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

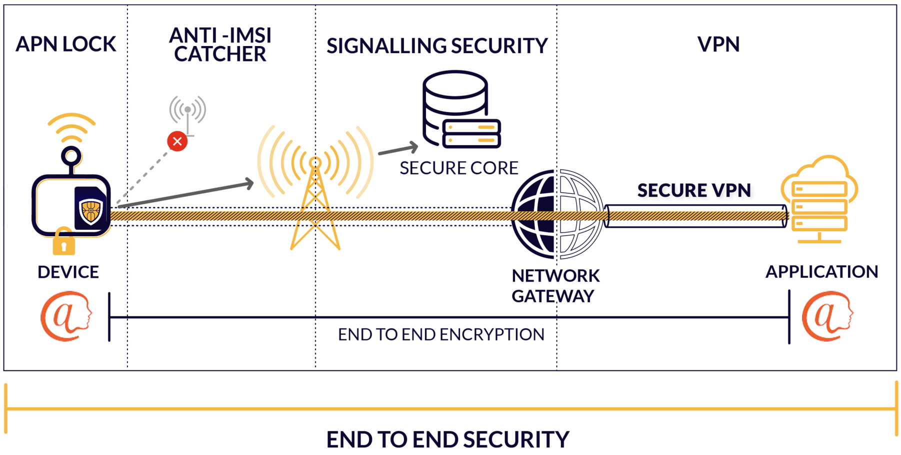
Global coverage in **190+** countries with **500** networks, utilising all mobile generations and IoT access

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

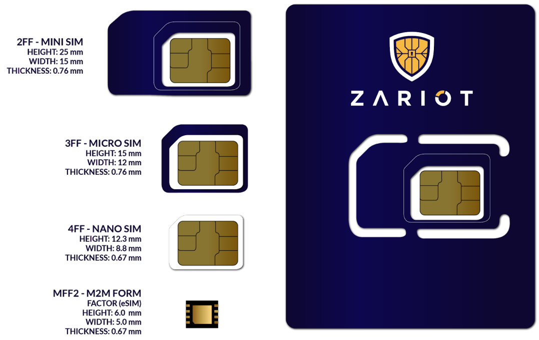
End-to-End Encryption
End-to-end user data encryption from device to core application and option to consolidate beyond, based on the @platform

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

Smart Grid and Renewable Energy

Remote data collection and operational technologies such as sensors, meters, gateways, routers, and switches increase the granular control of the grid, as well as increasing the speed and efficiency of response to blackouts, or even attacks by bad actors. However, if these devices are not properly secured, the potential increases for these connected devices to be taken offline in a cyber attack, or to be employed by the attacker to carry the attack out.

The data collected by sensors and meters, or at the point of a gateway or router may be invaluable in the wrong hands. Protecting the connectivity and data of these devices is paramount to a comprehensive security strategy. All smart grid devices, but especially those that are mission-critical must be protected from data interception, denial-of-service attacks of all kinds, and have access to the highest quality coverage, as well as redundant coverage from multiple networks where available.

Smart Meters

Utility revenue depends on billable usage, making meters a target for tampering and fraud. Revenue assurance for power providers is achieved through reliable, high-quality data. The connectivity of the meter must be protected to ensure it is always able to transmit data. The information transmitted must also be protected for two key reasons: revenue, and privacy. End-end-encryption ensures the data received by the provider is accurate and has not been modified, while also protecting the consumer by shielding energy usage patterns from a man-in-the middle (eavesdropping) attack. This kind of data breach could be disastrous at scale but may be equally damaging to an individual customer if used in conjunction with other information to build a picture of behavior. For remote applications where physical security is difficult to achieve, some consideration must be given to device tampering leading to theft and fraud, here again eSIM/iSIM are ideal technologies. In regional applications, multiple mobile networks may be needed to provide reliable coverage.

Lifecycle Management

Many IoT devices including smart meters and sensors are designed to be in the field for 10 to 15 years without the need for maintenance or monitoring. Designed for ultra-low battery and data consumption, these devices should provide data reliably for a decade or more. Regulated and standardized cellular technology allows governments to control critical connectivity so will stand the test of time.

SIM eUICC technology allows remote management of the connectivity profiles and settings. This effectively future-proofs the device and eliminates the need to change the SIM, or the device itself due to a change in connectivity or coverage needs. The SIM also future-proofs security in that it can be used as a tamper proof root of trust, as well as enabling a seamless progression to the next cellular generations and possibly allowing for new features to combat future security threats as they are discovered. Connectivity must be seen as an integral part of lifecycle management as well as a long-term security strategy.