
Three Ways to Validate Identifier Rotation

Method 1

Advanced RF Capture (Technical Lab Verification)

Purpose: External method to show that network-level identifiers (IMEI/IMSI) change over the air

Tools:

- Software-defined radio (SDR) setup (e.g., BladeRF, srsRAN)
- LTE protocol stack decoder
- RF-isolated lab or controlled test cell

Steps:

1. Power on the Klök device and let it connect to the mobile network.
2. Capture the LTE attach request and extract IMEI and IMSI.
3. Using the Klök cloud portal, trigger a rotation.
4. Re-capture the attach request after reconnection.
5. Compare the new IMEI/IMSI to the original.

Expected Result: The network sees a completely new device and SIM identity, confirming full rotation.

Method 2

Device Log Validation (Hands-On Terminal Method)

Purpose: To show identifiers change using AT commands or logs on the device

Tools:

- ADB access on Klök
- AT command shell
- Connected laptop

Steps:

1. Connect laptop to the Klök device.
2. Access Run commands:

- `mifitool`
- `AT+CGSN` # Check IMEI
- `AT+CIMI` # Check IMSI

Or, view logs:

- `mifitool`
- `logcat -b radio | grep -i imei`
- `logcat -b radio | grep -i imsi`

3. Trigger identifier rotation via the cloud.
4. Rerun the same commands.
5. Compare values pre- and post-rotation.

Expected Result: New IMEI and IMSI values confirm that rotation occurs under remote control

Method 3

Browser-Based Confirmation (End-User Visible Test)

Best for: Quick demonstrations, non-technical teams

Purpose: Show visible changes in IP address and operator identity

Tools:

- Any phone or laptop connected to Klök via WiFi
- A public website like Speedtest.net or ipinfo.io

Steps:

1. Connect your device to the Klök Wi-Fi.

2. Visit Speedtest.net and note the ISP/carrier name and IP address.
3. From the Klōk cloud console, trigger an identifier rotation.
4. Wait ~30 seconds and reload Speedtest.net or ipinfo.io.
5. Observe changes in:
 - Carrier/operator
 - IP address / ASN

Note: Because Klōk includes an integrated OpenVPN tunnel, the IP address may also reflect the VPN endpoint, not just the cellular provider. This allows additional control over IP-based geolocation, routing, and anonymity, further obscuring the user's origin.

Expected Result: Different carrier or IP address (or both) confirms that Klōk changed SIM connectivity and/or VPN routing.

Summary

Method	What It Proves	Complexity
RF Capture	Network-level identity fully changes	High
Terminal Logs	Device identifiers rotate on command	Medium
Speedtest	Public-facing IP and operator change (via SIM or VPN)	Low

Conclusion

Klōk doesn't just encrypt traffic, it erases digital identity trails. These three validation methods offer clear evidence that IMEI, IMSI, and IP rotation occurs securely and remotely, ensuring users are untrackable, uncorrelatable, and off the radar.

Klōk includes a built-in OpenVPN client, allowing IP addresses to be rotated or pinned to a specific endpoint, providing an additional layer of identity protection beyond the SIM.

Note: This is critical; Klōk is not just a device. It is a cloud-managed platform that abstracts the cellular network's ability to provision its service to the cellular device and control SIM identity. By virtualizing SIM provisioning and decoupling it from the mobile operator, Klōk ensures that even the cellular carrier cannot track the user or link activity over time. Control resides entirely with your organization.