



Open Gateway

# Overview, use cases and case studies on the SIM Swap API

Telefónica Open Gateway

March 04, 2024



# Table of Contents

**01.** Description, Features,  
and Categorization

**02.** Characteristics of SIM Swap

**03.** Use Cases

**04.** Start using SIM Swap API!

**05.** Documentation

**06.** FAQs

**07.** Other relevant information



**Description,  
Features, and  
Categorization**

01

**In a digital landscape where trust is paramount, the SIM Swap API emerges as a guardian - a defense against identity appropriation that leverages operator network information.**

This API focuses on tackling fraud related to anomalous SIM swap events that could compromise the use of the subscriber number in security applications. A recent SIM swap might indicate a risk of account takeover fraud. This insight gives you the ability to swiftly and proportionally adjust security protocols and measures.

# Features and Categorization

CAMARA	
COUNTRIES	
SECTORS	<p>SOCIAL &amp; CUSTOMER ENGAGEMENT</p> <p>ICT SERVICES</p> <p>FINANTIAL SERVICES &amp; INSURANCES</p>
SERVICES	IDENTITY



# Characteristics of SIM Swap

02

# Overview

## Characteristics of SIM Swap



### Two-Factor Authentication Reinforcement

SIM Swap amplifies traditional 2FA by adding a contextual layer. This layer evaluates risk levels in transactions, such as purchase PIN verifications, based on recent SIM events. It's like giving 2FA a risk assessment upgrade, ensuring not only user identity but also transaction security. As developers, this means you're coding a smarter, adaptable security solution that keeps up with evolving threats.



### Fraud detection

With the API SIM Swap, the monitoring of SIM-related activities becomes achievable. Alerts are triggered by any abnormal behaviour. This empowers you to architect applications that can promptly react to possible risks in real time, whether it's unexpected alterations in SIM particulars or patterns that raise suspicion.

### Secure Account Creation

Thanks to the SIM Swap API, it's possible to detect potentially fraudulent actions before creating new user accounts. This enables the prevention of modifying personal information such as addresses or initiating password resets, which is particularly crucial in the context of banking transactions.

# Overview

## Characteristics of one standard SIM Swap API



### Simplified Integration

With a standardized API, developers can seamlessly integrate SIM Swap functionality into their applications without the need for custom implementations for each telco operator. This simplifies the development process and reduces the time-to-market.

### Uniform Access to Telco Capabilities

The CAMARA standardized API offers consistent access to diverse telco capabilities, like SIM Swap detection, through a unified interface. This ensures uniformity and adaptability across varying operators and markets.

### Enhanced Dev Experience

The standardized SIM Swap API from CAMARA promotes a developer-friendly model. This approach not only saves valuable time and effort but also ensures a consistent and reliable user experience. Developers can focus on creating innovative solutions without the complexities of operator-specific implementations, thereby accelerating time-to-market and fostering a more efficient development ecosystem.



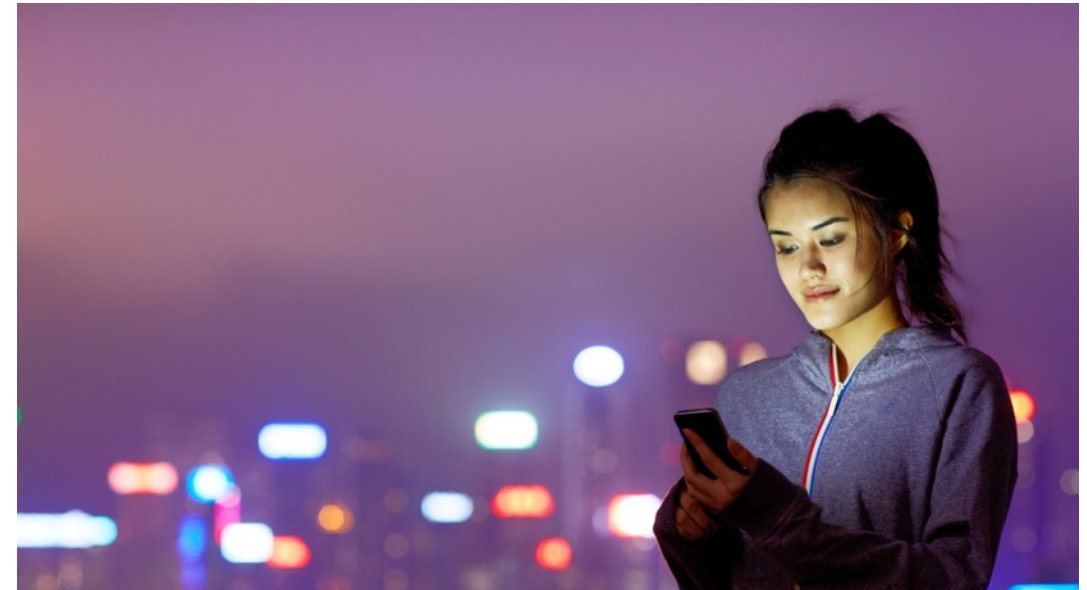
**Use Cases**

03

# Overview / Use Cases

## 2nd Factor Authentication (2FA) / Registration/ Fraud Prevention

Integrating the SIM Swap API into Second Factor Authentication (2FA) workflows enables a stronger user verification during registration. Through the API, you gain the ability to proactively identify and prevent potential fraudulent activities related to SIM swaps. This proactive approach adds an extra layer of protection, ensuring the security of your users' accounts.



<p><b>OTHER RELATED APIs</b></p> <p><b>Device Location</b></p> <p><b>Number Verification</b></p> <p><b>Know Your Customer</b></p>	<p><b>SECTOR</b></p> <p>MEDIA, ENTERTAINMENT &amp; XR</p>	<p><b>DEVELOPER NEEDS</b></p> <ul style="list-style-type: none"> <li>Enhanced User Verification: SIM Swap enables a stronger user verification process, particularly when integrated into Second Factor Authentication (2FA) workflows.</li> <li>User Data Protection: The use of SIM Swap adds an extra layer of protection to users' accounts, safeguarding their personal information from unauthorized access and misuse.</li> <li>Reduction of Identity Theft: SIM Swap helps minimize instances of identity theft by identifying and preventing unauthorized access attempts early in the process.</li> </ul>
	<p><b>SERVICE</b></p> <p>IDENTITY</p>	

# Overview / Use Cases

## Banking transactions (i.e. TAN procedures)

Integrating the SIM Swap API can bolster Transaction Authentication Number (TAN) procedures. By adding an extra layer of verification through SIM Swap, banks can ensure that TAN-based transactions are not only authorized by the user but are also executed through a secure SIM environment, minimizing the risk of unauthorized access and fraudulent actions.

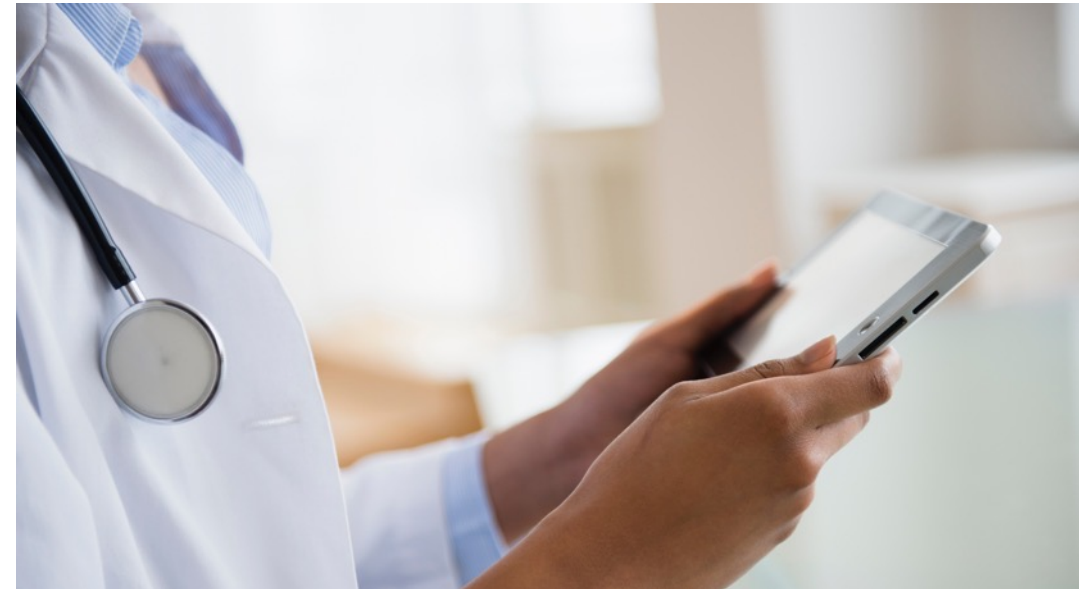


<p><b>OTHER RELATED APIs</b></p> <p><b>Device Location</b></p> <p><b>Device Status</b></p> <p><b>Know Your Customer</b></p>	<p><b>SECTOR</b></p>	<p>FINANCIAL SERVICES &amp; INSURANCES</p>	<p><b>DEVELOPER NEEDS</b></p> <ul style="list-style-type: none"> <li>Efficient Account Openings: The integration of SIM Swap expedites the account opening process by identifying and preventing unauthorized accounts, ensuring that only legitimate customers create accounts.</li> </ul>
	<p><b>SERVICE</b></p>	<p>IDENTITY</p>	

# Overview / Use Cases

## Healthcare Application Access

Incorporating SIM Swap into health applications enhances security for accessing sensitive medical data. SIM Swap aligns with regulations, fortifying digital healthcare. SIM Swap becomes a pivotal tool in securing electronic health records, telemedicine sessions, and remote monitoring systems, contributing to the evolving landscape of healthcare services.

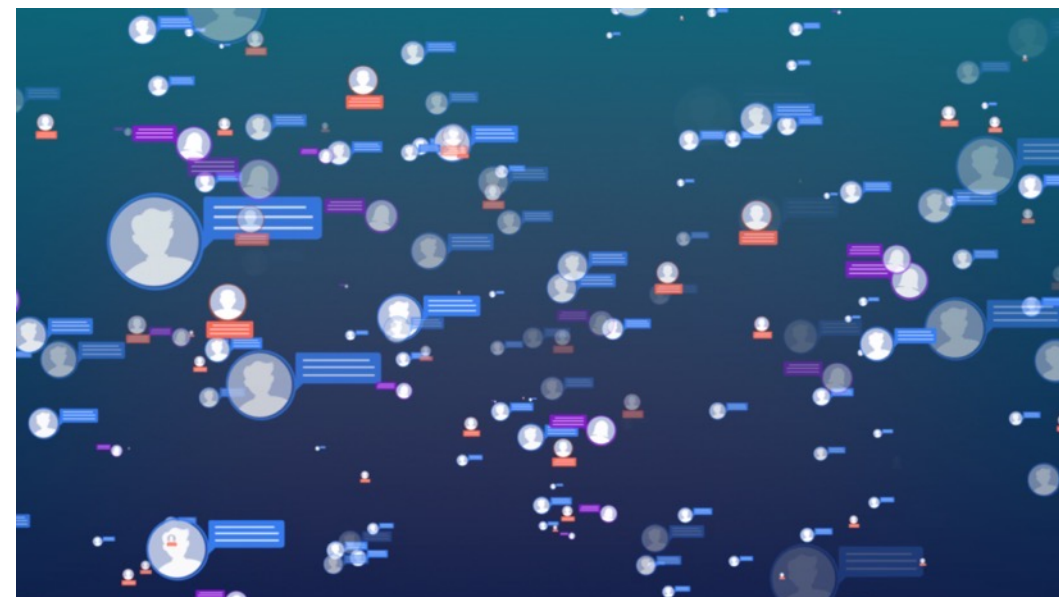


<p><b>OTHER RELATED APIs</b></p> <p><b>Device Location</b></p> <p><b>Device Status</b></p>	<p><b>SECTOR</b></p> <p>ICT SERVICES</p>	<p><b>DEVELOPER NEEDS</b></p> <ul style="list-style-type: none"> <li>Regulatory Compliance: Healthcare data is subject to strict regulations. SIM Swap's enhanced security measures aid in meeting compliance requirements, reducing the risk of legal and regulatory consequences.</li> <li>User Trust and Confidence: Users, especially patients, seek applications that prioritize their data security. Integrating SIM Swap enhances user trust by demonstrating a commitment to safeguarding their personal health information.</li> </ul>
	<p><b>SERVICE</b></p> <p>IDENTITY</p>	

# Overview / Use Cases

## Account Takeover Protection in Social Networks

Fraudsters frequently employ identity impersonation as a tactic within social networks. To counter this, leveraging the capabilities of the SIM Swap API becomes pivotal. Social networks can proactively monitor and identify suspicious SIM swap activities linked to user accounts. This proactive approach not only safeguards user identities but also bolsters the overall security of the platform, enhancing trust and ensuring genuine interactions among users.



<b>OTHER RELATED APIs</b>  <b>Device Location</b>  <b>Device Status</b>	<b>SECTOR</b>	SOCIAL & CUSTOMER ENGAGEMENT	<b>DEVELOPER NEEDS</b> <ul style="list-style-type: none"> <li>• Mitigation of Impersonation Threats: The solution addresses the specific threat of impersonation by identifying and thwarting fraudulent SIM swap attempts.</li> <li>• Genuine User Interaction: Preventing account takeovers leads to genuine user interactions, enhancing the authenticity and credibility of the social network platform.</li> <li>• Trust Building: Implementing the SIM Swap API builds user trust by assuring them of a safer online environment, minimizing the risk of identity-related fraud.</li> </ul>
	<b>SERVICE</b>	IDENTITY	

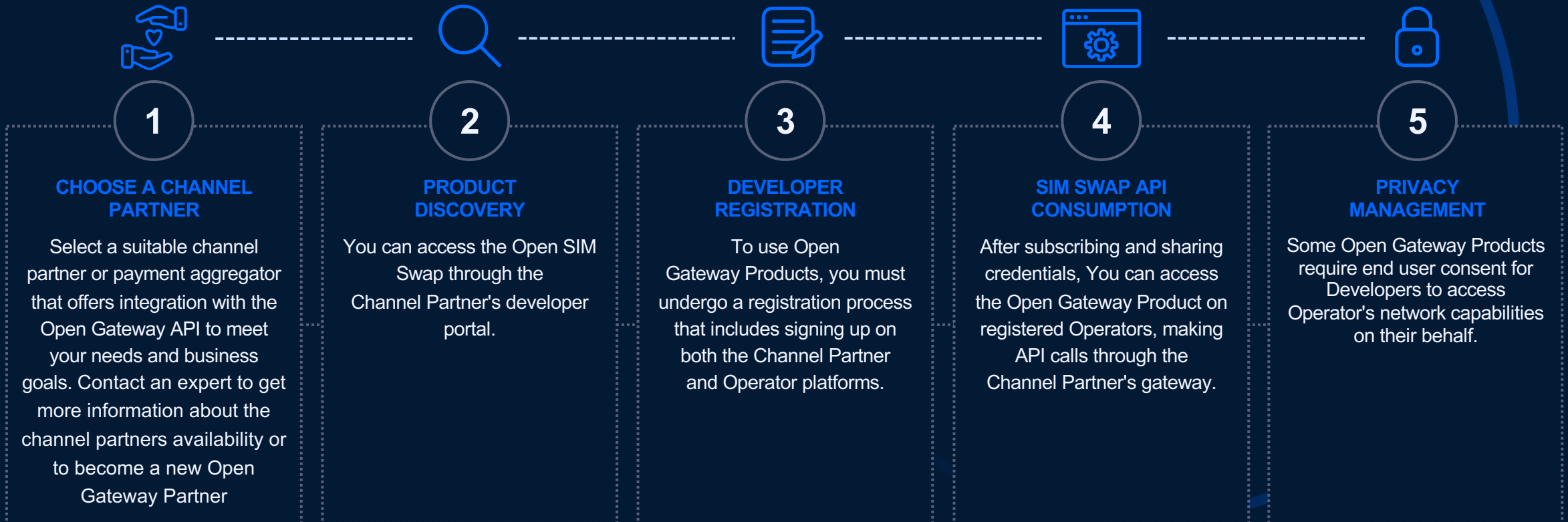
**Start using  
SIM Swap API!**

04

# Getting Started with SIM Swap API

Harness the power of Open Gateway and seamlessly integrate our API services into your app

Follow these initial steps for seamless API services to Developers within Channel Partners' environments, including Operators API Services integration for a cohesive product experience and efficient collaboration among stakeholders.



**Documentation**

05



# Official SIM Swap CAMARA API Documentation

## Over CAMARA

CAMARA is an open-source project within Linux Foundation to define, develop and test the APIs. CAMARA works in close collaboration with the GSMA Operator Platform Group to align API requirements and publish API definitions and APIs. Harmonization of APIs is achieved through fast and agile created working code with developer-friendly documentation. API definitions and reference implementations are free to use (Apache2.0 license).

## Camara is supported by:



### Meetings

- Regular Virtual Meetings
- Bi-weekly on Thursdays
- 8:30 to 9:30 CET

### Contributor ship & Mailing List

✓ [Subscribe](#)

### SIM Swap (Subproject)

✓ [CAMARA SIM Swap GitHub](#)

**FAQs**

06

# API SIM Swap / FAQs

## What is the CAMARA SIM Swap API?

The SIM Swap API is a technology solution that allows developers to integrate the functionality of detecting and managing SIM card swaps into their applications. It helps enhance security by identifying potential fraudulent activities and providing an extra layer of protection against unauthorized access.

## How does the SIM Swap API work?

The API works by interacting with the mobile network's data to monitor SIM-related activities. It detects any anomalous behavior, such as sudden or multiple SIM changes, which could indicate potentially fraudulent activities. When such activities are detected, alerts can be triggered, allowing for real-time response and preventive measures.

## What are the benefits of using the SIM Swap API?

Using the SIM Swap API provides several benefits, including improved security, fraud prevention, enhanced user verification, and the ability to proactively respond to potential threats. It strengthens authentication methods and helps maintain the integrity of user accounts.

## In which use cases can the SIM Swap API be applied?

The SIM Swap API can be integrated into various use cases, including banking transactions, two-factor authentication, healthcare applications, e-commerce, government services, and more. It can enhance security and prevent unauthorized access in scenarios where user identity is critical.

## How does the SIM Swap API prevent fraud?

By monitoring and analyzing SIM-related activities, the API can identify suspicious patterns that might indicate fraudulent behavior. The API also sends the timestamp of last MSISDN <-> IMSI pairing change for a mobile.

## How does the SIM Swap API enhance user experience?

By preventing unauthorized access and fraudulent activities, the API enhances user trust and confidence in applications. Users can feel more secure knowing that their accounts are being protected by proactive measures against identity theft and unauthorized access.

## API SIM Swap / FAQs

### How does the SIM Swap API integrate with existing security measures?

The SIM Swap API complements existing security measures by adding an additional layer of protection. It works alongside authentication methods like passwords, two-factor authentication, and biometrics to enhance the overall security posture of an application.

### Can the SIM Swap API be used in combination with other security solutions?

The SIM Swap API can be used in conjunction with other security solutions, such as device isolation and device status (roaming). Integrating multiple layers of security can create a more comprehensive and robust defense against various threats.

### What is the benefit of early detection through the SIM Swap API?

Early detection helps prevent potential financial losses by identifying and addressing suspicious SIM-related activities before they lead to unauthorized access and transactions. This proactive approach safeguards both user accounts and businesses' bottom lines.

### Can early detection minimize reputational damage?

Absolutely, early detection minimizes the risk of reputational damage caused by security breaches. By nipping potential threats in the bud, businesses can avoid negative publicity and maintain a positive brand image.

**Other relevant  
information**

07

# Discover more

## Join our Developer Hub

Join the [Telefónica Open Gateway Developer Hub](#) to test our APIs, develop use cases with the power of the network and improve user experiences.

## Enroll our Partner Program

If you are interested in the potential of Telefónica Open Gateway and you are willing to collaborate with us, you can [enroll our exclusive Partner Program](#).

## Subscribe our newsletter

Find out all about the latest of Telefónica Open Gateway in our [newsletter](#).

## Contact our experts

If you have any questions about the initiative, don't hesitate to [contact our experts](#).





Telefónica