

Secure Cellular Network



Global • Programable • As a Service

Designed For
Governmental Agencies
Nationwide Sensors
Critical Infrastructure



monogoto's Solution

For high profile organizations, monogoto provides its Secure Cellular Network solution for cellular phones & IoT connected devices. The solution provides advanced security capabilities for all its subscribers. In addition, it can provide enhanced features for a privileged sub-group of its subscribers, configuring their package and profile and enable them to switch identities or switch networks while maintaining the real/virtual phone number (MSISDN or DID) and the cellular Value-Added-Services (e.g. call recording, hunt groups etc.)

To ensure survivability and resiliency the Secure Cellular Network is able to connect to one or more mobile network operators (MNOs), allowing local and global multi-network coverage.

Each subscriber on the monogoto network can be assigned with a specific package (Voice, SMS ,Data) and security profile, either by the network policy manager (typically the CSO - Chief Security Officer) or by himself (if it is enabled in the network policy). Either way, the subscriber can manage his account with a simple and accessible My Account application on his mobile device.

The CSO has full control of monogoto network policy and the subscribers via a self-service platform and dashboard, enabling a variety of advanced capabilities, which are currently mostly available only to Tier 1 operators, such as:

Service Control

Allow/Block/Filter
Voice, SMS, Data

Network Visibility

View all signaling
events in real-time

Monitoring & Alerts

Set real-time alerts
based on any network
event

Anti Geo-Location

Recognize, block and spoof
hostile geo-location query
attempts through the signaling
(SS7/Diameter) channels

RF Equipment Detection

Detect IMSI Catchers and
Man-In-The-Middle attacks

Solution

Key Ingredients



Security

- Full visibility and control - get alerts on any network-related event
- Network-based protection - data / SMS / voice firewall
- Anomaly detection
- Create your own security policy based on traffic and signalling
- Security policy automation - network hardening
- Enhanced data protection - local breakout for data traffic
- SIM acts as secure element (HSM - cold wallet) to perform cryptographic signatures

Control and Management

- Self-service management platform
- +300 programmable (network and core) APIs
- Process automation to harden security and control the SIM life-cycle
- Tailor made offering powered by APIs for any IoT service creation

Services

- Cellular connectivity for IoT/M2M
- Private LTE for connected enterprises and campuses
- Governmental secure cellular core (MVNO)
- White label connectivity reseller platform (multi tenant)
- IoT service creation platform
- HSM/Secure element - secure signatures with AT commands or from the network

Technologies

- 2G, 3G, 4G, LTE CAT-M1, NB-IoT and 5G ready support eSIM profile
- Private LTE on CBRS, Guard or licensed bands
- Private LTE with local breakout
- Integrated with DPI tools
- Supported by any data protocol MQTT, CoAP, AMQP and more
- Network slicing

Deployment Options

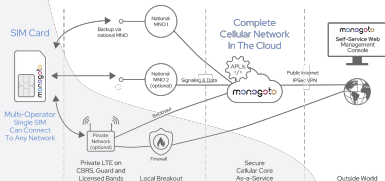
There are a variety of deployment options for monogoto secured network:

- Fully serviced from the cloud
- On-premise installation for a complete mobile-core
- Hybrid architecture (on-prem & cloud).

Note: integration to local partner is important for:

- In-country regulation
- National numbers (with/without portability)
- Reduce pricing (Voice, SMS, Data)

High-Level Solution Architecture



Add-ons

My Account Application

iOS and Android mobile application to manage the subscriber and his subscriptions. User-friendly interface which allows to check cellular plans status, purchase new plans and receive notifications. As a "bill shock" safety mechanism, the application subscribers receives push notification alerts after 50% and 75% of usage. monogoto my account app can be downloaded via Apple Store or Google Play.

Optional features:

- Customized branding
- Secure chat with unlimited groups
- Broadcast messages
- Security center with alerts
- Mobile payment
- Network actions (block data, view stats, check location etc.)

The CSO can decide features availability for each subscriber.



Secure Phones / PTT

Fully trusted devices with built-in security running on reliable bootloader and drivers. It provides true privacy with its custom-Built OS and rich kernel enhancements. In addition the secure mobile device encrypted voice and messaging, push-to-talk & secured attachments on any Android or iOS device.

The device comes with a diverse powerful suite of security tools including threat detection, antimalware and network monitoring. In order to guarantee performance assurance, the device comes with a built-in remote control technology & self-troubleshooting app enable remediation & productivity.



Technical Specifications

SIM Card

| | |
|----------------------|-----------------------------------------------------|
| Type | Classic, Industrial, Automotive |
| Form Factor | 2FF, 3FF, 4FF, eUICC, eSIM |
| Technologies | 2G, 3G, 4G, LTE CAT-M1, NB-IoT (coming soon) |
| Coverage | +170 countries, +500 network |
| Multi-IMSI | Dynamic IMSI swap according to business logic |
| Profile SWAP | Remote SIM provisioning (RSP) interoperability, OTA |
| Roaming Restrictions | Roaming policy for allowed networks |
| Steering | Override the operator's defined steering |
| HSM | SIM act as HSM to execute cryptographic signatures |

Platform

| | |
|----------------------|--------------------------------------------------------|
| Capabilities | Provisioning, management, monitoring |
| Self-Service Console | Flexible billing options for wholesale and retail |
| Billing | Define SIM groups policy and business logic |
| Event Stream | Action/alert triggers based on metric condition |
| RESTful APIs | Embed any function in your existing business processes |
| Anomaly Detection | Alerts from: usage, geo-fencing, MITM attack etc. |

Security

| | |
|------------------------------------|-----------------------------------------------------------------------------------------|
| Signaling Firewall | Incoming/outgoing voice, SMS rules |
| IP/Data Firewall | Inbound/outbound IP & protocol rules |
| Network Management | Address pools, VPN, routes, NAT, isolation, public and static |
| IMEI Lock | Allow SIM for specific IMEI |
| SMS VPN | Incoming/outgoing SMS via API |
| SMS Home Routing with Spoofed IMSI | Prevent basic ss7 attacks |
| Dynamic Registration | Additional registration decision within LU process |
| IMS/MSISDN Decoupling | Protect against ss7 attacks, hide MSISDN from the network (without service degradation) |

About Us

The Team

monogoto's management team brings global telecom and cybersecurity experience with veterans of the elite IDF technological units. Headquartered in Tel-Aviv, at the heart of Israel's thriving tech community, we serve customers throughout Europe, LAMEA, Asia-Pacific and North America, tailoring holistic secure cellular communication solutions.

Contact Information

Address: 94 Yigal Alon street, Tel Aviv, Israel

Website: www.monogoto.io

Email: info@monogoto.io

Website: www.hyperms.com

Email: info@hyperms.com



Hypermedia

monogoto

