Telefónica

Whitepaper

Architecture, requirements and use cases of the SIM Swap Open Gateway API

Telefónica Open Gateway

11 October 2023 v1.0

Index

1. Introducción

1.1 Document Objective

The objective of this whitepaper is to provide a comprehensive understanding of the CAMARA SIM Swap API, focusing on its role in helping companies to mitigate risks related to account takeover. It aims to cater to a technical audience, including developers, engineers, and integration specialists, who are seeking to implement the API within their systems.

By delving into the intricacies of the CAMARA SIM Swap API, this whitepaper aims to:

- Clearly articulate the purpose and functionality of the API.
- Provide technical insights and guidance on integrating and leveraging the API effectively.
- Showcase the advantages and benefits of adopting the CAMARA SIM Swap API for aggregators and service providers.
- Highlight best practices, recommendations, and real-world case studies to illustrate successful API implementations.

Through this document, readers will gain a solid understanding of the API's architecture, components, integration requirements, security considerations, and the overall workflow involved in leveraging SIM Swap capabilities. It aims to empower technical professionals with the knowledge and tools necessary to integrate the CAMARA SIM Swap API seamlessly into their systems, enhancing their strategies to prevent digital identity fraud.

1.1.1 SIM Swap is about account takeover

The mobile phone is the most common device to manage many kinds of products and services: from your food delivery or gym account to your car insurance or your bank account. In all of them, you have your own service account to do many types of transactions.

But account takeover is one of the most impactful ways of fraud. When a fraudster manages to control a user’s account, they can take advantage of all the functionalities associated with the account. The fastest way to monetize this fraud is transferring money or making purchases. But other problems can also occur, like making the real customer be involved in criminal acts.

1.1.2 How are SIM cards used by Telco operators?

The SIM card is a card inside the mobile phone, and it is identified by a number. The telco operator keeps a link between that number and your phone number. If your phone number gets linked to another SIM card different from yours, phone calls and SMSs will go to a different mobile phone than yours. At this point, the “new” mobile phone can be used, for example, to reset passwords, and then, to validate fraudulent transactions.

1.1.3 How can a fraudster take over my App account using SIM Swap?

The usual procedure to get a new SIM card linked to your phone number is to make the telco operator generate a new SIM card pretending that the original SIM card has been lost, damaged or stolen.

So, the first step for fraudsters to get prepared for requesting this SIM renewal is to get personal information about the user. In fact, they often get prepared gathering information about several users to maximize the monetization of their efforts. They can exploit data breaches in service providers, get the information from illegitimate providers that sell data, use spyware that sends data to them, analyze your social networks to collect the data, or get the information by using phishing techniques. Smishing is a particularly effective phishing strategy that consists of sending an SMS notifying, for example, a hypothetical unsuccessful parcel delivery, and asking the user to confirm personal data to arrange a new delivery.

STEP 1
Fraudster collects personal information, mostly using phishing strategies.

STEP 2
Using the personal data collected, fraudster impersonates user to ask the Telco operator for a new SIM.

STEP 3
Fraudster appropriates the account and make transactions. This step can be stopped by using SIM Swap API.

The second step for fraudsters is to ask the Telco operator of the user for a SIM renewal. The telco operator must follow a strict procedure to ensure that such a request is legitimate, but a compromise must be reached between making it easy for a legitimate user and making it difficult for a fraudster. This procedure often includes asking the requester about personal information that is supposed to be known only by the user and the operator. Given that the fraudster has managed to gather such information, there is a chance for them to success.

Once the fraudster has the new SIM, they already can take advantage of the usual procedures to validate accounts: they can intercept second factor authentication procedures where the second factor is an SMS, they can make or receive verification calls, etc. By doing so, they gain full control of almost any kind of digital account.

Finally, the fraudster uses the account to, for example, make money transactions, purchases of products, or even purchases of cryptocurrencies to make it more difficult to trace the money.

1.2 How does the SIM Swap API help prevent fraud?

The first step to prevent identity fraud is for users to keep their personal data safe. But given the use of digital services is getting more and more widespread, this is increasingly difficult.

Fortunately, besides Telco operators are always improving procedures to minimize the risk of fraudulent SIM renewal requests, such requests are always completely registered and documented, and can be used as fraud alerts when suspicious transactions are detected.

Thus, the last step described in the previous section can be stopped. For example, if a bank detects an unusual payment or money transaction, they can ask the corresponding Telco operator whether a SIM renewal has been done recently for that user, and even how recent the SIM renewal was. The response will help the bank to confirm the initial suspicion.

So, any kind of digital service provider can protect the transactions of their customers against identity fraud related to SIM Swap events.

1.3 SIM Swap API in CAMARA

The GSMA Open Gateway initiative, led by the GSMA (Global System for Mobile Communications Association), aims to drive collaboration and interoperability among telcos, aggregators, and service providers in the mobile ecosystem. It provides a platform for industry stakeholders to develop and deploy innovative mobile services, including digital identity solutions.

By participating in the GSMA Open Gateway initiative, telcos and aggregators can leverage the collective expertise and resources of the mobile industry to accelerate the adoption of digital services in different business scopes.

Figure 1: Logo for the CAMARA Project within Linux Foundation.

In the previous sections, the way SIM Swap API helps in preventing fraud has been explained. The mechanism underneath has been used in the industry in several ways for years. Now, the API itself has been standardized in the CAMARA Telco Global API Alliance, facilitated by the GSMA. The CAMARA standardization of this API brings together telcos and service providers from around the world to establish best practices, share knowledge, and promote industry-wide cooperation. As a result, in the scope of the Open Gateway initiative, this API can be integrated by any kind of company in the digital services industry around the world in an easy, fast, and seamless way.

2. Overview of the SIM Swap CAMARA API

2.1 Definition of the SIM Swap CAMARA API

The SIM Swap CAMARA API is a software interface that enables applications to request the last date of a SIM swap performed on the mobile line, or to check whether a SIM swap has been performed during a past period. This is provided in an easy and secure way, checking in real-time the activation date of a SIM card on the mobile network.

The API specifies the following two operations:

- `POST retrieve-date`: answers the question 'when did the last SIM swap occur?'. This operation just needs the phone number to be checked (parameter 'phoneNumber').

- `POST check`: checks whether a SIM swap occurred during last N hours?. This operation needs the following inputs:

    - 'phoneNumber': the phone number to be checked.

    - 'maxAge': the period in hours to be checked for SIM swap (minimum 1h, maximum 2400h, default 240h).

With the SIM Swap CAMARA API, any digital service provider can integrate the functionality of checking changes in SIM renewals directly into their software. Both alone and combined with other external inputs. Also, they can combine other Open Gateway APIs related to the anti-fraud scope that may be considered of interest.

Aggregators are important actors in the anti-fraud industry. They can integrate this functionality into their software and build more sophisticated algorithms integrating other security checks related to, for example, location verification, phone number verification, matching of contact information, external data sources, AI algorithms, etc. To do so, the aggregators can use other Open Gateway APIs such us Device Location Verification, Number Verify or KYC-Match.

2.2 Advantages and benefits of using SIM Swap API

The CAMARA SIM Swap API offers numerous advantages and benefits for the industry interested in enforcing identity protection. Here are some key arguments highlighting the advantages of using the CAMARA API:

1. **Two-Factor Authentication reinforcement:** SIM Swap enforces the security of the procedures that involve two-factor authentication based on SMSs. When

these procedures are used it is important to verify whether the mobile device involved in the second factor has been compromised by a SIM Swap. By using this verification, you are protecting your customer's account and your own business.

2. **Secure account creation:** thanks to the SIM Swap API, it is 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. This can be applied to any industry sector (e-commerce, in-app purchases, etc.) but it is particularly crucial in the context of banking transactions.

3. **Anti-fraud suite:** SIM Swap is just one of the Open Gateway APIs related to the protection of the customers identity in the scope of mobile digital services. Other APIs can be used to enforce this protection in different circumstances and use cases. For example, the APIs Number Verification, Device Location Verification, and Know Your Customer - Match, among others.

4. **Usability:** The CAMARA API is designed to be developer-friendly and easy to set up and use. It simplifies the integration process for telcos and any kind of clients, allowing them to offer SIM Swap as an option to check SIM renewals.

5. **Footprint:** The CAMARA standardization of SIM Swap guarantees a common accesso to the functionality across Telco operators and countries.

6. **Security:** The CAMARA guidelines guarantees a common privacy and security framework that tackles the needs of the service providers while preserving the rights of the customers and.

2.3 Common Use Cases

In this section, we will explore two common use cases for the SIM Swap CAMARA API, highlighting its relevance and benefits in the following domains: Gaming, Mobility (Smart Cities), and Live Sports Streaming (OTTs).

2.3.1 Protecting financial transactions

This is the basic use case that has been used as an example in the first sections of this document.

Financial companies are especially sensitive to fraud because the impersonation of a customer can result in direct, immediate, and crucial consequences. However, since the mobile phone is usually in the path of many digital transactions, clues about fraud attempts due to the SIM Swap mechanism can also be digitally detected. Thus, these attempts can be stopped when a suspicious SIM change is detected.

Figure 2: SIM Swap API helps you protect financial transactions.

Developer needs:

- Mitigate the risk of fraud due to the takeover of an account originated by a SIM Swap.
- Integrate the functionality of checking the age of a SIM in a fast and simple way.
- Having such information in real-time protects live transactions.

Additional use cases:

- Many companies where mobile payments are involved (e-commerce, gaming, in-app purchases, etc.) can be very interested in ensuring transactions protecting them from this kind of identity fraud.

2.3.2 Adding up functionalities to build sophisticated anti-fraud strategies

Aggregators and software companies play a fundamental role in the anti-fraud industry as they can integrate disparate inputs to evaluate identity risks and other kinds of vulnerabilities. For example, a company can use AI to read information from the ID card of a customer in an onboarding procedure and, at the same time, verify whether that data corresponds to the phone number given by the customer, verify the expected location, and ensure that the customer is not being victim of a SIM Swap.

Such combinations are easy to integrate due to the benefits of standardization of the anti-fraud suite of APIs in CAMARA.

Figure 3: Aggregators can combine Open Gateway APIs and external APIs to build sophisticated anti-fraud strategies.

Developer needs:

- Build sophisticated algorithms to evaluate fraud risks in different circumstances.
- Integrate disparate functionalities all following the same criteria regarding software implementation, privacy framework and through different telco operators.

3. Architecture and Components

3.1 High-Level Architecture

The following figures describe the high-level architecture of the three scenarios where SIM Swap CAMARA API can be used.

The first figure represents the scenario where a Service Provider uses the SIM Swap API from the marketplace of a Hyperscaler (e.g., Azure, AWS, Vonage, Google). The Service Provider uses the provided SDK to implement the integration with the API. In this way, the Service Provider can directly use the SIM Swap API. In fact, they could also use any other available APIs (whether they are related to the anti-fraud suite or not).

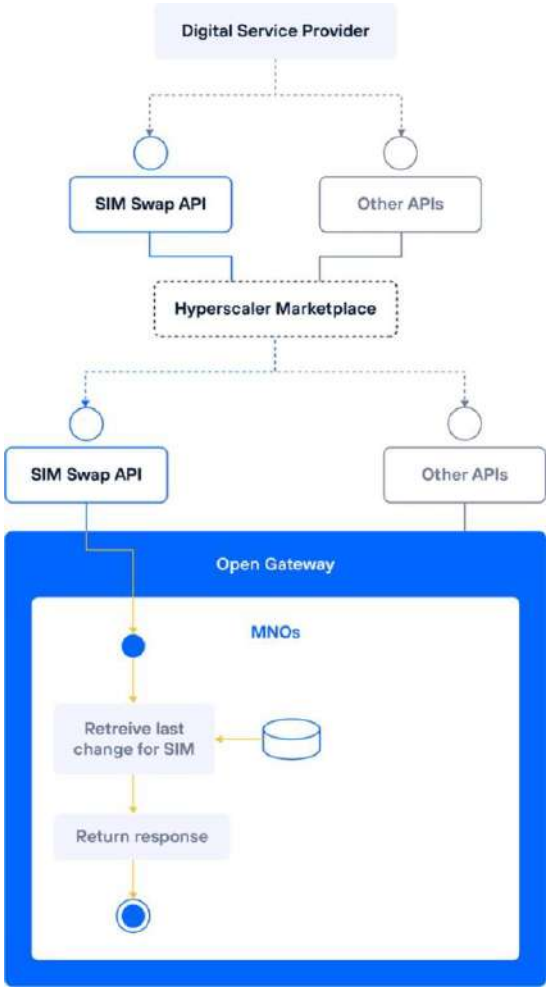


Figure 4: SIM Swap API used from a Hyperscaler's Marketplace

The second figure represents the scenario where a Service Provider uses the SIM Swap API from the service provided by an Aggregator. The Aggregator could build a sophisticated identity service by combining multiple APIs from Open Gateway, other external APIs, implementing their own in-house products, etc.

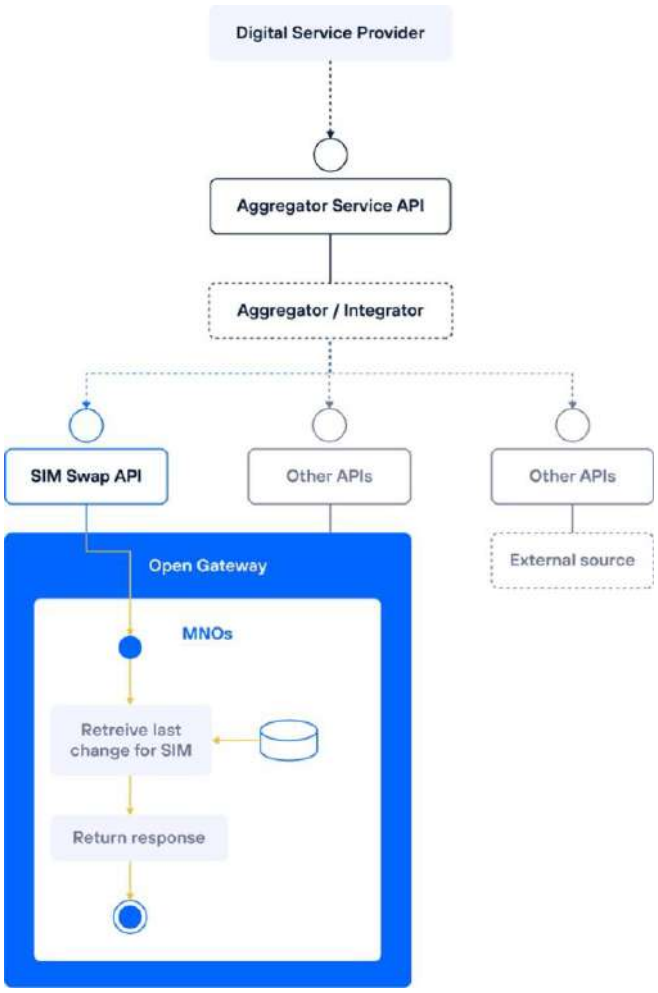


Figure 5: SIM Swap API used from the service of an Aggregator or Integrator

The third figure represents the scenario where a Service Provider uses the SIM Swap API directly from Open Gateway. It can be either integrating with operators or using a kind of gateway to them.

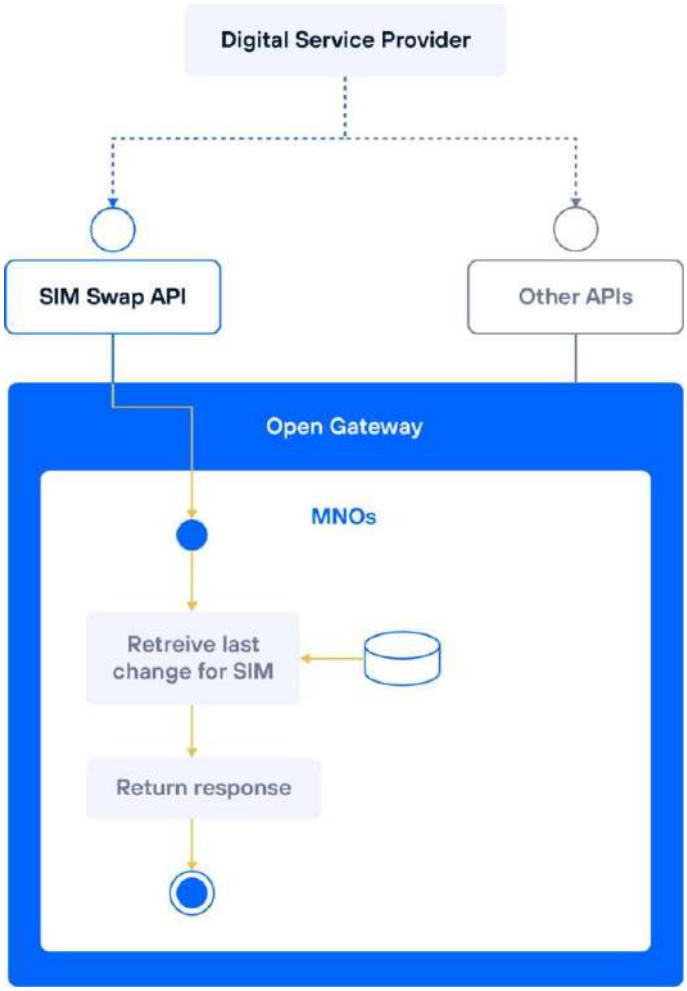


Figure 6: SIM Swap API used directly integrating with Telco operators.

- **Digital service provider:** this is the company interested in protecting their business and their customers from any identity fraud related to SIM Swap. When using the SIM Swap API from a Hyperscaler, the digital service provider must implement the request to the API by using the SDK provided by the Hyperscaler in the marketplace. When using the SIM Swap API from an Aggregator, the digital service provider must implement the request to the API exposed by the Aggregator. Such API could be non-standard but could give added value to the service provider.

- **Hyperscaler:** they are usually cloud players that provide marketplaces where APIs and other services can be contracted by clients that are used to consume cloud products. In this case, they reach agreements with MNOs in the Open Gateway

context to publish their APIs and then they set prices and conditions to the consumption of their products by the digital service providers.

- **Aggregator/Integrator:** the role is similar to the hyperscaler's one, but they can aggregate services to provide digital service providers with more sophisticated products and personalized experiences.
- **Open Gateway Operator platform:** the hyperscalers and aggregators set up integrations with the MNOs in the Open Gateway context.

3.2 How to use the API: workflow and implementation

The workflow consists just of sending the SIM Swap request and getting the corresponding response. There are two possible operations in the API.

The operation '**retrieve-date**' returns the last change of the SIM card associated to the phone number. The following figure represents the workflow for this operation and then, an example of request and response is included.

Request example:

```
{
      "phoneNumber": "34666111333"
}
```

Response example:

```
{
      "latestSimChange": "2019-08-24T14:15:22Z"
}
```

The operation '**check**' returns whether a change of the SIM card associated to the phone number happened in the last N hours specified by the 'maxAge' parameter. The minimum value for 'maxAge' is 1 hour, the maximum is 2400 hours, and the default value is 240 hours.

Request example:

```
{
      “phoneNumber”: “34666111333”,
      “maxAge”: 240
}
```

Response example:

```
{
      "swapped": "true"
}
```

Apart from the explicit definition of the API requests, when the API is used from the marketplace of a Hyperscaler, an SDK will be provided to make the corresponding requests. The objective of such SDK is to make it easy to integrate the API call into the software of the developer. The following is **just an indicative example of how the SIM Swap 'retrieve' operation could work using Python**:

```
from Example.OpenGatewaySDK import SimSwap

simSwapClient = SimSwap(credentials, phoneNumber)
maxAge = 48

# One-line Open Gateway query (returns true or false)
swapped = simSwapClient.check(phoneNumber, maxAge)
```

4. Technical Requirements and Considerations

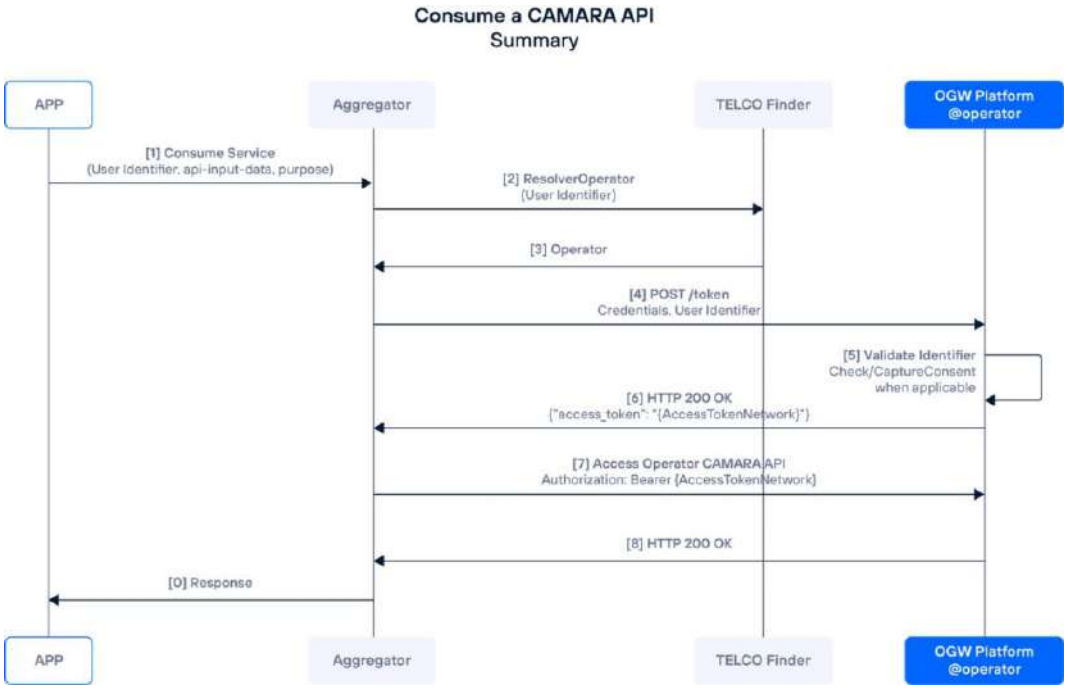
This chapter provides a comprehensive overview of the integration flows needed for seamless integration with the Open Gateway Operator platform (API Gateway).

4.1 Transparency Considerations

For certain Open Gateway products, explicit consent from the end user is required, especially during the initial usage, to authorize the Developer to access and utilize the network capabilities provided by the Operator through the Open Gateway.

It is important to note that the responsibility of collecting the final user's consent lies with the Operator, not the Channel Partner. Since the Operator is the provider of the network capabilities involved in the API consumption, they are responsible for managing the necessary consent from the end user. Although the legal basis for this API is Legitimate Interest, it is essential for the operators to manage the potential opt-out made by the user. To facilitate this process, the Operator may want to notify the end users their right to opt-out for the use of this API.

In the following consumption flow of CAMARA APIs, some parts like consent capture are not depicted for simplicity. The flow enables the aggregation platform to access and utilize the APIs securely and compliantly. It ensures that user privacy is respected, and legal requirements are met, allowing for various use cases like fraud prevention, service delivery, and quality of service optimization. The diagram provides a high-level overview of the flow, serving as an introduction to the general structure and interactions involved in consuming CAMARA APIs.



The initial step involves the application utilizing an aggregator service that requires a specific network capability provided by an operator. The aggregator receives a user identifier from the application (Step 1).

To determine the user's operator, the aggregator employs the telco finder mechanism (Steps 2-3). This allows the aggregator to identify the corresponding telco server it needs to communicate with, utilizing the CAMARA API.

Prior to invoking any CAMARA API, user authentication with the telco operator is necessary. This authentication process follows the standardized OpenID Connect (OIDC) mechanism, utilizing a backend-based OAuth2 Grant (such as CIBA or JWT-Bearer). This process enables user identification based on the provided user identifier. Additionally, consent verification and capture occur if required but not yet granted. If successful, the aggregator obtains an OAuth2 access token (Steps 4-6).

With a valid access token, the aggregator can proceed to invoke the operator's CAMARA API, as depicted in the final stages of the flow (Steps 7-8).

At this point, the aggregator can verify the application's authenticity and provide relevant information based on the specific use case (Step 9).

5. API Documentation

The SIM Swap API is standardized in CAMARA, and the corresponding documentation is in this repository at GitHub:
https://github.com/camaraproject/SimSwap

The version of the specification explained in this document is 0.4.1, which can be found in this link:
https://github.com/camaraproject/SimSwap/blob/main/code/API_definitions/sim_swap.yaml

The operations defined in the specification have been explained in this document in the section How to use the API: workflow. The CAMARA specification itself includes more documentation about the objective and use of the API.

6. Conclusions

The integration of the SIM Swap CAMARA API makes a relevant contribution to anti-fraud strategies in different scenarios: onboarding of users, protecting users' accounts

to be stolen, reducing risk of monetary losses for service providers and customers, and enforcing security of sensitive identity procedures.

On the one hand, it can be used directly by clients interested in this particular functionality and even combining it with other Open Gateway or external functionalities. On the other hand, aggregators and integrators can build sophisticated products and services on top of these functionalities. They can add up other sources of information and in-house developments to create new added value services. This can include AI products to help in the safety of identity and account protection.

Furthermore, the integration process itself has been streamlined, with easy-to-use documentation and smooth implementation experience. This has facilitated the adoption of the API by any kind of companies, enabling them to quickly leverage SIM Swap capabilities and improve the protection of their business and customers.

7. Other relevant information

You can join now the Telefónica Open Gateway Developer Hub to test our API, develop use cases with the power of the network and improve user experiences.
Join Developer Hub

If you are interested in the potential of Telefónica Open Gateway and you are willing to collaborate with us, you can access our exclusive Partner Program:
Join Partner Program

For further questions about the initiative, don't hesitate to contact our experts:
Contact our experts

8. References and Additional Resources

8.1 Additional information about Telefónica Open Gateway Initiative

Learn more about the SIM Swap API and other Open Gateway APIs and services in Telefónica in our website: https://opengateway.telefonica.com/

8.2 Additional information of the SIM Swap CAMARA API

The SIM Swap CAMARA API official documentation is collected in the following GitHub Repository:
https://github.com/camaraproject/SimSwap

8.3 Glossary of Terms

TERM	DEFINITION
Aggregator	Aggregator or 'Channel Partners' aggregate Operator's CAMARA standardized APIs to build Open Gateway-based services and implement Operator end-point routing based on final user identification on the network.
API Gateway	An intermediary platform that allows communication between different systems and APIs, providing a centralized and standardized approach for accessing and utilizing APIs. The Open Gateway operator platform is the API GW platform in the operator that exposes standardized APIs so third-party services can consume them in a secure and consistent way. Operator platform APIs are based on REST/HTTP. OAuth 2.0 and OpenID Connect are standard security mechanisms to control access to the APIs. APIs are reachable from the Internet and all traffic is encrypted with TLS.
AuthCode	Authentication method to validate the user's identity during the authentication process.
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). The tool to manage the work and outcomes of the APIs standardization at CAMARA is GitHub: https://github.com/camaraproject
SIM Swap	This refers to the act of asking a telco operator for a new SIM card arguing that the original one has been lost, damaged or stolen. When the new SIM card begins to be in force, the old one becomes invalid, and it is said that a SIM swap has happened. This can be a legitimate action. But

	this API helps to detect whether it happens due to an illegitimate action or not.
Consent	The explicit permission given by the user for the processing of their personal data, as required by privacy regulations such as GDPR (General Data Protection Regulation).
IDP	Identity Provider, a service that authenticates and verifies the identity of users.
Open Gateway	An industry initiative led by GSMA (Global System for Mobile Communications Association) that transforms telecom networks into future-ready platforms, enabling seamless integration and access to telco capabilities through standardized APIs.
Open Code Repository	A platform or repository where developers can access and collaborate on open-source code and projects, such as GitHub.
OAuth 2.0 / OpenID Connect	Standards and protocols for user authentication and authorization, allowing secure access to APIs and services.
Privacy-by-Default	A principle that ensures privacy protection is integrated into systems and processes by default, requiring explicit user consent for the processing of personal data.
SDK	Software Development Kit, a set of tools, libraries, and documentation that enables developers to build applications for a specific platform or system.
User Identifier	A unique identifier associated with a user, such as an IP address or MSISDN, used for authentication, routing, and identification purposes.

opengateway.telefonica.com