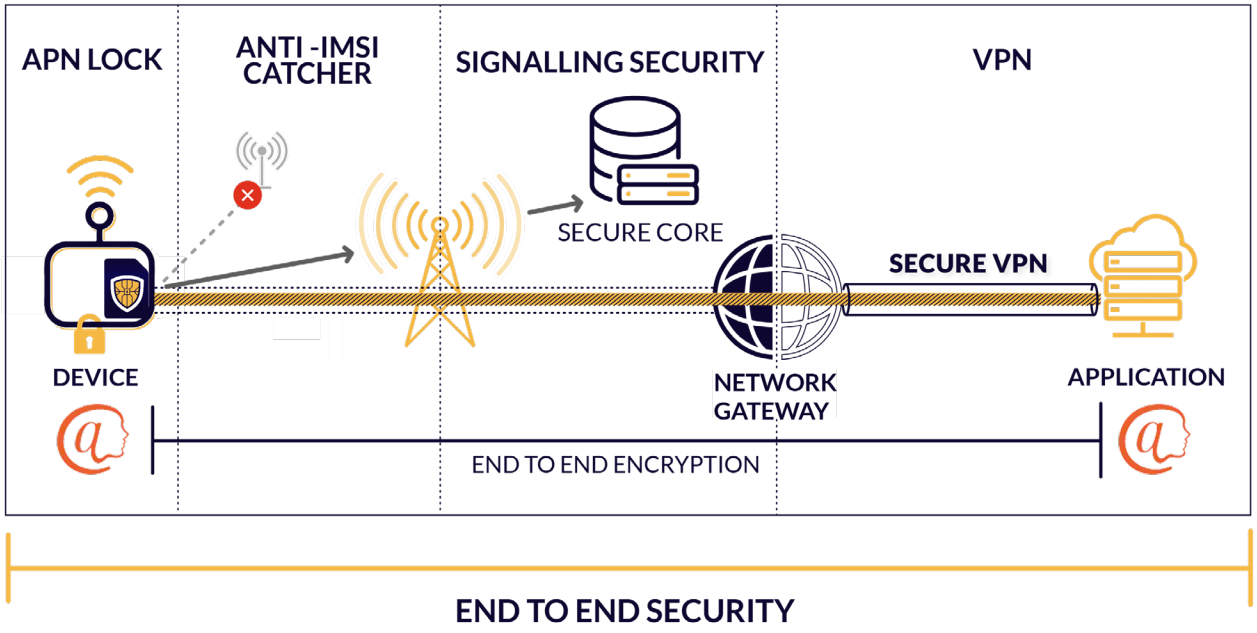
Why?

This solution can be retrofitted to any cellular device with an eUICC SIM and can bring a level of security to “things” that previously missed certification processes. Unlike other solutions, this does not leave data visible at any point, provides provably security and privacy, and does not require added device hardware.

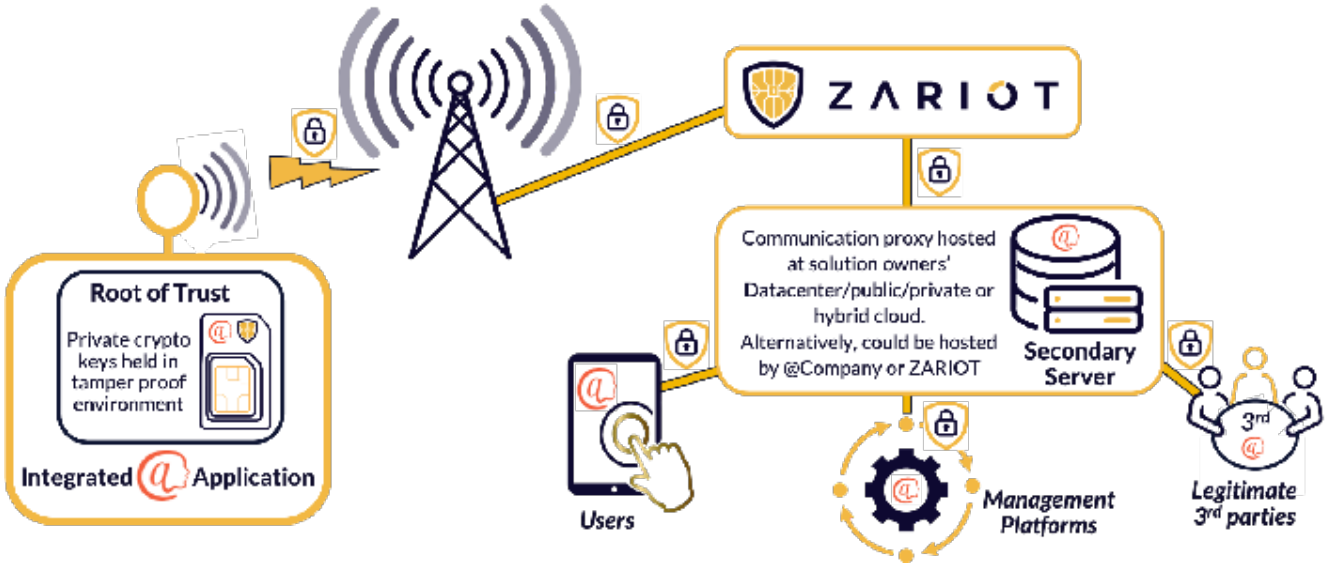
Overview

ZARIOT and The @ Company have partnered to provide an important step forward in securing the IoT industry. The innovative @ Company security technology combined with the connectivity and SIM expertise of ZARIOT simplifies the delivery of IoT solutions, making projects more effective and faster to deploy while providing all important end-to-end encryption, controlled data access, and futureproof security and provisioning.

The partnership extends the security model to include true end-to-end encryption of IoT data by integrating the open-source @platform, and using the SIM as a root of trust. This comprehensively secures the data plane, in addition to the existing security for the cellular control plane. It also radically simplifies the ability for applications to access data from IoT devices securely.



Solution at a glance



Keys on SIM

Any format of eUICC SIM (removable, embedded, or iSIM) can be used as the device's root of trust referenced to by the @platform service to enable complete control of data security to and from the application server.
The move to eSIM/iSIM form factor fully supported by ZARIOT, further enhances security as it hampers physically access making the keys even more difficult to tamper with.

True Privacy

The open-source @platform defines true end-to-end encryption and ensures secure exchange of information, exclusively between known trusted entities. The system uses an innovative design proxying encrypted data via a secure secondary server, meaning devices are never contacted directly.

Secure Provisioning

Data between known parties can only be decrypted using the secret encryption keys, held only by the respective parties i.e., the end device or user, the secondary server has no visibility. The necessary private keys are created on activation and are only held and known by that edge device, fully protecting data integrity and privacy. Initial unique parameters are loaded in real time automatically by the mobile network simplifying provisioning.

Beyond the Application

The protocol has been implemented with open-source tools and technology, enabling solution owners and designers to easily incorporate it into their solutions, and expand the use of user authentication further into their application to include users, management and administration and even possibly trusted 3rd party access. However, at all times under the auspices of the data owner's control.

Table of Contents

Flipping the Internet of Things

01.

Solution in Action – The Hypothetical Story of ACME Widgets

ACME is based in Spain and are implementing a variety of IoT devices in their digital transformation. They have an existing hybrid cloud, but IoT is something new for them and requires the project to be designed from the ground up. ACME are very security aware and in their traditional business have employed excellent IT protection but they are looking for something new, innovative and effective to support IoT.

Requirements

- Full security of IoT devices, connectivity and their application
- Data privacy: consumer protection and regulation compliance
- Improved customer experience
- Easy deployment and provisioning
- Simplified maintenance and administration

This customer journey will demonstrate how the ZARIOT and @ Company solution addresses each of these needs through:

- Secure IoT connectivity for the long-term
- Data privacy as a right and experience
- Consumer protection and regulation compliance
- Easy, efficient security and management at scale
- Simple provisioning and retrofitting
- Flexibility to support the evolution of the solution over a lifetime
- Straightforward, futureproof partnership experience

02.

Secure IoT Connectivity for the Long-term

Challenge:

- Current IoT solutions require networks and applications to provide the security of the device and data. This demands security at every layer in the network.

- Unlicenced spectrum connectivity is not subject to the same level of national regulation or enforcement rigour as licensed and therefore potentially has long term risks.

- All connectivity options have inherent vulnerabilities that could cause breaches of sensitive data or disruption to operations if exploited.

Solution:

Standards-based, global roaming connectivity within the licensed spectrum, fully secured to mitigate all known attacks, including data interception and denial of service.

Why Cellular?

ACME decide to use cellular connectivity, as their IoT widgets can be anywhere and cellular coverage is ubiquitous. They also see further security advantages in mobile networks being fully standards-based and using reserved licensed spectrum. Additionally, their legal department have highlighted that the global push for regulation means cellular access is probably seen by worldwide administrations as a long-term connectivity strategy for IoT.

As they had done with their device manufacturer, who had successfully completed their **GCF** and CE self-assessment criteria, **ACME** do due diligence selecting their connectivity provider. They value a flexible, dynamic, and committed partner to help deliver the project rather than just sell them connectivity.

Secure Cellular

ACME performed a risk assessment, and are quite aware that while cellular does provide the most robust connectivity, it still has security issues, so decide on a security focused option with **ZARIOT**, recently awarded **"Best Mobile Authentication and Security Solution"** at Mobile World Congress 2021 and shortlisted again in 2022.

ZARIOT are experts in mobile security, and operate a secure network core, which protects ACME and their customers from mobile network signalling attacks such as DoS, location tracking and data disclosure.

This is crucial to an end-to-end security strategy, however there are some vulnerabilities left to address: to protect the device from DoS and data interception via fake base stations (fake cell towers), ZARIOT have incorporated an Anti-IMSI catcher SIM applet.

ZARIOT also offers a VPN to protect data as it travels from their network to the application server location. However, ACME require even more robust data security. Through partnership with The @ Company, ZARIOT is able to deliver an end-to-end-encryption solution that uses the SIM itself as the root of trust.

03.

Data Privacy as a Right and an Experience

Challenge:

- Current solutions provide end-to-end encryption between an accepted TLS Client and a TLS Server. Beyond this, data is exposed so true end-to-end encryption data security is needed.
- Current encryption solutions rely on hyperscalers.
- Encryption solutions provide encryption from device to datacenter or application but do not extend to the user or other end entities, creating vulnerabilities at the edges.

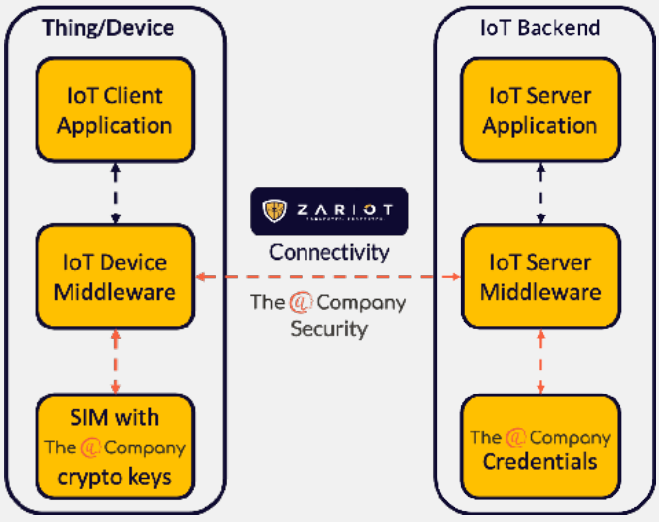
Solution:

To provide **true end-to-end encryption, network layer data security** for any cellular IoT device, without additional hardware requirements.

Simple, Light, and In-House

Device to application data protection is absolutely integral to IoT security and privacy, and can be provided by GSMA's excellent IoT SAFE program. The program uses the SIM as a tamper-proof security element to store the encryption keys i.e., the root of trust. However, ACME had thought they could not use this solution as IoT SAFE requires the use of one of the hyperscaler's (AWS, AZURE, GCP) clouds.

The ZARIOT and @ Company SIM-based solution works very similarly to the IoT SAFE program, but allows ACME to continue to utilise their previous infrastructure investment, inhouse capabilities, and processes. This also represents a significant saving at the point of manufacture as they do not need to deploy a separate secure element or Trusted Platform Module (TPM) in the widget but can simply reuse the SIM.



Zero Trust

The ACME project team are satisfied that the encryption secures privacy and security of data to their trusted environment. But sensibly, they employ a “Zero Trust” strategy, so protection and encryption must also be maintained within the local network.

Quizzing ZARIOT and The @ Company on the point, they received an unexpected response and one that opens a raft of opportunities to innovatively secure and simplify device administration, customer access and GDPR overhead.

End-to-End NOT End-to-Environment

The ZARIOT/@ Company solution is not “device to environment”, it is true “end-to-end”. The @platform exclusively enables encrypted communication, only between the end entities, and this is achieved by using an @platform secondary server as a proxy.

Described simply, the ACME widget reports its data to the secondary server using the encrypted data path.

The data is cached with access restricted at designated levels to various nominated individuals controlled by the device or user, who likewise communicate to the secondary server using the same encrypted connection as the widget.

For some ACME IoT services which consist of an IoT device controlled by a smartphone enabled with the @platform, the end-to-end encryption is all the way from the device to the user's hand.

- ACME Widget updates its data too secondary server with each element of data encrypted so it is only exposed & available to nominated users or tools via their individual secure signatures (keys).
- ACME tools and users can only see or adjust data of widgets open to them and the restrictions on that data allocated.

04.

Consumer Protection and Regulation Compliance

Challenge:

- At present, IoT hosting providers are potentially able to access data from the device. Data protection, if any, currently relies on the hope that the solution design includes network access security and application layer policies that are nearly impossible to enforce.
- GDPR, HIPPAA, and more data privacy regulations are being passed and enforced. Increasing cybersecurity regulations on consumer products creating greater need for provable data privacy, consent, and control. These permissions and configurations are difficult to administer and costly to manage.
- Some devices have multiple data sets that require different levels of privacy, and must be accessed by various 3rd party entities with unique access to only the data they are allowed to see.

Solution:

To put the end user in control of their data, and ensure that **only the intended recipients of the information can access it**, with no intermediaries (including ZARIOT and The @ Company) able to intercept, regardless of where the data transits or is stored.

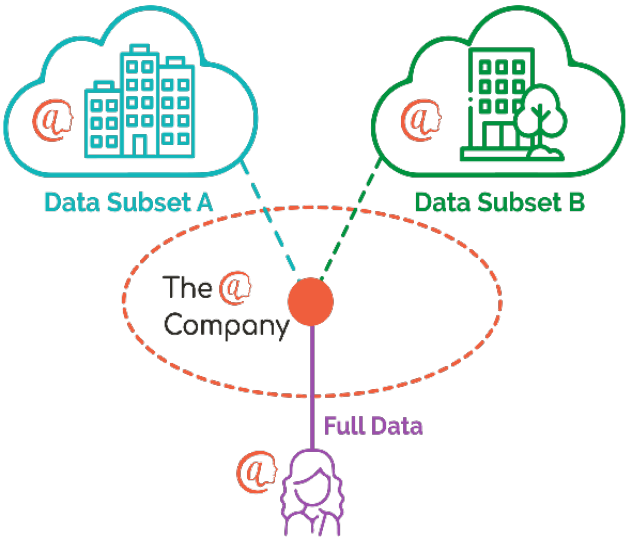
Server Access is Not Data Access

The above scenario maintains the Zero Trust philosophy, but ACME's CISO is understandably now suspicious of the secondary server. They employ some experienced white hat hackers to provide penetration testing to discover any vulnerabilities. The penetration testers are able to access the ACME network via a phishing ploy. "Naive Neville" in accounts opened a corrupted cat picture, allowing the hackers to move laterally through the network to the hosted server and successfully attach to the operating system with admin privileges.

This exposes the secondary server completely. However, they find all of The @ Company data is encrypted and they would need the keys of two end parties to read the information. Even then, it would be the subset they directly share with each other. While deeply disappointed in "Neville from accounts" the CISO realises that the data storage is provably secure, and they can rest easy that their customers' privacy and own GDPR responsibilities are met.

User Personas for Tailored Access

Since the @platform is end-to-end encrypted, each communication is point-to-point and unique. This, in turn, means every interaction can be tailored, with the widget effectively sharing different data depending on who asks.



The ACME COO immediately asks for each department to get its own persona to access and manage their appropriate data securely. They realise that this could be a real differentiator for personal information.

GDPR Made Simple

The ACME widgets can collect a lot of information, but ACME have a strong policy on customer privacy. They only store and use the minimum information unless the customer explicitly consents for ACME to retain more. This is hard to administer and can cause expensive calls to customer services to explain and setup.

As "@" communication is locked to an end-to-end encrypted, 1-1 communication, the COO resolves to allow each customer to open their own widget information settings, and to control at any given moment which information they share with ACME and/or other entities, and for how long.

This helps ACME maximise their potential functionality and the customer retains complete control over their data. The ACME COO is very happy with mitigation to their GDPR overhead and thinks there could be more options, so decides to call a meeting with the more commercial departments to brainstorm how else this can be utilised.

> ***"The EU General Data Protection Regulation (GDPR) is among the world's toughest data protection laws. Under the GDPR, the EU's data protection authorities can impose fines of up to up to €20 million (roughly $20,372,000), or 4 percent of worldwide turnover for the preceding financial year—whichever is higher."*** Source: www.tessian.com

Omnichannel Communication

The sales, marketing and accounts are full of ideas, from reducing administration by allowing customers to update their own addresses and contact details, to being able to allow users to dynamically opt in to new promotions and features. However, the head of the ACME customer contact centre is most excited.

If integration to the CRM was possible, the customer service agents could not only have access to client-administered data, but the customer could retain and make available all their conversations with ACME on demand. This would mean that however they contacted the ACME representatives, whether through chatbot, WhatsApp, or SMS, the info would be available to the agent. This massively improves the customer experience and is a step towards the ACME goal of Omnichannel interactions with the customer base.

05.

Easy, Efficient Security and Management

Challenge:

- Network addressability is a challenge that requires VPNs or on-premise gateways which are costly, complex and present security risks.
- Securely storing crypto keys centrally is a risk that is difficult to mitigate.
- IP network firewalls are expensive to implement and maintain, and difficult to manage for a mesh of internal and IoT network traffic.
- To access devices, many solutions require the use of a static IP, which are easy to find and attack.
- Lock-in effects can impact the future of a company, making business growth inflexible and difficult.

Solution:

Eliminate the requirement to use **gateways or VPNs** to access IoT devices, **static IP** addresses for devices, and **reliance on other** security infrastructure such as firewalling. **Prevent lock-in** with the use of open-source technologies and increased flexibility, and decentralise key storage.

Flexible Architecture for the Future

The ACME project team are highly skilled IT professionals and are naturally suspicious of solutions they have not tested. Many of their devices have lifecycles of a decade, and they are wary of long-term dependence on technology provided by vendors.

As The @platform is open-source, they realise there is no lock-in, which increases ACME's business flexibility in the future.

The team are further put at ease when they find they can host the whole solution within the ACME hybrid datacentre cloud environment.

They can connect directly from their network to the ZARIOT network via a private LAN, facilitated by a VPN tunnel.

Fully Encrypted Keys

Where are the @platform keys held?
The private keys only ever reside on the ACME device's SIM, individually created by the device itself, never shared, and only written securely to the ZARIOT SIM by encrypted communication.

No Static IPs

Having resolved the question of the secondary server security, the ACME CISO considers the impact of all the widgets on the network and asks the white hat hackers to attack the widgets and report back on the devices, firewalls, and other security infrastructure that protect them. Happy for the extra work, they ask for some test widget IP addresses they can use.

ACME operations team tell the CISO that they haven't been asked to provide any IPs. On investigation he finds that the @platform proxying the data via the secondary server means that the ACME devices only communicate in one direction, so there is no need for static IPs. If you can't reach the device, you can't hack it. "Great," thinks the CISO, it is secure and it will significantly reduce his firewall budget, but he does wonder how on earth the COO will manage all these widgets.

Data Management

Prompted by the CISO, the ACME COO decides to take a much closer look at widget administration.

Initial deployment is zero touch, so it is very straightforward using the ZARIOT API, but what happens afterwards? How can you communicate with the widget to get its data or change its settings?

The ACME engineering team explain their test findings. If the widget is offline for any reason, it doesn't stop you looking at its data, because the data is all held on the secondary server. Not having to directly interrogate the device has additionally removed a potential delay in data availability. This significantly improves the customer portal experience that has caused them issues previously.

Simplified Updating

Updating the widgets is also simplified as the secondary server is the master database. The engineering team explain that by simply making a change on the secondary server means that when the widget next connects, the synchronisation will update the settings. Each device has its own data, so changes can be managed for the whole deployment base or for individual units.

Visibility at all times, coupled with the database being incrementally updated on each communication, means that any changes are quickly and easily detected.

This allows very quick identification of any unexpected differences or changes to data or software, allowing ACME to react before issues occur.

Device Performance

The ACME widgets are wide ranging and have various functions, and therefore connection characteristics. These are supported by the comprehensive ZARIOT coverage, providing access to multiple networks in each country with the most appropriate type of cellular service.

Some of the widgets are very low power devices (LPWAN) so remain dormant when not in use in order to maintain battery life.

While dormant in Power Saving Mode (PSM) or Extended Discontinuous Reception mode (eDRX), they are only contactable on “Paging Occasions”, at small regular intervals for PSM or the short periods after data upload for eDRX. The ACME engineers recognise that the minimal incremental updates provided by the secondary server synchronisation at the time of data upload mean that they can optimise the use of the “Paging Occasions”. They tell management this will need testing but that it could possibly boost battery performance.

06.

Simple Provisioning and Retrofitting

Challenge:

- Provisioning is costly and slow.
- End-to-end encryption solutions based on industry standards require lengthy certification and cannot be retrofitted to existing devices.
- Designated secure storage solutions require a separate secure element or TPM, which adds cost and complexity.

Solution:

ZARIOT/ The @ Company provides **simple provisioning** options that reduce cost while increasing security. Ensure that the technology can be **retrofitted to suitable existing solutions and devices**, and enable cellular IoT applications to **easily incorporate** these advantages without additional hardware cost.

Zero Touch Provisioning

The process is zero touch for the device on delivery of the ACME widget, achieving an effective, easy deployment and excellent customer experience, while securing all the data to the ACME environment. The process is explained to ACME from the point of manufacture.

1- Bootstrapping

KIGEN, the partner SIM manufacturer provide SIM with default ZARIOT profile to support bootstrapping.

2- SIM Profile

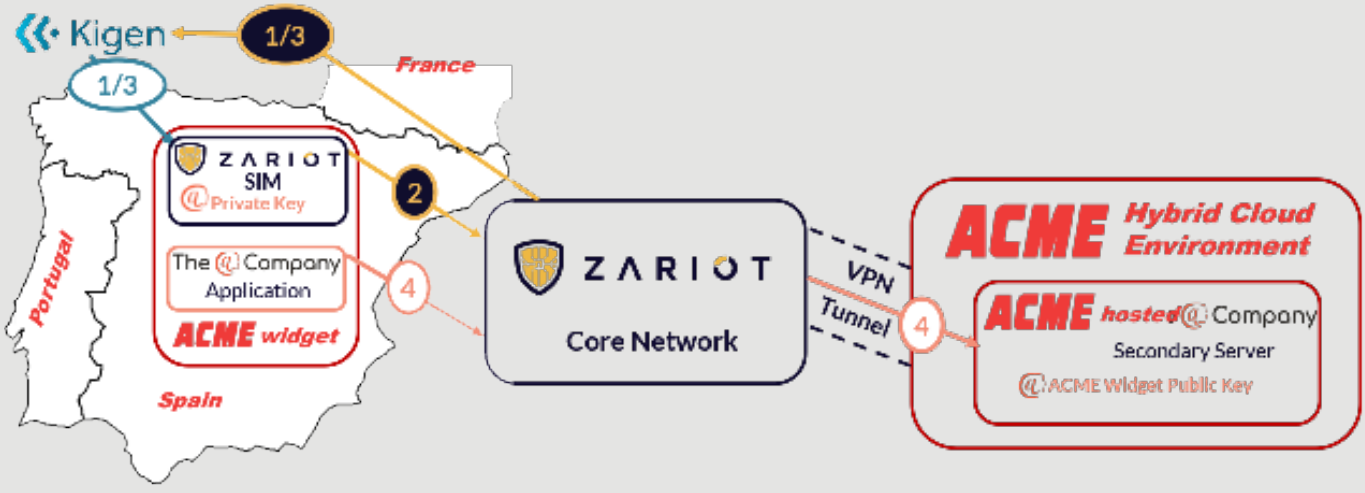
Using bootstrap detection, ZARIOT informs **KIGEN** that the @ enabled profile should be used. This is updated via the Remote SIM Provisioning (RSP) platform. The profile adds the file structure, @sign (a derivation of the IMSI), secondary server details, and temporary symmetric key.

3- Connect to Server on Boot Up

The ACME "@" secondary server IP address is internally locked down and routable via the ZARIOT network using VPN. Once the widget boots up and connects to the cellular network, it can then use the secure data channel to ACME and communicate with the hosted secondary server.

4- Private Key on SIM, Public Key to Server

Using bootstrap detection, ZARIOT inform **KIGEN** that the @ enabled profile should be used. This is updated via the Remote SIM Provisioning (RSP) platform. The profile adds the file structure, @sign which is a derivation of the IMSI, secondary server details, and temporary symmetric key.



Retrofit to Existing Devices

The ACME engineers have a wide range of widgets to support, and ubiquitous end-to-end encryption of all data across the install base really helps.

However, as a company, ACME expands not only through in-house innovation but also through acquisition.

The latest acquisition, a security camera, would obviously benefit from encrypting the video stream, but it is already deployed.

The good news is that the cameras use the new network programable eUICC eSIMs, and after discussion with ZARIOT, ACME have discovered that the SIM profiles can be remotely updated.

This allows ACME to retrofit the same connectivity and security to the deployed cameras as the green field widgets, homologising the whole install base and avoiding the need to send engineers on-site. This creates a huge saving in both time and money.

@ Platform Deployment Options

Deployment with Layered Encryption

Add end-to-end payload encryption layered on top of current TLS encryption. The existing capabilities for remote provisioning of network credentials remains as is. From there, device access and data encryption key pairs are generated on the device, never leaving the device and are thus more tamper resistant.

Device-Originated Connectivity

End to end encryption with device originated connectivity eliminating the need for device side TLS Client certificates.

In this case, the device always initiates connectivity sessions to TLS Servers, removing the need for a device side TLS Client certificate, IP connectivity, gateway, VPN or special firewall configuration as a result.

This further simplifies the provisioning process and increases accessibility through firewalls, etc.

07.

Straightforward, Futureproof Partnership Experience

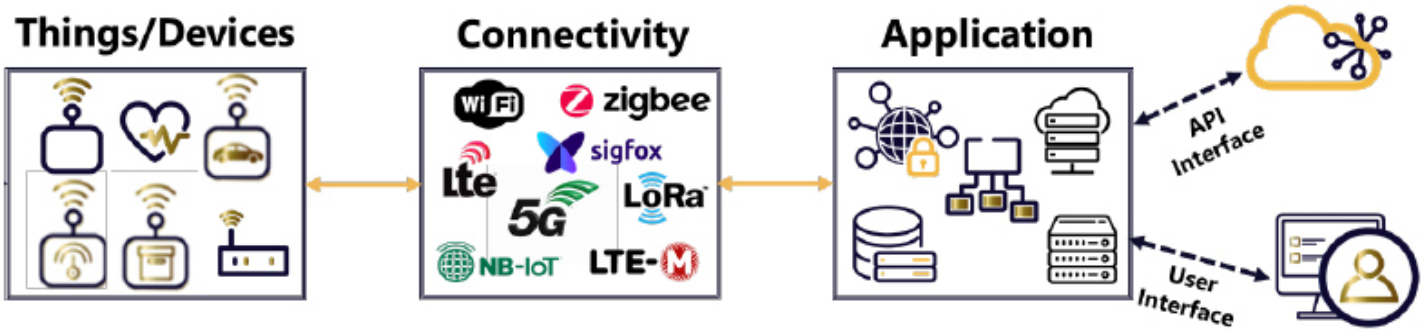
Growing Partnerships

IoT connectivity and security need to be as agile as your business to be successful and this can only be achieved when all vendors in the ecosystem work together to deliver a shared ultimate IoT solution goal.

The @ Company/ZARIOT partnership brings together innovative security technology and connectivity expertise to simplify the delivery of IoT solutions, making projects more effective and faster to deploy.

Truly secure and successful IoT ecosystems can only be achieved through collaboration, cooperation and partnerships. This strong belief extends beyond the ZARIOT/@ Company collaboration to include all those in the ecosystem.

ZARIOT promises not customer service, but partnership support to ensure successful integration and flexibility of new connected systems for the lifetime of devices.



The ACME team can address a wide range of challenges by combining the innovative @ Company/ZARIOT technology and connectivity.

Continuing Innovation

For ACME, the open and transparent relationship unlocks a wider discussion on SIMs, with ACME engineers interested in the other applets ZARIOT could provide.

The answer is hugely open. In all devices that ZARIOT supports, the SIM is evolving to become even more embedded, support more flexibility, and to be utilised in more ways than ever before. ZARIOT is currently looking at how to open up the potential of the SIM to support overall solution design.

Custom functions tailored for the device or service can be developed by ZARIOT in combination with OEM or IoT solution owner.

Some additional applets are already available, such as the patented Anti-IMSI catcher applet which returns the widget back to a real network should it come under attack from a fake base station. Other applets are in development. More important to ACME is the openness to support the ACME devices directly with custom SIM development.

Flexible, Lifetime Collaboration

ZARIOT explains that they believe that the complexity of IoT means that cooperation and collaboration between experts from multiple disciplines and technologies is the only way to deliver a service.

This will only increase in the future, so ZARIOT makes available an ACME technical contact to work with them on development using not only the SIM but the other monitoring and analytic tools available on the network.

08.

The Solution in More Detail

The ZARIOT/@ Company SIM applet provides:

A simple microcontroller API that IoT client applications can use to access the secure capabilities of the SIM when using TLS, DTLS and GBA protocols to secure an IP connection to an IoT service platform.

The properties of a common SIM application where the credentials (e.g. certificates / keys) associated with TLS or DTLS mutual authentication protocols can be stored and used by the IoT application.

A common way for IoT service providers to initially provision (i.e. one time), and potentially update (i.e. dynamic management) their internet security credentials (e.g. certificates / keys) and policies within the SIM using over-the-air management capabilities.

Secured Information

Secure Exchange of Information

A method for the secure exchange of information only between known parties where the data can only be decrypted using the encryption secret keys held only by the respective parties.

Local and Remote Data

The @platform implementation allows the IoT device to persist data locally, notify others that there is data to be looked up and cached for access, and synchronise data with a remote service where the data is encrypted with keys that remain on the device.

All devices using the @platform always initiate the connection to the secondary server to communicate with each other. The IoT device data cannot be directly accessed externally, instead it can only communicate via other cryptographically validated endpoints.

Unique Data Access

Provides a kind of polymorphism wherein different information can be provided to different parties for the same lookup. For example, every IoT device could look up @ configuration-acme and each would only receive their particular response which only they can decrypt and even validate the provider is legitimate with non-repudiation.

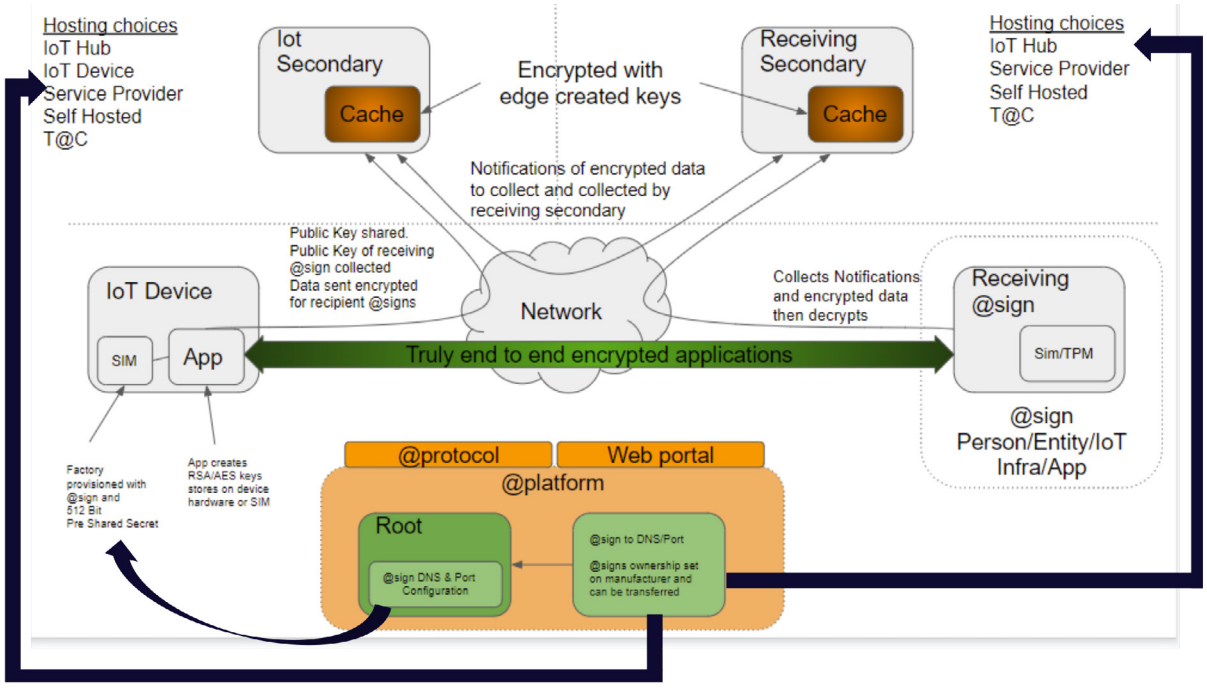
Provable Restricted Access

Where the data is cryptographically secured in such a way that it is provably true that intermediaries cannot access the data and only the recipient is able to.

Keys

Bootstrapping

A method for bootstrapping a device using a shared nonce secret that is deleted after the RSA secret keypairs are cut on the device from which they never leave. In production, the only thing that is required to be added to the SIM are an @sign and a small shared secret.



Security Keys Self-Generated

Presents no production risk associated with the generation of security secrets as they are generated on the device itself, not created by some service during production or activation and then loaded onto it, leaving them open to risk of being tampered with or accessed.

Separate Key Pairs

Authentication and encryption are enforced by separate key pairs.

Increases Ease, Reduces Cost

Standalone Encryption

After provisioning, the proposed scheme can work with, but does not require the deployment of any gateways, VPNs or firewall configurations to provide true end-to-end encryption.

Contact us for more information

ZARIOT
CONNECTED. PROTECTED.

connect@zariot.com

www.zariot.com

The @ Company

www.atsign.com

Kigen

www.kigen.com

Definitions/Glossary

API (Application Programming Interface)
A connection or interface between computers or software to allow exchange of information, usually to support integration of functionality or support business processes.

Bootstrapping
The technique for producing a self-compiling compiler — that is, a compiler (or assembler) written in the source programming language that it intends to compile.

CRM (Customer Relationship Management)
The databases and processes a business use to interact with customers. Frequently the customer contact and history database used to manage ongoing interaction including marketing outreach is referred to as the CRM system.

Device Certificates
An electronic or digital signature embedded into a hardware device, that enables mutual authentication and secure connections between two devices.

DoS (Denial of Service)
A denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network.

eUICC (electronic Embedded Universal Integrated Circuit Card)
A software stack which allows for remote provisioning of mobile operator profiles over-the-air, effectively changing the mobile operator it ‘belongs to’ without changing the SIM card in a device.

Endpoint
Any connected device or node that communicates across the network. e.g. IoT Thing, laptop, phone, router or switch.

End-to-End Communication Encryption (DTLS)
Ensures the data between a Client and Server is encrypted during transport. After decryption by the Server, information is exposed and in the clear.

End-to-End Data Encryption (The @platform, RSA PKI & AES 256)
The secure exchange of information only between known entities meaning that only the originator and intended recipient are able to access the data.

GDPR (General Data Protection Regulation)

This is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. These regulations require strict controls on how data is collected, stored and used. Violations of these regulations carry enormous fines and penalties. used. VIolations of these regulations carry enormous fines and penalties.

GSMA IoT SAFE (IoT SIM Applet For Secure End to End Communication)

Developed by the mobile industry, IoT SAFE (IoT SIM Applet For Secure End-2-End Communication) enables IoT device manufacturers and IoT service providers to leverage the SIM as a robust, scalable and standardised hardware Root of Trust to protect IoT data communications.

HIPAA (Health Insurance Portability and Accountability Act)

United States legislation that provides data privacy and security provisions for safeguarding medical information.

IMSI (International Mobile Subscriber Identity)

A number that uniquely identifies every device on a cellular network.

IMSI Catcher

An IMSI catcher is a device that appears to a mobile device as a cell tower (base station). The IMSI catcher is able to locate, track and effect all mobile phones and devices that are in its vicinity, When the device attaches to the fake base station, it detaches from the real network and effectively loses service and cannot be reached. In some circumstances the device can be forced to use previous less secure earlier generations of the cellular network e.g. 2G making data interception possible.

LAN (Local Area Network)

A network that interconnects computers and devices within a limited area, such as a residence, school, or office building, such as WiFi and BlueTooth.

Licensed Spectrum

“Spectrum” refers to the radio frequencies that carry wireless signals. Governments manage spectrum use, and spectrums can be unlicensed, meaning anyone can use the frequency, or licensed, bought for exclusive use by specific providers. GSM or Cellular spectrums are licensed, whereas networks like LoRa and Sigfox are unlicensed.

LPWAN (Low-Power Wide-Area Network)

A type of wireless telecommunication wide area network designed to allow long-range communications at a low bit rate among things, such as sensors operated on a battery. Sigfox and LoRa are examples of LPWANs.

Nonce secret

Nonce (number once) is an arbitrary number that is used just once in a cryptographic communication.

Penetration Testing
A penetration test, colloquially known as a pen test or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system; this is not to be confused with a vulnerability assessment.

Provisioning
The supplying of service to the network elements or device, connected to the mobile network.

Root of trust
Highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. Roots of trust provide a firm foundation from which to build security and trust.

RSA
RSA is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym "RSA" comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who publicly described the algorithm in 1977.

Service Activation Portal
This is used to orchestrate the enrolment of the device with AWS IoT Core, Azure IoT Hub (and soon Google Cloud) and to download the operational endpoint in the case of open market devices.

SIM (Subscriber Identity Module)
The module in a device that allows communication with the mobile network. It serves to identify and authenticate the device, and can also be used to store data. SIMs are traditionally referred to as SIM “cards” however new varieties of SIM are embedded (hardwired) to the circuit board of the device.

SIM Applet
A small application hosted on the SIM that performs a specific task supporting the wider software functionality.

SIM Profile
The configuration file used to enable mobile network connectivity and functionality. Multiple profiles can be stored on eUICC SIMs allowing the device to switch mobile operators or enabled additional functionality or applets.

Secondary Servers
@platform solution proxy providing the central point of communication for all @sign enabled devices, services, or users.

TLS Client
Client side of Transport Layer Security (TLS) a cryptographic protocol designed to provide communications security over a computer network.

TLS Server

Server side of Transport Layer Security (TLS) a cryptographic protocol designed to provide communications security over a computer network.

TPM (Trusted Platform Module)

Also known as ISO/IEC 11889, is an international standard for a secure crypto processor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.

VPN (Virtual Private Network)

Protected information system link utilizing tunnelling, security controls, and endpoint address translation giving the impression of a dedicated line.

Zero Trust

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.

www.zariot.com
www.@sign.com
www.kigen.com

@zariot1
connect@zariot.com
+3531 690 9000