Telefónica

Open Gateway

Device Swap API

Protecting Against Device Swap Risks for Trusted Digital Services

GSMA™ CAMARA THE TELCO GLOBAL API ALLIANCE

Open Gateway is a global initiative, **enabling telco operators to expose core network capabilities** as standardized, interoperable APIs.

- **Global & Multi-telco:** Backed by GSMA, adopted by Telcos Worldwide
- **Standardized & Secure:** Built on CAMARA open standards, privacy-first by design.
- **Trusted Network Intelligence:** Telco-grade accuracy and trust.

80 Operator Groups

291 Mobile Networks

>80% Network Connections

Device Changes Create **Security Gaps** and Operational Challenges

Unauthorized Access

Fraudsters exploit device changes to hijack accounts and gain control of sensitive services.

- Accounts compromised easily
- Customer trust eroded

6.5%

of device checks flagged as high risk (Incognia)

Transaction Risk

High-value actions occur without confirming device legitimacy, increasing exposure to fraud.

- Payments processed unchecked
- Financial losses escalate

$11.5k

Average financial loss to consumer per incident (ICCC)

Operational Complexity

Manual checks slow processes and increase costs, reducing efficiency and scalability.

- Delayed service activation
- Higher operational overhead

150M

Device changes every year in the US (Incognia)

A solution is needed to **verify device integrity instantly and prevent fraud** during migrations and sensitive actions…

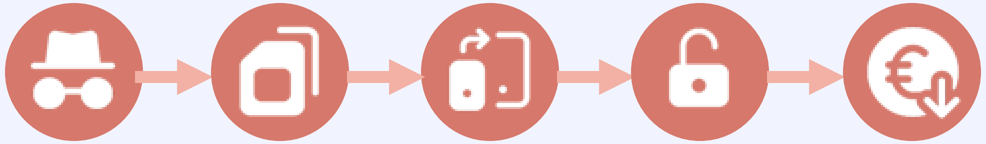
Device Swap Detection – **Real-time protection for account integrity**

Instantly verify device changes to **prevent unauthorized access**, secure transactions, and **deliver a frictionless customer experience** across platforms.

Device Swap **confirms device integrity** in real time

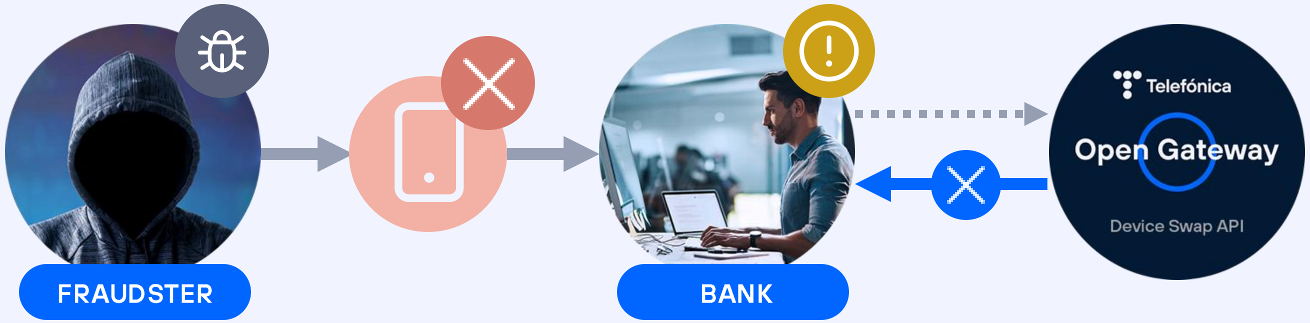
Queries network data to detect recent changes in a user's device IMEI, enabling real-time risk assessment and enhanced fraud prevention.

WHITOUT DEVICE SWAP API



The attacker inserts a stolen or cloned SIM card into a new device. They now have access to the messages or calls meant for the user and can now access applications, reset passwords, authorize transactions and commit other types of identity fraud.

WITH DEVICE SWAP API



The Device Swap API detects when a SIM has been inserted into a different device. The business can flag this suspicious activity early, enforce re-authentication or block high-risk transactions.

Device Swap API is applicable **to different use cases**

Account Takeover Prevention

Detect suspicious device changes before granting access, reducing account compromise and identity theft.

Unauthorized Transaction Protection

Verify device integrity before high-value payments or transfers to safeguard assets.

Corporate Device & VPN Security

Ensure only authorized devices access corporate networks and VPNs, protecting sensitive data.

IoT SIM Security

Detect unauthorized SIM swaps in connected devices to prevent fraud in IoT ecosystems.

Automatic Logoff for Compliance

Trigger device-based session termination to enforce security policies automatically.

Premium Service Safeguarding

Validate device legitimacy before granting access to subscriptions or sensitive services.

Device Swap API **benefits**

Fraud Reduction

Instantly flag high-risk device changes to cut off fraudulent activity before it impacts customers or operations.

Operational Efficiency

Lower support costs and reduce manual review workloads through automated, real-time device trust signals.

Frictionless Experience

Provide low-latency, invisible verification that protects users without adding authentication steps or onboarding delays.

Regulatory Confidence

Simplify compliance with global security and KYC standards by enforcing consistent, auditable device checks.

Stronger Digital Security

Strengthen account and transaction protection across apps, channels, and services with continuous device integrity insights.

Future-Ready Risk Intelligence

Leverage advanced device insights for smarter risk scoring, proactive threat alerts, and scalable future services.

Next Steps to start using the Device Swap API

Sandbox Testing

✓ Join Partner Program ✓ Test use case ✓ PRO environment

Try & Buy

✓ Proof of Concept ✓ Validate use case ✓ Business model discussion

Related Open Gateway APIs: to be combined with Device Swap API in particular use case for added value

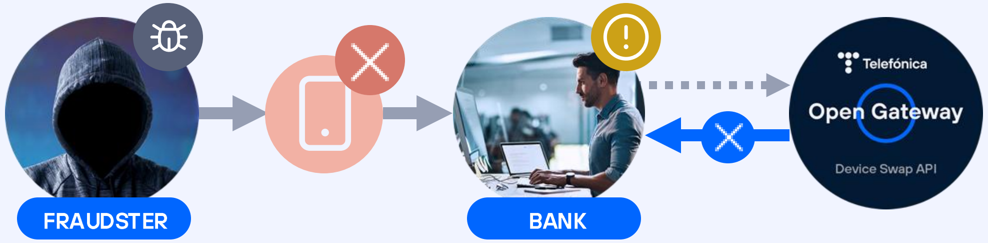
SIM Swap API	Checks if a user's SIM card has recently been changed, aiding businesses prevent fraud by alerting them to potential unauthorized account access, enhancing security during logins and transactions.
KYC - Match API	Validates identity information against trusted operator data, using a sophisticated scoring system to provide a reliable approach to rapid online identity verification, onboarding and security.
Number Verification	Authenticates the user of an app or online service by checking if the phone number they provide matches the one associated with the device they are currently using.

Telefónica

opengateway.telefonica.com

Device Swap API: Real-Time Detection for Device Security

Queries network data to detect recent changes in a user's device IMEI, enabling real-time risk assessment and enhanced fraud prevention.



Account and Transaction Protection

Detect suspicious device changes before access or high-value actions, reducing account takeovers and fraud.

Corporate & IoT Device Security

Ensure only authorized devices access networks, VPNs, and IoT systems, preventing misuse.

Compliance & Service Safeguarding

Trigger automatic logoffs and validate devices before granting access to services, enforcing security policies.

✓ Stronger Security & Fraud Reduction

Detect risky device changes instantly to block fraud and protect accounts and transactions.

✓ Frictionless, Efficient Experiences

Deliver seamless verification for users while reducing manual reviews and operational costs.

✓ Compliance & Future-Ready Intelligence

Automate security checks to meet global standards and enable smarter risk scoring for emerging threats.

CHECK

Request	phone number and max age (1 to 2400 hours; default is 240 hours)
Response	True/False (depending if the Device has changed)

RETRIEVE

Request	phone number
Response	YYYY-MM-DD HH:MM:SS (date & time of last change