Mobile ID
SAML and SuisseID

Integration guide

Version: 1.1

Swisscom (Schweiz) AG
IAM & Security

Contents

1 Introduction

The Swisscom Mobile ID (MID) provides a generic SOAP interface that can be addressed natively or indirect over a protocol translation. This document provides information and possible solutions on how to integrate SAML enabled services with Mobile ID. As SuisseID is using SAML as underlying technology, this integration guide applies to SuisseID enabled services, too.

The solution presented in this document suggests adding at the customer side a SAML/SOAP gateway server. This document also includes the detailed steps in order to achieve this kind of server setup. This manual assumes that you are familiar with the Swisscom MID service and the related “Mobile ID - SOAP client reference guide”.

The proposed solutions are under the sole responsibility of the customer installing and using them. There will be no support provided for this.

1.1 Terms and abbreviations

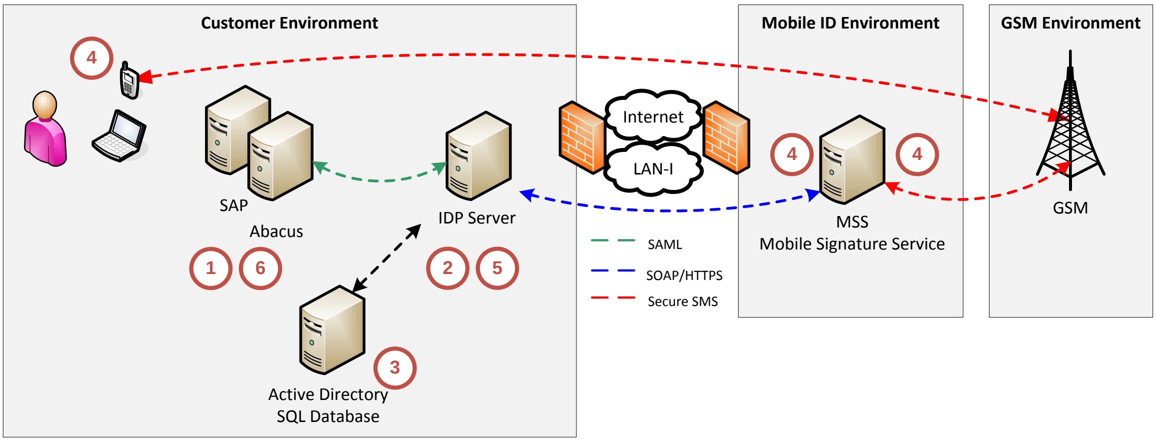
Abbreviation	Definition
AP	Application Provider
Assertion	Packet of security information delivered by the IDP and consumed by the SP
DTBD	Data to be displayed
DTBS	Data to be signed
IDP	Identity provider
M-ID or MID	Mobile ID platform providing the mobile signature service
MSISDN	Number uniquely identifying a subscription in a GSM/UMTS mobile network
SAML	Security Assertion Markup Language (SAML) is an XML-based open standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee.
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
WS	A Web service (WS) is a method of communication between two electronic devices over the Web (Internet). The W3C defines a "Web service" as "a software system designed to support interoperable machine-to-machine interaction over a network". It has an interface described in a machine processable format (specifically Web Services Description Language, known by the acronym WSDL).

1.2 Referenced documents

[1] Mobile ID - SOAP client reference guide.pdf

2 Overview of SAML to Mobile ID SOAP

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



This shows several SAML enabled services like SAP and Abacus sending their SAML request to a IDP server acting as SAML/SOAP gateway. The IDP server will invoke the Swisscom MID service over SOAP and provide the answer back to the clients with SAML. The IDP server may also be connected to an external user store, like Microsoft Active Directory, where additional end users details like phone number or credentials could be retrieved. Here the dataflow:

1. The SAML enabled service makes a request to the IDP server
2. The MID enabled IDP server calls the MID service over SOAP
3. The IDP server, optionally, verifies the user credentials against internal user stores and/or maps to a valid mobile phone user
4. The MID platform ensures that the end-user signature request is allowed and forwards the signature request to the end-user's mobile phone
5. The end-user answer will be processed by the MID platform and provided to the IDP server
6. After verification of MID response by the IDP server, the SAML request will be answered

3 SOAP/SAML gateway 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 SAML protocol natively and only provides a SOAP Web Service Interface. Nevertheless, most of the IDP servers provide support for SAML and 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 IDP server must provide 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.

3.3 Define the Data to be Signed (DTBS)

The IDP 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 SAML client.

3.4 Set the user language

Beside the DTBS the SOAP request requires also the user language. This language is relevant for resource push from the MID service platform to the mobile user. The SAML 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 Example: How to integrate Mobile ID into simpleSAMLphp server

This chapter presents the integration of the MID service into a widely adopted and deployed open source SAML server: simpleSAMLphp[1]. The explanation is related to the MID service call itself and is not a complete guide/solution for simpleSAMLphp deployment itself. It assumes knowledge of SAML and the related SAML client solutions as well as of the simpleSAMLphp server itself.

The callout to the MID service is done over a simpleSAMLphp module[2] that invokes the MID SOAP protocol.

Preconditions:

- Installed and running server that supports simpleSAMLphp
- Functional and tested MID Web Service interface

4.1 Install simpleSAMLphp

Refer to the simpleSAMLphp installation documentation for proper setup.

<simplesamlphp> in this guide refers to the base URL of your IDP server e.g https://myidp.com
The Single Sign-On endpoint of simplesamlphp is normally *<simplesamlphp>*/saml2/idp/SSOService.php

4.2 Generic configuration steps

4.2.1 Install and enable the Mobile ID module

Refer to https://github.com/SCS-CBU-CED-IAM/simplesaml-mobileid#install

4.2.2 Configure and test the authentication source

Refer to https://github.com/SCS-CBU-CED-IAM/simplesaml-mobileid#configuration

Once configured you can test the authentication source like the other modules. All information and errors will be logged over the logging facility of simplesamlphp.

4.2.3 Service Provider configurations

The Mobile ID module provides a list of attributes that can be defined as SAML ***nameidattribute*** and optionally provided as SAML attributes to the Service Providers:

`uid`	the userid attribute defined at the login window
`mobile`	the Mobile ID validated mobile number in international format with 00 as prefix e.g. 0041792742619 for +41 (0) 79 274 26 10
`preferredLanguage`	the language used during the validation process e.g FR, EN, IT, DE
`userCertificate`	the Mobile ID user certificate (PEM encoded)
`serialNumber`	the serialNumber contained in the Distinguished Name (DN) of the Mobile ID user certificate. Refer to the “User Mapping” chapter of the Mobile ID SOAP Guide
`pseudonym`	the mobile attribute in the Swisscom SuisseID format with 1100-7 as prefix. This attribute is only set when the mobile number is from a whitelisted country: Switzerland 1100-741x-xxxx-xxxx: 1100-7417-9274-2610 for +41 (0) 79 274 26 10 Lichtenstein 1100-7423-0xxx-xxxx: 1100-7423-0399-4444 for +423 399 44 44

[1] http://simplesamlphp.org
[2] http://simplesamlphp.org/docs/stable/simplesamlphp-modules

Example of a SP remote configuration[3] with serialNumber as NamedIDAttribute:

```
$metadata['https://mysp.com'] = array(
  'Description' => 'SP Demo Example',
  'AssertionConsumerService' => 'https://mysp.com/module.php/saml/sp/saml2-acs.php/my-
sp',
  'SingleLogoutService' => 'https://mysp.com/module.php/saml/sp/saml2-logout.php/my-sp',
  'certData' => 'MIICyjCCIwNzE0MzcxOIhv...1hpybT2DKP9/oAtxCcW0rnqesKdu0MHm69hXfw==',
  'ForceAuthn' => TRUE,
  'simplesaml.nameidattribute' => 'serialNumber',
  'simplesaml.attributes' => TRUE,
);
```

[3] SP remote documentation http://simplesamlphp.org/docs/stable/simplesamlphp-reference-sp-remote

4.3 Advanced integration options

In this section you will find several advanced integration options that can be covered with the simpleSAMLphp server.

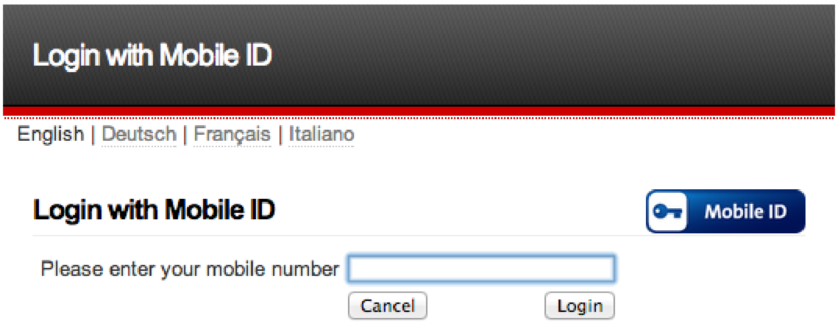
4.3.1 Login with mobile number (MSISDN) defined by the user

The simplest configuration is to have any SAML client redirecting to the simpleSAMLphp server and let him do the MID service call. At the end the SAML client will get a SAML assertion with the related information in order to proceed to the consumption.

This assumes that:

- the SAML client will redirect to the IDP server for authentication
- the IDP server will authorize/deny users solely based on MID service decision
- the MSISDN will be entered at the IDP server side by the end-user or provided by the SAML client in his request
- the DTBS message is defined by the IDP server
- the User Language is set by the IDP server

This configuration is the default one and here a screenshot of the Login screen at the simpleSAMLphp server:



Login with Mobile ID

English | Deutsch | Français | Italiano

Login with Mobile ID

Please enter your mobile number

4.3.2 Returning additional attributes to the Service Provider

In SimpleSAMLphp, there is an API[4] where you can configure the IDP server for additional processing after authentication is complete, and just before you are sent back to the SP. It is possible to use this for additional authentication checks like delivering attributes to the user, modifying the users attributes, and other things which should be performed before returning the user to the SP he came from.

Examples of potentially valuable features using Authentication Processing Filters:

- Adding eMail attribute in a format like mobilenumber@example.net

```
'authproc' => array(
    10 => array(
        'class' => 'core:PHP',
        'code' => '
            $id = $attributes["mobile"][0];
            $mail = $id . "@example.net";
            $attributes["mail"] = array($mail);
            ',
```

- Checking the mobile number in corporate Active Directory to get eMail and/or User ID
- Checking the mobile number in an SQL Database to get eMail address

[4] http://simplesamlphp.org/docs/stable/simplesamlphp-authproc

4.3.3 Acting as a SuisseID IDP for a service using the SuisseID SDK

If the SuisseID SDK is used at the Service Provider the simpleSAMLphp server can be used as an IDP and return the SuisseID number after a successful Mobile ID login.

SuisseID Number out of Mobile ID mobile number:

The SuisseID number is a novel concept to identify SuisseID owners[5]. This number is provided in the following format: cspId{4}- [0-9]{4}- [0-9]{4}- [0-9]{4}. Example for a Swisscom SuisseID: 1100-4567-8901-2345.

The Swisscom SuisseID 1100-7 prefix has been exclusively reserved for Mobile ID by Swisscom CSP. Therefore the following format has been implemented for the `pseudonym` attribute in order to be able to do a direct transposition of the mobile number to the SuisseID Number: 1100-7[0-9]{3}-[0-9]{4}-[0-9]{4}. This transposition is only applied for specific whitelisted countries:

Country	SuisseID Template	Example
Switzerland	1100-741x-xxxx-xxxx	1100-7417-9274-2610 for +41 (0) 79 274 26 10
Lichtenstein	1100-7423-0xxx-xxxx	1100-7423-0399-4444 for +423 399 44 44

SuisseID SDK[6]:

The authentication assertion can be consumed without any code change at the SP side. Just add a configuration on the SDK that defines the simpleSAMLphp IDP server. For the combined assertion the use of the guidance in chapter 4.3.2 may be required depending on the required attributes by the SP itself. The attribute query request and the QC signed attributes are not supported.

SuisseID Java SDK:

Adjust the `suisseid.properties` configuration file with following entries:

sp.name	Internal SDK Name of the Service Provider
sp.issuer	SAML Issuer Name of the Service Provider
sp.destination.swisscom	IDP SSO endpoint
sp.url	SAML ConsumerServiceURL of the Service Provider SDK
sp.privacy_notice	URL with the Service Provider privacy notice

or set following attributes directly at the call of BuilderFactory.Init:

Service Provider	URL of the Service Provider
SP ConsumerURL	URL where the IDP assertion must be posted
IDP Endpoint	IDP SSO endpoint
SP Entity	Service Provider Issuer Name
SP Privacy Notice	URL with the Service Provider privacy notice
SP Sign Public	Optional certificate (public key) to sign the SAML requests
SP Sign Private	Optional certificate (private key) to sign the SAML requests

SuisseID .NET SDK:

Adjust the SDK configuration file as described in the documentation and at the call of SuisseIdSdkObjectFactory.GetAuthenticationRequest() set following attributes:

request.Issuer	Service Provider Issuer Name
request.AssertionConsumerServiceUrl	URL where the IDP assertion must be posted
request.PrivacyNoticeAddress	URL with the Service Provider privacy notice

[5] http://www.suisseid.ch

[6] http://develop.suisseid.ch

4.3.4 Integrating Mobile ID into other authentication sources

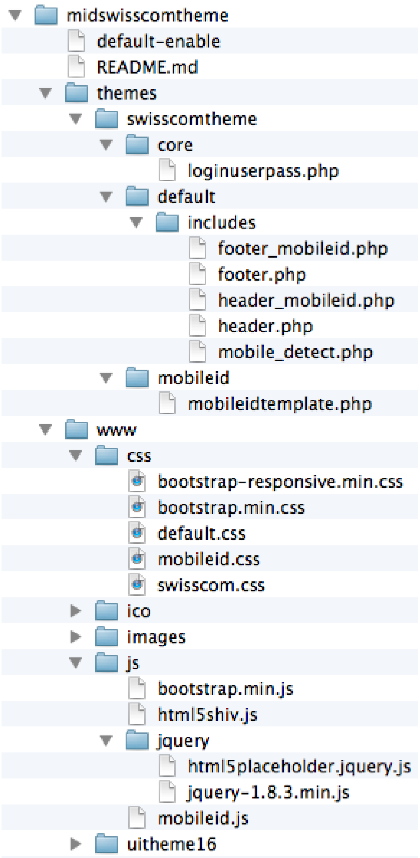
An alternative way to the direct Mobile ID login is to use another authentication source and to call the Mobile ID afterwards.

For this kind of setup you can setup an Active Directory/LDAP authentication[7] or an SQL database[8] based one and use the Authentication Processing Filter[9] for the related Mobile ID call.

4.3.5 Theming simpleSAMLphp and the Mobile ID module

The module follows the 'Theming the user interface in SimpleSAMLphp'[10] rules and it can be overridden by copying and adjusting the `mobileidtemplate.php` in your own theming module.

Sample structure `'theme.use' => 'swisscomtheme:swisscomtheme'` in `config/config.php`



```
▼ midswisscomtheme
    default-enable
    README.md
  ▼ themes
    ▼ swisscomtheme
      ▼ core
          loginuserpass.php
      ▼ default
        ▼ includes
            footer_mobileid.php
            footer.php
            header_mobileid.php
            header.php
            mobile_detect.php
      ▼ mobileid
          mobileidtemplate.php
  ▼ www
    ▼ css
        bootstrap-responsive.min.css
        bootstrap.min.css
        default.css
        mobileid.css
        swisscom.css
    ▶ ico
    ▶ images
    ▼ js
        bootstrap.min.js
        html5shiv.js
      ▼ jquery
          html5placeholder.jquery.js
          jquery-1.8.3.min.js
        mobileid.js
    ▶ uitheme16
```

[7] http://simplesamlphp.org/docs/stable/ldap:ldap
[8] http://simplesamlphp.org/docs/stable/sqlauth:sql
[9] http://simplesamlphp.org/docs/stable/simplesamlphp-authproc
[10] http://simplesamlphp.org/docs/stable/simplesamlphp-theming

5 Sample solutions where Mobile ID can be integrated over SAML

5.1 Google Apps

Google Apps provides a standard SAML authentication module that can be configured[11] in order to identify the users over an external IDP server.

<simplesamlphp> refers to the IDP server base URL e.g myidpserver.com
<hosteddomain.com> refers to the Google Apps hosted domain e.g mydomain.com

- Configuration at Google under Security / Advanced - SSO

Sign-in page URL:	https://*<simplesamlphp>*/saml2/idp/SSOService.php
Sign-out page URL:	https://*<simplesamlphp>*/saml2/idp/initSLO.php?RelayState=https://google.com
Change password URL:	https://www.google.com/a/*<hosteddomain.com>*
Verification certificate:	Upload the public certificate signing the assertions of your simpleSAMLphp server
Domain specific issuer:	Checked

- Configuration elements at simpleSAMLphp

```
$metadata['google.com/a/<hosteddomain.com>'] = array(
  'AssertionConsumerService' => 'https://www.google.com/a/<hosteddomain.com>/acs',
  'NameIDFormat' => 'urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified',
  'simplesaml.nameidattribute' => 'serialNumber',
```

5.2 Dropbox

Dropbox for Business service now offers single sign-on (SSO) via the standard. Any off-the-shelf or homegrown identity management system that's compatible with SAML can be configured to automatically sign users into Dropbox.

<simplesamlphp> refers to the IDP server base URL e.g myidpserver.com

- Configuration at Dropbox[12] under the Authentication menu item of the Admin Console

Sign in URL:	https://<simplesamlphp>/saml2/idp/SSOService.php
X.509 Certificate:	Upload the public certificate signing the assertions of your simpleSAMLphp server

- Configuration elements at simpleSAMLphp

```
$metadata['Dropbox'] = array(
  'AssertionConsumerService' => 'https://www.dropbox.com/saml_login',
  'NameIDFormat' => 'urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified',
  'simplesaml.nameidattribute' => 'mobile',
```

Currently Dropbox does not support Single Log-Out.

5.3 SAP

Information about SAML support in SAP - http://wiki.scn.sap.com/wiki/display/Security/Single+Sign-On+with+SAML+2.0

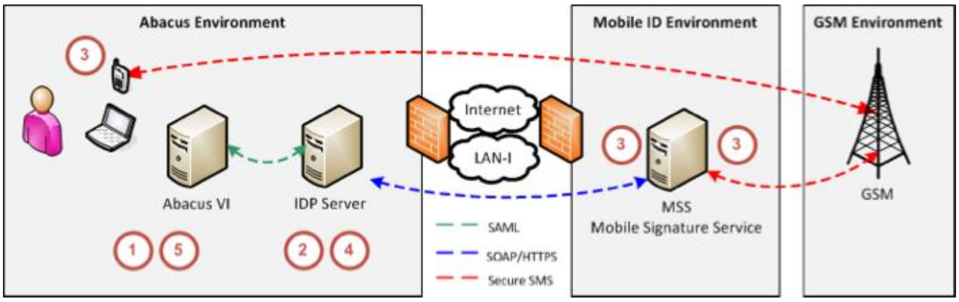
5.4 Office 365 and Windows Azure

Single sign-on, also called identity federation, allows you and your users to access Microsoft cloud services with your Active Directory corporate credentials. Without single sign-on, you, the administrator, and your users will need to maintain separate user names and passwords for your online and on-premises accounts. Single sign-on requires both a security token service (STS) infrastructure and Active Directory synchronization. Information can be found http://technet.microsoft.com/en-us/library/hh967628.aspx

[11] https://developers.google.com/google-apps/sso/saml_reference_implementation
[12] https://www.dropbox.com/help/1909/en

5.5 Abacus VI

Abacus VI since Version 2012 integrates the SuisseID authentication over SAML. The simpleSAMLphp configuration can be adjusted to be compliant to the SAML specification (See 4.3.3) and provide Mobile ID integration.



<simplesamlphp> refers to the IDP server base URL e.g myidpserver.com
<abacusSPidentifer> refers to the Abacus VI defined SP name
<abacusserverConsumerURL> refers to the Abacus IV URL where the answer should be posted

- Configuration at Abacus VI

  Contact Abacus Support for proper setup.

- Configuration elements at simpleSAMLphp

```
$metadata['<abacusSPidentifier>'] = array(
  'AssertionConsumerService' => '<abacusserverConsumerServiceURL>',
  'NameIDFormat' => 'urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified',
  'simplesaml.nameidattribute' => 'serialNumber',
);
```