



SuisseID Mobile Service

Makes your application login mobile

SuisseID can provide you with support for identity management and also for authentication device management. With the SuisseID Mobile Service the authentication part has now also been given the addition of a mobile component.

What is the SuisseID Mobile Service?

With the SuisseID Mobile Service the possible uses of SuisseID are being expanded. Your customers can also use the SuisseID login via mobile devices such as smartphones and tablets / iPads without SuisseID having to be connected to the device.

The SuisseID Mobile Service is based on a valid SuisseID and works on every portal / in every application which is connected to the IdP server (Identity Provider Service) of the SuisseID. The service can be activated by customers at www.post.ch/suisseid.

Advantages for your customers

- No large keychain, instead just one key (master key)
- With the Mobile Service, SuisseID can also be used on tablets and other mobile devices.
- Easy to use because based on what users already know (SMS code).

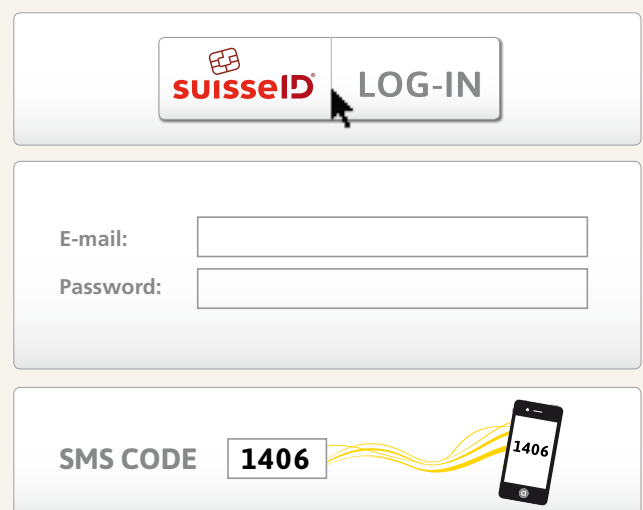
Advantages for you as a service provider

- The needs of your customers are covered (mobility, usability, data protection, security)
- Use of double authentication (e-mail / password, SMS code)
- People are identified unequivocally thanks to the tested and standardised processes
- Benefit from the innovative improvements of SuisseID
- You as a service provider can concentrate on your core competences

How the login process works (End User View)

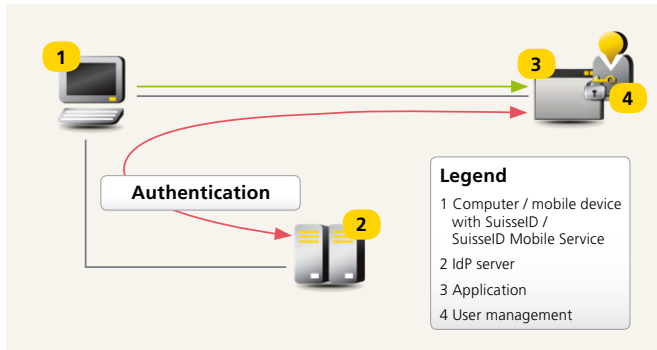
The customer login is based on the known mechanisms and is done via a simple and secure process for the customers.

1. You log in at a portal using your mobile device – as usual with the SuisseID login button.
2. You are asked to enter the e-mail address and password of your SuisseID Mobile Service.
3. Your details are checked and for login you receive an SMS code to be entered. Now you are logged in.

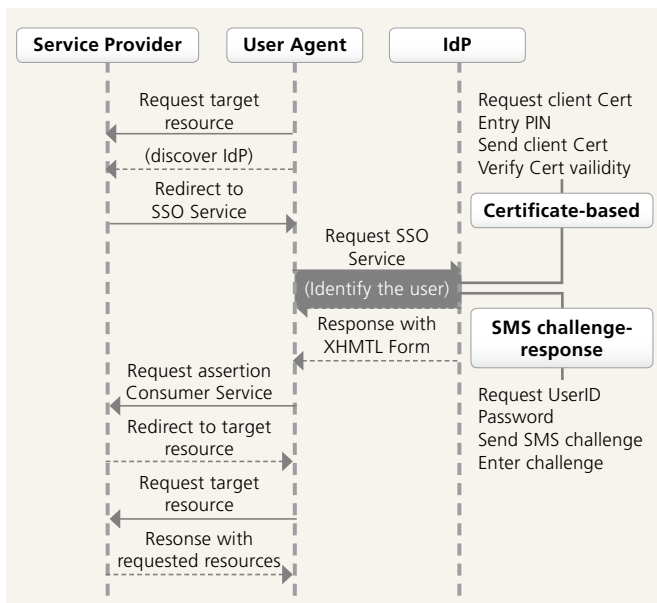


Setup

Unlike certificate-based authentication, in a solution with the SuisseID Mobile Service the IdP service (Identity Provider Service) is used in addition. Here the IdP does the actual authentication work. This can be a two-sided certificate-based or also an SMS challenge-response procedure. If the user does not have a smart card available, the IdP immediately switches to challenge-response mode.



In the diagram below the rough technical procedure can be seen.



How to start

The SuisseID Mobile Service covers many of the requirements of your customers. This means you provide your customers with an innovative solution without having to worry about this. With the authentication check by the identity service provider of the SuisseID and the corresponding SuisseID Mobile Service you are relying on a solution from a strong partner.

As a service provider with integration in our IdP server you have all the requirements for activating the SuisseID Mobile Service.

Register as a service provider on our [website](#).

Security

We want to demonstrate the security of these solutions using the following model:

Cryptography

- SMS challenge (one-time password) must not be guessed. This is done by using the state-of-the-art algorithm HOTP, an HMAC-based one-time password algorithm. HOTP was published as an informational IETF RFC 4226 and is a result of the Initiative for Open Authentication (OATH).

Secure infrastructure / used protocols

- Our IT infrastructure is operated in a secure physical environment (computer centre) which corresponds with the Swiss Financial Market Supervisory Authority's (FINMA) requirements and has the corresponding certifications.
- Our IT infrastructure is regularly checked for weak points by external experts.
- We focus on the international standards.

Organisation / processes

- Our organisation and processes have been approved according to the Swiss Electronic Signature Act ZertES and certified according to ISO 27001, ETSI TS 101 456, among others.
- SuisseID owners and also the application providers can decide individually if they want to use the mobile service or not.
- If there is corresponding danger, we allow ourselves to deactivate the authentication procedure.

Policy / law

- We are obliged to observe the strict security requirements according to ZertES and data protection.
- We focus on international standards so that investment protection is also guaranteed for our customers / partners (for example IdP follows the international standard SAML 2.0).

User-friendliness

- We are convinced that high security and good usability can be combined. This is why we try to make user guidance as simple as possible, and of course while always adhering to the high security requirements.

Swiss Post Solutions Ltd.

ePost Product House
Sägereistrasse 25
8152 Glattbrugg

+41 (0) 44 838 36 00
suisseid@post.ch
www.post.ch/suisseid

