mobile connect

Mobile Connect Link
Delivered by the GSMA

Product Name:	Product Code:
Mobile Connect Authenticate Mobile Connect Authenticate Plus	MC Authenticate MC Authenticate Plus

Mobile Connect Authenticate

Simple and secure user authentication on a global scale.

Product Summary

Enables a Service Provider (SP) to authenticate a user via the user's mobile device. Two levels of assurance (LoA) are supported to address different SP needs and use cases (e.g., trade-off between security and user convenience):

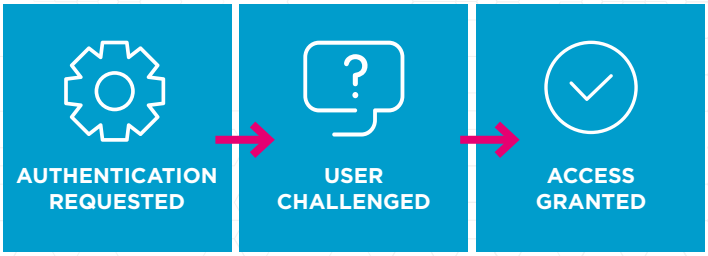
- **MC Authenticate:** 1-factor of authentication (LoA2) = possession & control of the mobile device associated with the target MSISDN
- **MC Authenticate Plus:** 2 factors of authentication (LoA3) = possession & control of the mobile device PLUS either a PIN or biometric (based on authenticator capability)

Where the user is accessing the SP over a mobile network, the MNO can optionally authenticate the user towards the SP without any user interaction to provide a seamless authentication experience (SP choice on whether affirmative user acknowledgement is needed or not).

How it works

- SP issues a request for user authentication (stipulating the required LoA) via the Mobile Connect OIDC API to the user's Operator[1]
- The Operator processes the request and uses an appropriate authenticator (based on the requested LoA) to authenticate the user via their mobile device
- The Operator provides success or failure response back to the SP along with a pseudonymous customer reference (PCR) unique for each user:SP pairing (SP can use this PCR going forward for identifying a returning user or binding to an existing SP user account)

HOW IT WORKS



Example use cases

- Login to a website (user account)
- SMS OTP replacement (ensuring a new user is who they claim to be by verifying the phone number they provide)
- Captcha replacement (proof of human interaction)
- Step-up authentication for high value/sensitive transactions (e.g., online banking) replacing need for costly hardware tokens
- Simpler authentication to Customer Care Centre where user is not interacting via an IP-connected device
- Secure verification for forgotten password and account recovery

Product features/benefits

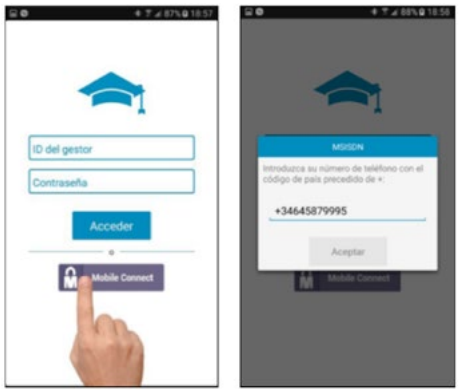
- Simple authentication via user's mobile device without reliance on passwords (option of leveraging biometrics)
- Reduces Fraud by confirming the user is who they say they are when consuming an SP's service
- Supports different levels of assurance to enable SPs to trade-off security vs user convenience based on intended use case
- Seamless authentication option if the user is connected to the SP over the mobile network
- Common authentication experience irrespective of the channel through which the user is interacting with the SP service (e.g., tablet, PC. mobile, Smart TV etc.)
- Underpinned by the security of the mobile network to mitigate device malware, VoIP numbers and SS7 hacks
- Single open standard API (OIDC) from multiple operators worldwide and single contract for accessing the service
- Can be initiated by the end user (e.g., via the user's browser when interacting with the SP website) or by the SP in the background hence supporting a range of diverse use cases
- MC Authenticate can be combined with the MC Phone Number service if the SP would like to receive the user's MSISDN [pending user consent]
- MC Authenticate Plus can be combined with the MC National ID service (where supported) to enable an SP to authenticate a user and obtain information on who that user is (i.e., real identity) [pending user consent]
- MC Authenticate Plus can be combined with the MC ATP service (where supported) to enable an SP to authenticate a user and check that the user's SIM hasn't recently been changed hence providing more assurance that the right person has been authenticated (e.g., LoA3+)

1. The SDK includes a Discovery service to determine the correct Operator for a given user

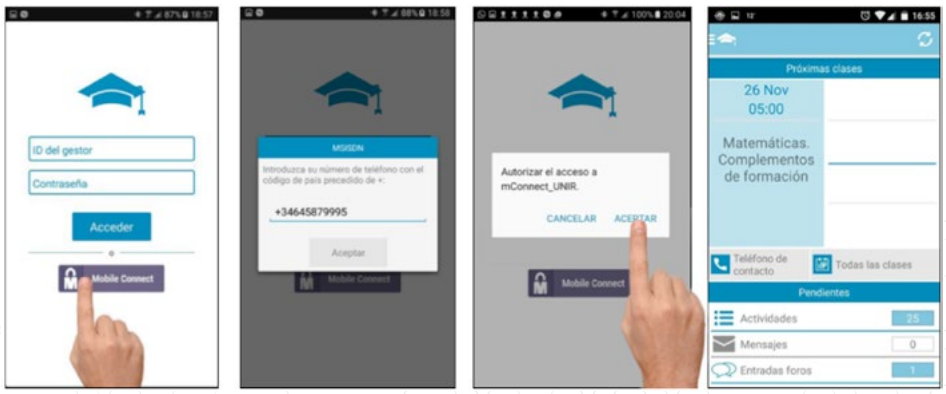
Product Specifications

OIDC <scope> value	openid mc_authn
Level of assurance	MC Authenticate: LoA2; MC Authenticate Plus: LoA3
Applicable Authenticators	MC Authenticate: Smartphone app, SIM applet, USSD, SMS+URL, Seamless[2] MC Authenticate Plus: Smartphone app (PIN, biometrics), SIM applet (PIN)
API	MC OIDC Device-Initiated Profile; MC OIDC Server-Initiated Profile[3]
Input parameters	<scope>= openid mc_authn; required LoA (acr=2 or acr=3); [Optional] MSISDN or PCR[4] of the target user to be authenticated
Service response	Authentication result + PCR
Supported platforms	PHP, JAVA, .NET

Example user flow



Seamless user experience on mobile network with authentication occurring in the background



Authentication user experience on Wi-Fi with SIM Applet authenticator (Click to authenticate)

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.**

2. Seamless authentication option only available where Device-Initiated Profile is used and the user is connected over the mobile network
3. Server-Initiated mode can be used where the user is not interacting via an IP-connected device
4. Pseudonymous Customer Reference (subject identifier issued by Mobile Connect per user:SP pairing)