Mobile ID
PingFederate - Ping Identity

Solution guide

Version: 1.0

Swisscom (Schweiz) AG
Security Solutions

Swisscom (Schweiz) AG
Security Solutions

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 like the one of Ping Identity: PingFederate. 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 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] PingFederate https://www.pingidentity.com/products/pingfederate/

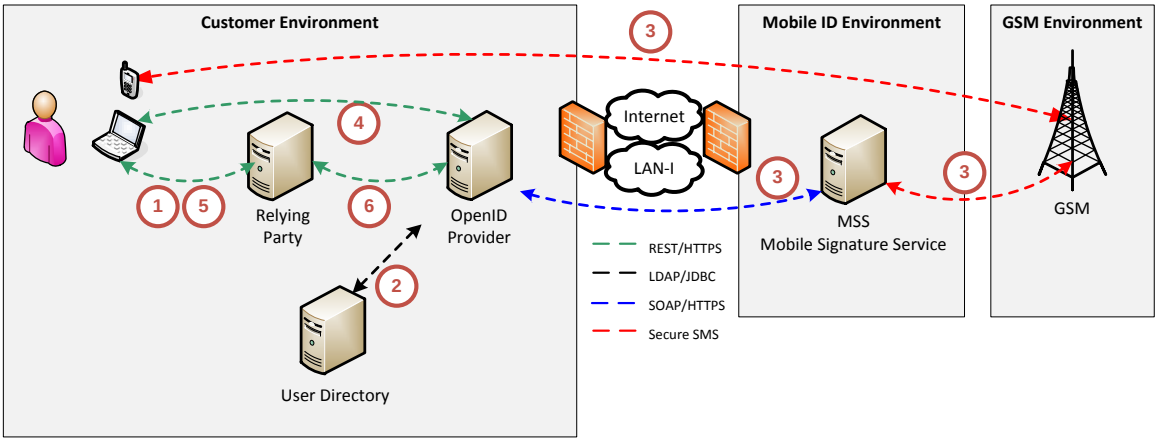
2 Overview and main Scenario

This chapter describes a possible solution to interface a PingFederate with Mobile ID.

PingFederate provides an extensible interface that allows the development of a Mobile ID SOAP plug-in.

Scenario - Strong Authentication with PingFederate:

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 Provider (OP) server acting as OIDC/SOAP relay (here PingFederate). The OP server will invoke the Swisscom MID service over SOAP and provide the answer back to the clients with OIDC. The OP server may also be connected to an external User Directory, where additional end users details like phone number or credentials could be 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 Provider (OP – PingFederate) 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 Mobile ID add-on for PingFederate

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

The MID service only provides a SOAP Web Service Interface. Nevertheless, PingFederate has extension capabilities that can be adapted in order to integrate the MID service.

IC-Consult, the Ping Identity Swiss partner, developed a plug-in for PingFederate to relay the SOAP request towards Mobile ID. For additional details, please contact IC-Consult: http://www.ic-consult.com

3.2 Best Practices

Even if this document doesn't cover the details of the configuration of PingFederate, here some important elements related to the Mobile ID options:

- User credentials - PingFederate provides an option to convert user credentials into a valid mobile number (MSISDN). Common ways to store such mappings are local files, LDAP / Active Directory and SQL databases.
- Data to be Signed (DTBS) – Ping Federate 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 client.
- User language - The language of the DTBS message must be defined in the SOAP request. PingFederate 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.