Mobile ID OpenID Connect

Secure and robust authentication service – fully integrated in the user process

Because of new licensing and deployment models (SaaS), there are deployed systems with different requirements for IAM and MFA solutions. Mobile ID OpenID Connect (OIDC) enables a wide range of usage scenarios in conjunction with federated systems. It allows the easy use and deployment of Mobile ID when the technical terminals are specified in your Identity Provider (IdP).

Swisscom ensures all users can rely on a strong authentication service, regardless of their initial situation. If Mobile ID isn't already installed and activated on the device, the user is guided through the process on how to activate it. Your users always see a closed authentication. Various additional data, such as the user's location, can be entered as an optional service.

There is only one prerequisite for using Mobile ID OIDC: the user must have a mobile phone and be able to receive messages by SMS. Mobile ID works all over the world. To pinpoint their location, the user must have a Swisscom SIM or install the Mobile ID app.

Your advantages with Mobile ID OIDC

Easy integration

Easy configuration of pre-specified terminals with IdP. ✓

User guidance from Swisscom

Complete web-based processes for your users. ✓

Perfect for hybrid environments

Coexistence with other Mobile ID integrations. ✓

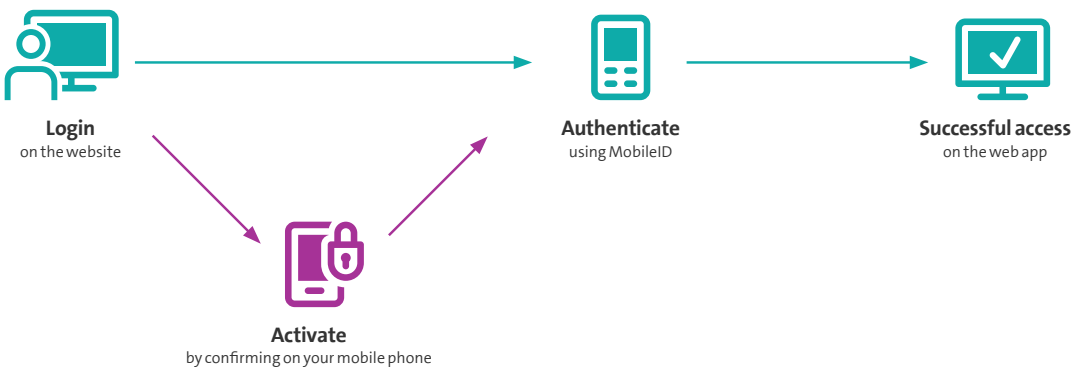
Compatible with cloud

For example for Microsoft Azure MFA, Microsoft Active Directory or AWS. ✓

Optional additional services

Individual and customer-based upgrades possible. ✓

This is how Mobile ID OpenID Connect works



swisscom

Mobile ID OpenID Connect at a glance

What does the Basic package include?
A brief description of the Basic Services for Swisscom Mobile ID OpenID Connect.

Basic Services

- **Use as a second factor:** Authenticator as a simple add-on to existing authentication for all owners of a mobile device.
- **Mobile ID to verify ID:** Robust SIM and/or app-based authentication based on "possession, knowledge & inherence". Available in Switzerland, the EU and other countries.
- **Mobile ID Open ID Connect interface:** Easy support of web-based apps in federated systems (IdP) by referencing the Mobile ID OIDC service terminal.
- **Ensure a defined level of protection:** The Mobile ID deployment, activation and replacement processes resolve the problems typically faced with Tokens, and ensure the user ID is verified through "Knowledge & Possession".
- **Unique, unchangeable pseudonym:** The "sub" always ensures that it is the same, previously registered user.
- **Standardised OIDC authentication:** Get access to the OpenID Connect Provider (OP) provided by Swisscom with the scopes "openid" and "profile".
- **Mobile ID & Microsoft Azure AD:** Configurations provided by Microsoft for using Mobile ID with Azure AD B2C.

We offer you the following additional services:
The Swisscom Mobile ID OIDC add-ons for your needs.

Optional Services

- **More information:** Get even more security and information with the scopes "phone", "mid_profile", "mid_cms" or "mid_location".
- **Pseudonym as a persistent name identifier:** To recognise the same person across multiple applications and application instances.
- **Robust authentication:** Based on the possession of a specific hardware and an additional corresponding security element (AL3).
- **Personal user identification:** Robust authentication and ensure possession of a certificate (AL4).
- **Individual text:** Customer freely supplements the authentication text.
- **Mobile ID Zero Trust:** All confirmations are based on strong cryptography. These can be checked by the customer and assigned to the respective owner of the Mobile ID without the possibility of them being edited.
- **Continuous authentication:** Current user data can be repeatedly compared.
- **Combined use and billing:** Through the Mobile ID contract (REST API) already in place.

Additional services: Customer-specific layouts can be used during the authentication process. The processes and content of the authentication are adapted to suit the specific needs of the customer. Currently used Tokens such as an authenticator or RSA, are migrated using the standardised procedure. Our Consulting Services offer specialised advice on IAM, Security and Business Continuity.

Swisscom (Switzerland) Ltd Business Customers, P.O. Box,
CH-3050 Berne, Telephone 0800 800 900, www.swisscom.ch/enterprise