

# The Digital Battlefield

---

## Executive Summary

Global security operations face unprecedented challenges from advanced communications surveillance techniques and compromised network infrastructure especially when operating in foreign territories. This white paper presents a revolutionary approach to defeating surveillance from mobile networks that transcends conventional security measures, offering a level of communications secrecy and independence previously thought to be impossible.

Conventional measures primarily focus on securing communication content against man-in-the-middle (MITM) attacks. However, these approaches fail to address a critical vulnerability: mobile network meta-data. This unprotected information represents a treasure trove of easily gathered intelligence that, if/when exposed, poses very serious threats –including physical – to both individuals and organizations. Moreover, emerging surveillance technologies can now bypass traditional content security measures, rendering them increasingly ineffective against sophisticated attacks. To combat these evolving threats effectively, organizations must adopt a radically different approach that goes beyond content protection.

The proposed solution is a system to intermediate the provisioning of data service between Mobile Network Operators (MNOs) and an in-the-field agents' cellular devices<sup>1</sup> (the UE – User Equipment). The effect of controlling the provisioning of service dynamically enables an agency to operate its own global cellular mobile network independently of, and without installing, any MNO infrastructure. This system, a

---

1. The cellular device to be distributed to each in-the-field staff is a proprietary Klök handheld data hotspot equipped with IMSI and IMEI swapping capabilities.

Software-Defined MNO (SD-MNO) is a communications management platform installed in the cloud that uses the existing worldwide cellular infrastructure and piggybacks on the services of established MNOs (either home country or local in the host country) without integration, cooperation, or even the MNOs' knowledge.

An SD-MNO defeats sophisticated hackers and state actors (and MNOs) by disrupting their ability to identify targeted individuals' devices. It de-contextualizes traffic and dis-aggregates metadata from user identity. By controlling UE settings remotely in addition to the "identity" transmitted to/through the MNO over the services it provisions, the SD-MNO fragments and obfuscates the data and metadata transmitted rendering targets invisible and impervious to network attacks.

Provisioning UEs with service requires only the acquisition of ordinary plastic SIM cards (from any MNO in the world) that are, then, inserted into a "SIM Carousel(s)" physically hosted in generic data center(s) and connected to a Klök Cloud<sup>2</sup>. The SD-MNO selects/swaps/removes IMSIs by rotating a desired SIM (in the carousel) into service onto a target UE anywhere in the world thus changing its IMSI; it manages device profiles remotely including IMEI, IP addresses and controls other UE identifiers. Moreover, because UE identifiers can be managed, a target UE can be setup as a decoy, or for example a UE can have identifying parameters applied to smoke out or disrupt an adversary for example by creating suspicion of their own personnel by applying an individual's known identifiers to a UE planted in a compromising location.

This white paper outlines how Klök's SD-MNO technology provides unparalleled protection for field agents, embassy staff, and government personnel by ensuring full control over communications, operational secrecy and independence from external networks.

## Introduction

Klök combines on-premises cloud-based infrastructure with proprietary UE. This provides a multi-layered, sovereign defense against tracking, locating, interception, and metadata analysis, while ensuring that no external entity can piece together a complete picture of the communications stream. We will explore how this innovation protects government workers and maintains operational integrity in hostile environments by creating a truly elusive communication network.

## The Threat Landscape

- Government personnel (especially when operating abroad) face numerous threats, including:
- Stingray devices a/k/a IMSI catchers
- SS7 & Diameter vulnerabilities
- Advanced persistent threats (APTs)
- Physical surveillance enhanced by modern technology

---

2. The Klök Cloud is deployed and operates independently of Klök on agency owned or contracted cloud infrastructure e.g. AWS.

- Metadata analysis of Call Detail Records (CDRs)
- Compromised or coerced network operators
- Man-in-the-Middle attacks

These threats exploit vulnerabilities in traditional communication methods and protocols and the reliance on foreign network infrastructure, potentially exposing operatives' identities, locations, and communication patterns to adversaries.

## Understanding IMSI, IMEI, Routing Tables, CDRs, and Roaming Vulnerabilities

- IMSI: Unique identifier for SIMs.
- IMEI : Unique identifier for cellular devices.
- Routing Tables: Determine call and message paths through networks.
- CDRs: Metadata logs of communication events.
- Roaming: Reliance on foreign MNOs when operating internationally.

### Vulnerabilities

Static IMSI: Enables long-term tracking and targeted interception by hackers, state actors, MNOs and their roaming network partners of cellular devices.

Standard Routing: Allows metadata collection by MNOs and their roaming network partners.

CDR Analysis: Can reveal operational patterns and relationships.

Roaming or foreign network dependence: Subjects operations to foreign network surveillance (host country local MNO) and potential compromises when in foreign territory.

## Our Advanced Solution: On-Premises SD-MNO with IMSI and IMEI Rotation and Routing Control, post quantum encryption, and IP & location spoofing.

Our technology creates a sovereign, invisible communication network under licensee control through a multi-faceted approach:

### On-Premises SD-MNO

- Operate your own virtual MNO entirely on your premises
- Independence from external MNO infrastructure
- Misdirect and obscure information from all networks

### Dynamic IMSI Rotation

- As many IMSIs per device as there are SIMs in the Carousel
- Seamless switching

## **Dynamic IMEI Management**

- Infinite IMEIs per device
- Seamless switching

## **Intelligent Routing Control**

- Custom routing tables
- CDR obscuring
- SMS re-routing

## **Benefits**

- Unprecedented operational secrecy: No roaming network can piece together a complete picture of operations
- Complete control over all aspects of communication
- Enhanced anonymity and tracking resistance because devices don't have a static IMEI/IMSI pair
- Total metadata protection
- Superior interception resistance
- Defeat "track and locate"
- Operational security through fragmented, misleading communication patterns
- Rapid deployment without any external negotiations or integrations
- Rapid discovery of hacking attempts
- Operates covertly in any country, regardless of local network infrastructure

## **Use Cases**

### **Scenario 1: Field Agent Operations**

Consider 'Sarah', operating undercover in foreign city.

Without our technology:

- Vulnerable to tracking via static IMSI by roaming networks
- Vulnerable to IMSI catchers

- Communication patterns exposed to foreign carriers
- Communication and pattern of life exposed to hackers
- Risk of operation compromise through roaming network surveillance
- Must find “burner phones” and hope for the best

With our SD- MNO, IMSI rotation, and routing control:

- Sarah’s communications are fragmented and obscured across multiple roaming networks
- Her cellular regularly changes its IMSI, thwarting any tracking attempts
- Custom routing and spoofing ensure no accurate metadata is ever generated
- Whether local networks are compromised, or hackers land an attack vector, they only see disconnected pieces of the operation
- Rapid deployment of new agents without a consistent network footprint

This scenario demonstrates how our technology provides unprecedented security and invisibility for the most sensitive field operations, effectively misdirecting all roaming networks.

## **Scenario 2: Embassy Communications**

At a U.S. embassy in a foreign nation:

Traditional vulnerabilities:

- IMSI catchers around the embassy
- Comprehensive surveillance by local roaming networks
- Risk of operation patterns being analyzed by foreign entities

Implementing our technology:

- State Dept. operates its own invisible global SD-MNO in its domestic premises
- Embassy Staff communications are fragmented and obscured across multiple local and roaming networks
- Integrates seamlessly into State Dept. controlled switching kit
- State Dept. controls all inbound and outbound communications (white lists/ black lists/ recordings) without MNO participation and without CAMEL protocol.
- Rotating IMSIs, modified IMEIs and custom routing prevent “track and locate” of embassy staff and any meaningful data collection
- Sensitive communications appear as disconnected, misleading patterns to local MNOs
- Seamless, secure integration of visiting officials into the covert network

This scenario illustrates how our solution provides a completely autonomous, undetectable communication infrastructure for entire embassy operations, consistently misdirecting local network surveillance efforts.

### **Scenario 3: Military Operations**

Officers issuing orders on the battlefield targeted and killed. Russia's Ukraine campaign has seen a number of attacks on senior officers based on their use of cell phones (IMSI tracking).

Traditional vulnerabilities:

- IMSI catchers
- Comprehensive surveillance by local roaming networks
- Risk of operation patterns being analyzed by foreign entities

Implementing our technology:

- Rotating and modifying IMSI and IMEI to prevent user identification
- Clone officer's real IMSI and IMEI onto a UE planted in an alternative location to draw targeting away

## **Additional Security Features**

Our core technology can be complemented with:

- End-to-end post quantum encryption
- Secure boot and runtime integrity checking
- Remote wipe capabilities
- Anonymous routing
- Location spoofing and decoying

## **Implementation and Integration**

Klōk technology offers unparalleled ease of deployment and security:

- Set up your own SD-MNO on-premises in your AWS environment with minimal hardware
- Become independent from external carriers by simply adding a SIM card
- No need for any external network integrations or agreements
- Centralized, on-site management and customizable policies
- Scalable from individual operatives to entire agencies
- Comprehensive training and 24/7 support, all managed internally

## Conclusion

In an age of pervasive digital surveillance and network vulnerabilities, Klök's SD-MNO technology with IMSI rotation and routing control offers a revolutionary tool for maintaining absolute security, anonymity, and sovereignty in government communications. By operating an infrastructure completely independent of MNOs and dynamically altering device identifiers and communication pathways, we provide a comprehensive solution that makes your operations and communications truly invisible to all external entities, consistently misdirecting and fragmenting information available to mobile networks.

The scenarios presented demonstrate the practical, real-world benefits of our technology. From protecting field agents to securing entire embassy communications, our solution offers unparalleled protection against tracking, interception, surveillance, and metadata analysis, all while providing complete operational secrecy on foreign soil.

As global threats continue to evolve, so too must our approach to security and operational independence. By implementing our advanced technology, government agencies can achieve a level of communication autonomy and invisibility previously thought impossible, ensuring the utmost safety of their personnel and the absolute integrity of their most sensitive operations worldwide.

We invite you to contact us for a demonstration of how our technology can be tailored to your specific security needs and operational requirements. Together, we can build a future where your most critical communications remain truly invisible and indecipherable to all foreign networks and adversaries.

---

End

© 2024 Klök All Rights Reserved