mobile connect

Mobile Connect Link
Delivered by the GSMA

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

Mobile Connect Authorise

Simple and secure user authorisation of online transactions.

Product Summary

Enables a Service Provider (SP) to authenticate a user and request them to authorise an action or transaction[1]. 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 Authorise:** 1-factor of authentication (LoA2) = possession & control of the mobile device associated with the target MSISDN; simple Click OK to authorise the SP request
- **MC Authorise Plus:** 2 factors of authentication (LoA3) = possession & control of the mobile device + either a PIN or biometric (based on authenticator capability) used to authenticate and authorise the SP request

How it works

- SP issues a request for user authorisation (stipulating the required LoA and descriptive text of what the user is being asked to authorise) via the Mobile Connect OIDC API to the user's Operator[2]
- The Operator processes the request and uses an appropriate authenticator (based on the requested LoA) to authenticate the user via their mobile device, present the SP's request (descriptive text) and obtain the user's response (approve or deny)
- The Operator provides the user's 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 the user)

HOW IT WORKS

Example use cases

- Step-up authorisation for high value/sensitive transactions (e.g., online banking)
- Payment authorisation
- Parental consent for an action requested by their child via an online service
- Approval of expense claims/budget etc.
- Secure verification for forgotten password and account recovery

Product features/benefits

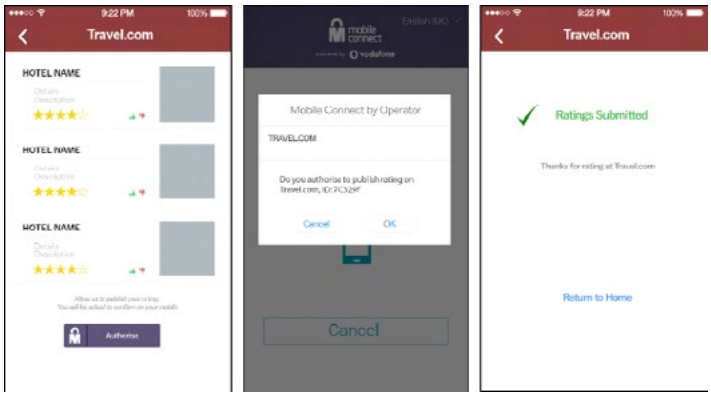
- Simple mechanism for capturing user's permission/ authorisation via the user's mobile device
- Common authorisation experience irrespective of the channel through which the user is interacting with the SP service (e.g., tablet, PC. mobile, Smart TV etc.)
- Underpinned by the security of the mobile 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
- Supports different levels of assurance to enable SPs to trade-off security vs user convenience based on intended use case
- 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 Authorise Plus can be combined with the MC ATP service (where supported) to enable eCommerce Guest Checkout; i.e., payment authorisation and provision of shipping details

1. Note that it is important that the user is authenticated first to ensure the right person is authorising the transaction hence this aspect is included within the user flow
2. The SDK includes a Discovery service to determine the correct Operator for a given user

Product Specifications

OIDC <scope> value	openid mc_authz
Level of assurance	MC Authorise: LoA2; MC Authorise Plus: LoA3
Applicable Authenticators	MC Authorise: Smartphone app, SIM applet, USSD MC Authorise 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_authz; required LoA (acr=2 or acr=3); descriptive text of what the user is being asked to authorise; [Optional] MSISDN or PCR[4] of the target user
Service response	Authorisation result + PCR
Supported platforms	PHP, JAVA, .NET

Example user flow



Mobile Connect Authorise SIM Applet authenticator experience

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.**

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)