Mobile ID
OpenID Connect

Integration guide

Version: 1.0

Swisscom (Schweiz) AG
Business Development & Security

Contents

1 Introduction

The Swisscom Mobile ID (MID) provides a generic SOAP interface that can be addressed natively or over a protocol translation. This document provides information and possible solutions on how to integrate OpenID Connect (OIDC) enabled services with the MID service.

The solution presented in this document suggests adding at the customer side an OpenID (Connect) Provider server. This document does not yet include the detailed steps in order to achieve this kind of server setup and relies on 3rd party solutions. This manual assumes that you are familiar with the Swisscom MID service and the related "Mobile ID - SOAP client reference guide" [1].

1.1 Terms and abbreviations

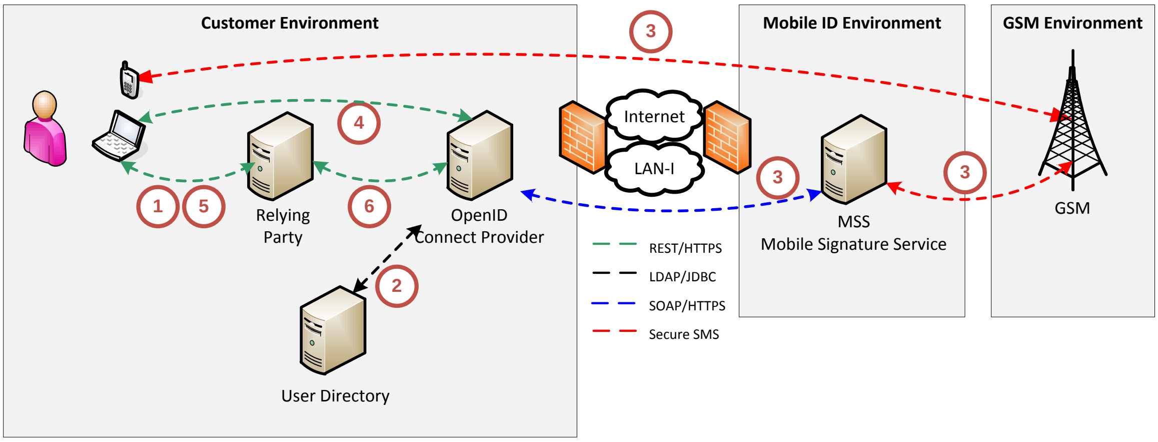
Abbreviation	Definition
AP	Application Provider
DTBS	Data to be signed. A UTF8 encoded text string that is signed by the SIM card and also displayed to the user on the mobile phone screen.
M-ID or MID	Mobile ID platform providing the mobile signature service
MSISDN	Number uniquely identifying a subscription in a GSM/UMTS mobile network
OIDC	OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.
OP	OpenID (Connect) Provider is the authorization server of the OpenID Connect design
RP	Relying Party of the OpenID Connect design is a for example a Web application. It is seen as an AP/SP from Mobile ID point of view.
SOAP	Simple Object Access Protocol (SOAP) is a protocol specification for exchanging structured information in the implementation of Web Services relying on Extensible Markup Language (XML)
SP	Service provider

1.2 Referenced documents

[1] Mobile ID - SOAP client reference guide.pdf
https://www.swisscom.ch/en/business/mobile-id/technical-details/technical-documents.html

2 Overview of OpenID Connect to Mobile ID SOAP

Before entering into more technical details, let's have a short look at the overview:



This shows OIDC enabled services (Relying Party or RP) sending their OIDC request to an OpenID (Connect) Provider server (OP) acting as OIDC/SOAP relay. The OP server will invoke the Swisscom MID service over SOAP and provide the answer back to the RP with OIDC. The OP may also be connected to an external User Directory, where additional end users details like phone number or credentials could be stored & retrieved. Here the dataflow:

1. A user accesses a Relying Party (RP, e.g. web application) with a User Agent (e.g. browser). The RP redirects the user to the OpenID (Connect) Provider (OP) via the User Agent for authentication.
2. The user authenticates (e.g. with credentials) at the OP. The OP verifies the user credentials (e.g. against internal user store) and maps the related phone number to the user.
3. The OP calls the Swisscom Mobile ID to authenticate the user via Mobile ID.
4. The OP requests a permission from the user to share his authentication/user information with the RP.
5. The user is redirected back to the RP via the User Agent and the RP identifies the user based on the authentication information.
6. The RP can request additional user information from the OP.

3 SOAP/OIDC relay capabilities for MID service use

3.1 Extensible in order to place SOAP requests to the MID service

The MID service does not support the OpenID Connect natively and only provides a SOAP Web Service Interface. Nevertheless, some OpenID (Connect) Provider servers have extension capabilities or flexible modules that can be adapted in order to integrate the MID service.

3.2 Translation of user credentials into mobile number

The OpenID (Connect) Provider server must provide an option to convert the user credentials into a valid mobile number (MSISDN). Common ways to store such mappings are local files, LDAP / Active Directory and SQL databases.

3.3 Define the Data to be Signed (DTBS)

The OpenID (Connect) Provider server has to define the DTBS message that will be displayed on the end users mobile. This can either be a generic/global service message like “server.com: Login?” or a specific, user translated, message for each OIDC client.

3.4 Set the user language

The language of the DTBS message must be defined in the SOAP request. The OpenID (Connect) Provider server can use one global language or generate request specific communication. In this case the DTBS and user language should be consistent to avoid a language mix at the end user device.

4 List of products that could act as SOAP/OIDC gateway

Among others the Product PingFederate of PingID support the Mobile ID extension. For more details, please refer to IC-Consult . Alternative solutions may be considered as well.

Here we list some products that could act as SOAP/OIDC relay:

- PingFederate made by PingID - https://www.pingidentity.com/products/pingfederate/
  & IC-Consult, their Swiss Partner: http://www.ic-consult.com
- Nevis made by AdNovum - http://www.adnovum.ch/en/solutions/nevis.html
- OpenAM made by Forgerock - http://forgerock.com/products/open-identity-stack/openam/
- OpenID-Connect-Java-Spring-Server - https://github.com/mitreid-connect/OpenID-Connect-Java-Spring-Server