PAiCore TECHNOLOGY

Open Source Telecom Signaling

PAiCore Network APIs: Sample Use Cases

Reigniting telecom innovation and sustainable profitability via open source signaling solutions

Overview

PAiCore's Network API Platform exposes eight CAMARA-aligned APIs that let a business replace guesswork and SMS codes with answers from the operator's network and systems. This document shows where each one fits in real customer journeys.

Capabilities at a glance

API	Functional use
Silent Network Authentication	Authenticates a mobile user through the device's SIM, without passwords, SMS codes or user interaction
Number Verification	Confirms that a phone number belongs to the device using the service, by network-based or SIM-based verification
SIM Swap	Shows when the SIM behind a number last changed, or whether it changed recently, to flag account takeover risk
Location Retrieval	Returns the geographic area where a mobile device is located
Location Verification	Confirms whether a mobile device is within a specified geographic area
Geofencing Subscriptions	Notifies a service when a mobile device enters or leaves a defined geographic area
Know Your Customer Age	Confirms whether a subscriber is above an age threshold, without sharing their birth date
One-Time Password SMS	Sends a one-time code by SMS and verifies the code the user enters

All eight run on one platform: customer onboarding, OAuth clients registered for a declared purpose, subscriptions and rate-limit tiers, and a usage record for every call.

Use cases by industry

Banking

Use case	APIs	Description	Outcome
Silent login on mobile	Silent Network Authentication or Number Verification	The app authenticates the user through the device's SIM or mobile data session	Login with no SMS code or password step
Payment approval	Silent Network Authentication	Re-authenticates the customer silently before a payment is approved	Strong authentication without interrupting the payment
Password or PIN reset	SIM Swap	`check` with a short `maxAge`, such as 72 hours, before the reset is allowed	A recent swap routes the reset to a stronger factor or a branch
New payee or high-value transfer	SIM Swap	`retrieve-date` feeds the date of the last SIM change into the risk score	Transfers on a freshly swapped number are held for review
Card-not-present fraud screening	Location Verification	Checks whether the customer's phone is in the area of the transaction	A `FALSE` adds risk weight; `PARTIAL` is treated as uncertain
Travel-aware card controls	Geofencing Subscriptions	Notifies the bank when the customer's phone leaves or re-enters the home country	Card rules adjust to travel, with fewer false declines
Customers without mobile data	One-Time Password SMS	Sends a code to the registered number when silent authentication is not possible	Every customer can complete authentication

Fintech, mobile money and crypto

Use case	APIs	Description	Outcome
Wallet registration	Silent Network Authentication or Number Verification	The app authenticates the user through the device's SIM or mobile data session	Login with no SMS code or password step
Transaction confirmation	Silent Network Authentication	Re-authenticates the customer silently before a payment is approved	Strong authentication without interrupting the payment
Password or PIN reset	SIM Swap	`check` with a short `maxAge`, such as 72 hours, before the reset is allowed	A recent swap routes the reset to a stronger factor or a branch
Withdrawals and cash-out	SIM Swap	`retrieve-date` feeds the date of the last SIM change into the risk score	Transfers on a freshly swapped number are held for review
Device change or SIM change recovery	Location Verification	Checks whether the customer's phone is in the area of the transaction	A `FALSE` adds risk weight; `PARTIAL` is treated as uncertain
Agent network oversight	Geofencing Subscriptions	Notifies the bank when the customer's phone leaves or re-enters the home country	Card rules adjust to travel, with fewer false declines
Feature-phone and low-data users	One-Time Password SMS	Verifies users by SMS code where silent methods are not available	Inclusion of basic handsets without weakening verification

Marketplaces, delivery and ride-hailing

Use case	APIs	Description	Outcome
Sign-up	Number Verification	Silent check of the number at registration	Fewer fake accounts and no SMS cost per sign-up
Returning-user login	Silent Network Authentication	Signs users in silently on mobile	Faster checkout and fewer abandoned sessions
Payout account changes	SIM Swap	`check` on the seller's or driver's number	Payouts are protected against account takeover
Driver or courier presence	Location Verification	Confirms the device is in the expected pickup or service area	Fewer location-spoofing claims
Arrival and departure alerts	Geofencing Subscriptions	Subscribes to a courier's device entering or leaving a delivery area	Customers are notified automatically, with no tracking app on the phone
Delivery handover	One-Time Password SMS	Sends a code to the recipient that the courier enters at handover	Proof of delivery to the right person

Retail, logistics and field services

Use case	APIs	Description	Outcome
Fleet arrival and departure	Geofencing Subscriptions	Subscribes to drivers' devices entering or leaving depots and customer sites	Automatic arrival records and dispatch updates
Click-and-collect arrival	Geofencing Subscriptions	Notifies the store when a consenting customer's phone enters the pickup area	The order is ready on arrival
Field workforce check-in	Location Verification	Confirms a technician is at the job site when a visit is logged	Verified site visits
Driver location on demand	Location Retrieval	Retrieves the area of a driver's device	Location visibility without a tracking app

Age-restricted services

Use case	APIs	Description	Outcome
Online gaming, alcohol, tobacco, adult content	KYC Age Verification	Sends the number and the age threshold	A yes or no answer; the service never receives the birth date

Aggregators and CPaaS

Use case	APIs	Description	Outcome
Safer OTP delivery	SIM Swap, One-Time Password SMS	Checks the number for a recent SIM change, then sends and verifies the code	A premium "verified OTP" product
Silent verification alongside SMS	Number Verification, One-Time Password SMS	Offers network verification first, with an SMS code as fallback	Lower cost per verification and higher completion
Silent authentication as a product	Silent Network Authentication	Offered to enterprise customers through the same integration as SMS	A higher-value authentication product

Operators

Use case	APIs	Description	Outcome
Launch a GSMA Open Gateway portfolio	All	Exposes CAMARA APIs on existing network elements and BSS, through operator connectors and the NAGw	New API revenue without new core infrastructure
Protect the operator's own channels	SIM Swap, Number Verification	Applied to the operator's self-care app and eSIM transfer flows	Fewer account takeovers and port-out frauds

Combined flows

The APIs are strongest together: Number Verification proves the device holds the number, and SIM Swap shows whether the number has just moved.

Account recovery on a new device

1. Number Verification confirms the new device is using the customer's registered number.
2. SIM Swap `retrieve-date` returns when the SIM last changed.
3. Verified with no recent swap: recovery proceeds. Verified with a recent swap: recovery steps up to a stronger check. Not verified: recovery is refused through this channel.

Digital onboarding for a regulated service

1. Number Verification confirms the number belongs to the device registering.
2. KYC Age Verification confirms the contract holder meets the age threshold.
3. SIM Swap `check` flags numbers whose SIM changed in the last few days.
4. The account opens with no SMS code or document upload for these checks, and risky applications go to manual review.

High-value transaction

1. SIM Swap `check` on the customer's number.
2. Location Verification confirms the device is in the expected area.
3. Both clear: the transaction proceeds silently. Either raises a flag: step-up authentication.

Login with a fallback

1. Silent Network Authentication or Number Verification runs first, with no user interaction.
2. If the device is on Wi-Fi or the check cannot complete, the service falls back to One-Time Password SMS.
3. SIM Swap `check` confirms the number has not just moved to a new SIM before the code is trusted.
4. Most users sign in silently; the rest still complete verification safely.

To discuss a use case or a pilot, visit the PAiCore Network API Gateway or contact our team.