

Mobile ID

Microsoft SharePoint

Solution guide

Version: 1.1

Copyright

This document, its content and the ideas and concepts used herein are confidential and the property of Swisscom (Schweiz) Ltd. They may not be made accessible to third parties or other persons who are not involved in the project for which this document has been prepared, nor may they be exploited or utilised for execution or implementation, without the company's written consent.



Swisscom (Schweiz) AG
Security Solutions

Contents

1	Introduction.....	3
1.1	Target readership, requirements of the reader.....	3
1.2	Terms and abbreviations.....	3
1.3	Referenced documents.....	4
2	Overview.....	5
3	Architecture und main Scenario.....	6
4	Setup.....	7
4.1	Installation and configuration of AD FS / IDP.....	7
4.2	Configuration of SharePoint.....	7
4.3	Microsoft Technical Guides.....	7
4.3.1	SharePoint 2013: Claims-Based Authentication and Plan for user authentication methods	7
4.3.2	Configure SAML-based claims authentication with AD FS in SharePoint 2013.....	7
4.3.3	Implement SAML-based authentication in SharePoint Server 2013	7
4.3.4	Increase SharePoint Execution Timeout	7
4.3.5	Other useful links.....	7

1 Introduction

Mobile ID (MID) provides strong authentication based cryptographic materials stored and protected in the SIM card in user's mobile phone. Microsoft SharePoint is a web application platform in the Microsoft Office server suite. SharePoint combines various functions, which are traditionally separate applications: intranet, extranet, content management, document management and so on.

This document focuses on installation, configuration, and troubleshooting of the Mobile ID Authentication Provider for SharePoint 2013 Server.

1.1 Target readership, requirements of the reader

The purpose of the Integration Guide is to provide an overview for system administrators, IT Professionals and support technicians who are responsible for designing, implementing and maintaining SharePoint farms. This manual assumes that you are familiar with the Swisscom Mobile ID service [1] and Microsoft SharePoint 2013.

1.2 Terms and abbreviations

Abbreviation	Definition
AD	Active Directory
ADAL	Active Directory Authentication Library https://azure.microsoft.com/en-us/documentation/articles/active-directory-authentication-libraries/
AD FS	Active Directory Federation Services. https://technet.microsoft.com/en-us/windowsserver/dd448613.aspx
AP	Application Provider
CA	Certificate Authority
CRL	Certificate Revocation Lists
IDP	Identity Provider also known as Identity Assertion Provider , is responsible for providing identifiers for users looking to interact with a system, and asserting to such a system that such an identifier presented by a user is known to the provider, and possibly providing other information about the user that is known to the provider.
MID	Mobile ID. http://www.swisscom.com/mid
MFA	Multi-Factor Authentication. Authentication methods that require more than one independent "factors". A factor can be a knowledge factor ("what you know", e.g. password), possession factor ("what you have", e.g. Mobile ID SIM card), inherence factor ("what you are", e.g. fingerprint, retina pattern, voice).
SAML	Security Assertion Markup Language 2.0 (SAML 2.0) is a version of the SAML standard for exchanging authentication and authorization data between security domains
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)
MFA	Multi-Factor Authentication. Authentication methods that require more than one independent "factors". A factor can be a knowledge factor ("what you know", e.g. password), possession factor ("what you have", e.g. Mobile ID SIM card), inherence factor ("what you are", e.g. fingerprint, retina pattern, voice).
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)

1.3 Referenced documents

- [1] Mobile ID - Client reference guide v2.x
<https://www.swisscom.ch/en/business/mobile-id/technical-details/technical-documents.html>
- [2] Mobile ID – SAML and SuisseID v1.1
<https://www.swisscom.ch/content/dam/swisscom/de/biz/mobile-id/technische-details/pdf/mobileid-saml-and-suisseid-integration-guide-v1-1.pdf>
- [3] Mobile ID - Microsoft AD FS solution guide v1.2
https://www.swisscom.ch/content/dam/swisscom/de/biz/mobile-id/technische-details/pdf/biz_mobile_id_microsoft_AD_FS_solution_guide_v1.2.pdf

2 Overview

Office customers can use Windows Active Directory or various non-Microsoft (third party) identity provider (IDP) to store their users.

Security Assertion Markup Language 2.0 (SAML 2.0) is a version of the SAML standard for exchanging authentication and authorization data between security domains. This interface communicates with a SAML server which could relay the Mobile ID authentication requests over SOAP. We call it an “on premise” SAML/SOAP gateway solution. Basically it 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 simpleSAMLphp in [2].

By using the WS-Federation (WS-Fed) and WS-Trust protocols, Active Directory Federation Services (AD FS) provides claims-based single sign-on for the services in the Microsoft Office service offering. The benefits of using identity federation is to provide the users in the enterprise with a single sign-on (SSO). Microsoft AD FS supports multi-factor authentication (MFA), which adds additional authentication methods to the so-called primary authentication method. Immediately after a successful primary authentication, AD FS passes the primary authenticated user’s identity to the additional authentication method, which performs the authentication and hands the result back to AD FS. At this point, AD FS continues executing the authentication/authorization policy and issues the token accordingly.

Mobile ID Authentication Provider for AD FS is an additional authentication method of AD FS. It implements the client interface of Mobile ID service [3], communicates via SOAP/HTTPS with Mobile ID Servers, and authenticates user with Mobile ID. The Mobile ID Authentication Provider retrieves the user attributes (mobile number, etc.) needed in the authentication process from AD.

3 Architecture und main Scenario

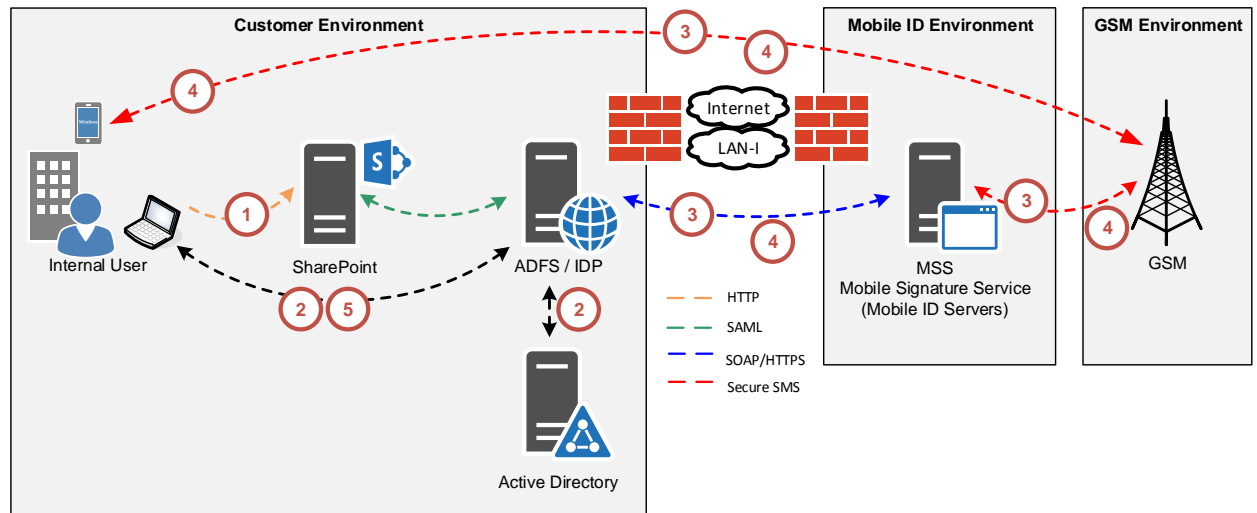


Figure 1: An example of Mobile ID and AD FS / IDP Integration

In this example, the user accesses a Microsoft SharePoint 2013 Server, which supports Multi-Factor authentication, with Mobile ID as the additional authentication method. The (simplified) sequence of data flow is as follows:

1. An unauthenticated user requests a SharePoint site. The SharePoint server redirects the browser to a Mobile-ID enabled AD FS / IDP server(s).
2. AD FS / IDP server authenticates the user with one of the primary methods (e.g. username/password) and hand over the control to the Mobile ID Authentication Provider for AD FS / IDP.
3. The Mobile ID authentication provider sends a SOAP/HTTP request¹ in a mutually authenticated TLS/SSL connection to a Mobile ID server. The request contains the text for login prompt and the mobile number of the user. The Mobile ID server sends the specified login prompt via secure SMS to the specified mobile number.
4. The user enters his Mobile ID PIN in his mobile phone to acknowledge the login request, the mobile phone returns a signed² acknowledgement via secure SMS to the Mobile ID server, which (optionally) verifies the signature, embeds the signature in the SOAP response, and replies to the request in previous step.
5. The Mobile ID Authentication Provider (optionally) verifies the signature in SOAP response, and returns the authentication outcome to AD FS / IDP. AD FS / IDP builds up the claims and redirects the browser back to the SharePoint site, which then grants access to user.

¹ The MSS_SignatureReq service is invoked, see Mobile ID Client Reference Guide [1], chap. 4.2 for details.

² The signature is calculated with the Mobile ID private key in the SIM card, the text to be signed is specified in the SOAP request (step 3).

4 Setup

4.1 Installation and configuration of AD FS / IDP


Refer to [3] and [2] on how to install and configure the AD FS / IDP part.

4.2 Configuration of SharePoint

To allow SharePoint to perform a Mobile ID authentication, SharePoint authentication must be configured for Claim-Based Authentication as described in 4.3.1 to reroute the user requests towards the AD FS / IDP server.

The configuration of SharePoint for AD FS must be performed as described in 4.3.2.

The configuration of SharePoint for a generic, non-AD FS, IDP must be performed as described in 4.3.3.

 SharePoint login timeout is set by default to six minutes, however we suggest you to adapt the execution timeout of SharePoint to 90 Sec. This gives enough time to Mobile ID to handle the authentication requests and ensure a good responsiveness. The process is described in 4.3.4.

4.3 Microsoft Technical Guides

Relevant technical information from Microsoft:

4.3.1 SharePoint 2013: Claims-Based Authentication and Plan for user authentication methods

<http://social.technet.microsoft.com/wiki/contents/articles/14214.sharepoint-2013-claims-based-authentication.aspx>

[https://technet.microsoft.com/en-us/library/cc262350\(v=office.15\).aspx](https://technet.microsoft.com/en-us/library/cc262350(v=office.15).aspx)

4.3.2 Configure SAML-based claims authentication with AD FS in SharePoint 2013

[https://technet.microsoft.com/en-us/library/hh305235\(v=office.15\).aspx](https://technet.microsoft.com/en-us/library/hh305235(v=office.15).aspx)

4.3.3 Implement SAML-based authentication in SharePoint Server 2013

[http://technet.microsoft.com/en-us/library/dn720355\(v=office.15\).aspx](http://technet.microsoft.com/en-us/library/dn720355(v=office.15).aspx)

4.3.4 Increase SharePoint Execution Timeout

<http://geekswithblogs.net/DennisBottjer/archive/2009/04/13/increase-sharepoint-execution-timeout.aspx>

4.3.5 Other useful links

SharePoint Authentication and Session Management

<http://blog.robgarrett.com/2013/05/06/sharepoint-authentication-and-session-management/>

Azure Active Directory Authentication Libraries

<https://azure.microsoft.com/en-us/documentation/articles/active-directory-authentication-libraries/>

SharePoint for IT pros

<https://technet.microsoft.com/en-us/office/dn788776>