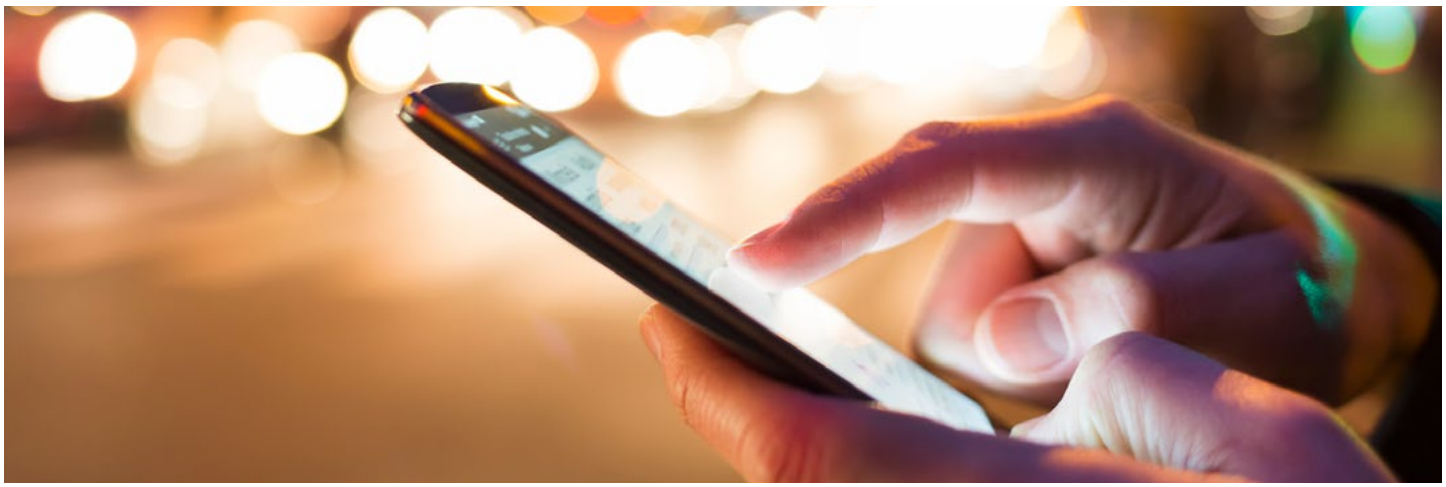
mobile connect

Mobile Connect Link
Delivered by the GSMA

Product Name:	Product Code:
Account Takeover Protection	MC ATP

Mobile Connect Account Takeover Protection

Fraud protection for digital services.



Product Summary

Provides a Service Provider (SP) with an indication of whether the SIM has been swapped in order to mitigate SMS OTP fraud where the mobile device is being used by the SP for 2FA (secondary authentication factor).

How it works

- SP issues a request for the ATP service via the Mobile Connect OIDC API to the user's Operator[1]
- The Operator processes the request and returns a timestamp for the last SIM swap[2] for that particular MSISDN

Example use cases:

- Mitigating fraud against 2FA solutions that utilise either SMS OTP for verifying the user; e.g.:
  - Enhanced fraud checks for payments
  - Securing sensitive banking transactions
- Increasing authentication robustness (by combining MC Authenticate with MC ATP)

Product features/benefits

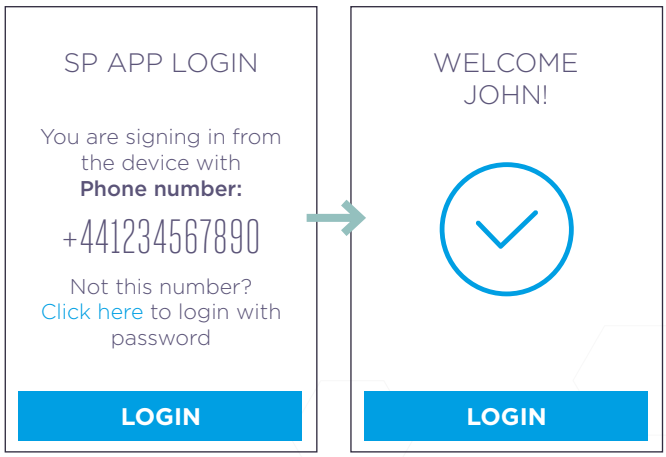
- Unique signals to mitigate the risk of account takeover fraud
  - i.e., whether the user's device has been compromised in an attempt to intercept a 2FA solution to take-over a user's account with the SP
- Verified data from the network (cannot be spoofed by device malware)
- Omni-channel: service can be invoked irrespective of the channel through which the user is interacting with the SP service (e.g., tablet, PC. mobile, Smart TV etc.)
- Single open standard API (OIDC) from multiple operators worldwide and single contract for accessing the service
- Additional information may also be available from the Operator on a case-by-case basis, e.g.:
  - Whether an Unconditional Call Divert has been set (IVR fraud)
  - Whether the device has been reported lost/stolen
  - Whether there has been a device change[3]
  - Mobile account state (active/inactive)

1. The SDK includes a Discovery service to determine the correct Operator for a given user
2. i.e., change in the pairing of IMSI <-> MSISDN
3. Timestamp of last MSISDN <-> IMEI pairing change

Product Specifications

OIDC <scope> value	openid mc_atp
Applicable Authenticators for acquiring user consent	N/A
API	MC OIDC Device-Initiated Profile; MC OIDC Server-Initiated Profile[4]
Input parameters	<scope>= openid mc_atp; MSISDN or PCR[5] of the target user
Service response	PCR; SIM change (timestamp) [Optional]: Unconditional call divert active (Yes/No) (device) Is lost/stolen (Yes/No) Device change (timestamp) Account state (Active/Inactive)
Supported platforms	PHP, JAVA, .NET

Example user flow



End user flow for password-less login

About Mobile Connect

Mobile Connect is a worldwide initiative by mobile operators to bring a wide portfolio of identity services to market that enable SPs and end-users to transact with one-another more securely through strong authentication, authorisation and exchange of user-consented verified information.

For more information please visit **gsma.com/identity** or email us at **mobileconnect@gsma.com.**

4. Server-Initiated mode can be used where the user is not interacting via an IP-connected device
5. Pseudonymous Customer Reference (subject identifier issued by Mobile Connect per user:SP pairing)