ZARIOT

CONNECTED. PROTECTED.

Securely connect all your IoT devices worldwide with one contract. ZARIOT leverages the global coverage of mobile networks while offering secure end-to-end encryption and security.

CONNECTED

Global coverage in **190+** countries with **500** networks, utilising all mobile generations and IoT access

PROTECTED

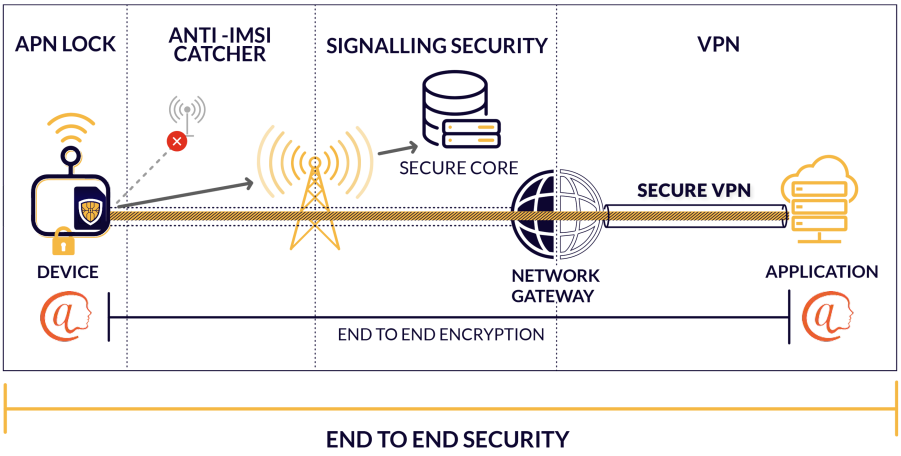
ZARIOT not only secures connectivity but drives true end-to-end security through partnerships and cooperation.

APN Lock

Individual username and password ensure authenticity of each device preventing SIM fraud.

Anti-IMSI catcher

Patented method and system for protecting the air interface and authenticating a base station.



Enhanced Signalling Security

Protects against location tracking, DoS, and fraud via mobile network signalling protocols

End-to-End Encryption

End-to-end user data encryption from device to core application and option to consolidate beyond, based on the @platform

Virtual Private Network

Complex encryption and hashing algorithms guarantee security over internet.

True End-to-End Encryption and Security

Using the SIM as the root of trust eliminates additional hardware requirements, extends encryption beyond the application, to the solution owner or device user and can be retrofitted to existing devices. Our security technologies deliver an end-to-end security solution by protecting the device, network, and application and beyond. By securing the data itself and not just the data path, access breaches and a multitude of attach vectors are rendered inconsequential.

eUICC capable SIMs and eSIM/iSIM

- One SIM for all destinations, simplifying logistics
- Automatic switching to optimal network for roaming and static devices
- Custom SIM Applet Development

Management Portal

- Manage, organise and view SIM usage and access
- Manage data session, security and VPN
- API Integration and webhooks

Gartner predicts attacks on operational technologies causing injury and possibly death will be weaponized by 2025, by 2023 the financial impact of cyber-physical attacks will reach over $50 billion, and that most CEOs will be held personally liable. Contact us to learn how we can improve your security posture and help you develop a secure control framework.

@zariot1 www.zariot.com connect@zariot.com +353 1 690 9000

	Connected	Protected
	The connection from devices to the cloud is the first step in connecting the data points, and the last step in leveraging them.	*The adoption of smart city initiatives depends largely on public trust. Every city has a responsibility to protect their infrastructure, residents, and data.*
Smart City	The smartest cities will be the most well connected cities. Cellular connectivity is the best option for many applications: • Available, accessible, and reliable in all cities • Futureproof: Standardized and regulated spectrum • All bandwidths for all applications. NB-IoT to 5G • Secure backhaul from local network gateways	Any attack or data breach is highly visible, damaging, and expensive. Smart cities must consider IT (and IoT) security to be their best insurance policies. Cellular is the most secure of all network types, however there are well-known vulnerabilities that must be considered. ZARIOT offers end-to-end data and device security, including secure cellular, end-to-end encryption, and more. We are working to build a secure ecosystem because we understand that security is more than the sum of its parts; security requires real collaboration.
Smart Energy	The complex smart grid system, includes many mission-critical components, is expansive and sometimes rural, making cellular the obvious choice in many cases. • Multiple carriers per country/city for best coverage • Automatic network switching for best quality • Futureproof SIM technology is 5G and 6G ready • NB-IoT designed for high density urban environments and low power devices environments.	Smart grid and smart meter projects increase efficiency and quality and pave the way to the integration of more renewable energy sources in our cities, however they are also a prime target for bad actors and opportunists. Any one of the millions of devices in a smart system has the potential to become a backdoor to the grid if left unsecured. Secure SIMs can play a key role in cellular and device security. SIMs are difficult to tamper with and can be used to create a root of trust, which is crucial to a trusted computing base and security policy.
Mobility	Connected vehicles require higher bandwidth, as well as highly mobile and expansive coverage. Smart fleet management demands high visibility and control to benefit from predictive analysis and other technologies. Cellular provides a range of benefits: • 2G, 3G, 4G, 5G, NB-IoT • 5G MEC: ultra-low latency • Regulated spectrum prevents interference and adds security • Most reliable and secure for critical infrastructure	Cities are known by their public transport. Any disruption creates bad publicity and diminishes trust in local governance, making it a tempting target for hackers. Transportation must be considered critical infrastructure and secured as such. Location data and other sensitive information must be safeguarded to protect the privacy of citizens. ZARIOT offers data security from device to cloud and beyond, and maintains location privacy to protect citizens and smart cities from attacks and data breaches.