Mobile ID
SalesForce.com

Solution guide

Version: 1.0

Swisscom (Schweiz) AG
Business Development & Security

Swisscom (Schweiz) AG
Business Development & Security

Contents

Swisscom (Schweiz) AG
Business Development & Security

1 Introduction

The purpose of this document is to provide clarifications **how** to interface Mobile ID with SalesForce.com to authenticate a user with Mobile while using the services of SalesForce.com.

This manual assumes that you are familiar with SalesForce.com and Swisscom Mobile ID.

More details about Mobile ID can be found in the Mobile ID SOAP client reference guide [1].

Terms and abbreviations

Abbreviation	Definition
	Please note:
	Be careful, important:
AP	Application Provider
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
SF	SalesForce.com
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)
WS	A Web service (WS) is a method of communication between two electronic devices over the Web (Internet).

1.1 Referenced documents

[1] SOAP Client Reference Guide
[2] SAML and SuisseID Integration Guide
[3] SalesForce.com Security Implementation Guide
http://help.salesforce.com/help/pdfs/en/salesforce_security_impl_guide.pdf
[4] Configuring SAML Settings for Single Sign-On
http://help.salesforce.com/apex/HTViewHelpDoc?id=sso_saml.htm
[5] Salesforce SSO with simpleSaml PHP
http://salesforce-developer.net/salesforce-sso-with-simplesamlphp/

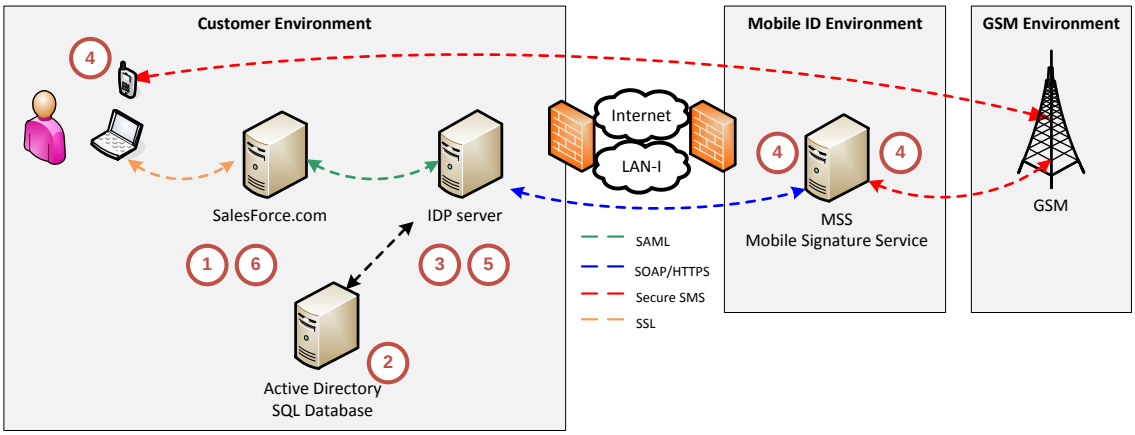
2 Overview and main scenario

This chapter describes a possible solution to interface a SalesForce.com services with Mobile ID.

The solution detailed in this guide is based on the available SAML interface at SalesForce.com side. This interface communicates with a SAML server, in our case an "on premise" IDP server. This can be done with any SAML server that is extensible and would allow the integration of the Mobile ID. We documented such a Mobile ID integrated server based on the open source SAML server simpleSAMLphp see [2].

Scenario - Strong Authentication with SalesForce.com:

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



This picture shows a user who request access to SalesForce.com (SF). SF then sends the SAML requests to the IDP server (here the simpleSAMLphp server) to authenticate the user. The IDP server will invoke the Swisscom Mobile ID service over SOAP and provide the answer back to the SAML client interface of the SF. The IDP server may also be connected to an external user store, like Microsoft Active Directory, where the end users details like phone number or credentials are stored.

Here is the authentication dataflow:

1. When a user tries to connect on SF, SF makes a request to the defined IDP server (like simpleSAMLphp) to authenticate the end user with Mobile ID.
2. The IDP server, optionally, verifies the user credentials against internal user stores and/or maps to a valid mobile phone user.
3. The IDP server (which enabled the Mobile ID module) calls the Mobile ID service.
4. The Mobile ID 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 Mobile ID platform and provided to the IDP server.
6. After verification of Mobile ID response by the IDP server, the answer will be forwarded to SF (over its SAML client interface). This answer will be processed by SF to grant or reject the access requests.

3 Configuration and Best Practices

In this reference guide we assume that:

1. The preconditions defined in [1] are met.
2. The customer has built an intermediate protocol gateway like the simpleSAMLphp server described in [2] (with the Mobile ID module).

3.1 Configuration of simpleSAMLphp on SalesForce.com

To allow an SF to perform a Mobile ID authentication, the SF authentication must be configured to reroute the user requests towards the simpleSAMLphp server. The configuration of the SF must be performed as described in [5] and [4].

SF must define a Session-level Security as such:

1. Obtain the Recipient URL value from the configuration page and put it in the corresponding configuration parameter of the IDP server (in our case simpleSAMLphp).
2. Salesforce allows a maximum of three minutes for clock skew with the IDP server. The "Timeout" should be configured to 90sec in order to give enough time to Mobile ID to handle the authentication requests.
3. Since the IDP server can perform the mapping of the MobileID usernames (the MSISDN) and Salesforce usernames, We suggest you to choose to delegate this to the IDP server.

3.2 simpleSAMLphp server and end-users details

The document [2] describes as well how to inter-connect an external user store to the simpleSAMLphp server, like Microsoft Active Directory (where the end users details like phone number or credentials are stored).

3.3 Additional documentation

Refer to [3], [4] and [5] for additional documentation and information regarding this setup.