Mobile ID for Microsoft Solutions

Solution guide

Version: 1.0

Swisscom (Switzerland) Ltd

swisscom

Contents

1 Introduction

Mobile ID (MID) provides strong authentication based cryptographic materials stored and protected in the SIM card of the user's mobile phone. Microsoft Office is a suite of office productivity applications used in homes and businesses of all size. Microsoft Office 365[1] is a Web-based version of Microsoft's Office suite of enterprise-grade productivity applications. It is delivered to users through the cloud and includes Exchange Online for email, SharePoint Online for collaboration, Skype for Business (formerly Lync Online) for unified communications and a suite of Office Web Apps, Web-based versions of the traditional Microsoft Office suite of applications.

This document provides information on how to integrate Mobile ID Authentication as an additional authentication method into Microsoft Office, Office 365 and Skype for Business based on AD FS. It also includes a brief outlook about the upcoming modern authentication, which brings Active Directory Authentication Library (ADAL)-based sign to Office 2013 Windows Clients as well as Lync / Skype for Business and potentially to the Windows Login.

1.1 Targeted 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 Microsoft Office Suite and the Active Directory Federation Services (AD FS). This manual assumes that you are familiar with the Swisscom Mobile ID service [1] and Microsoft Office Suites, including the Active Directory Federation Services [1].

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
Azure AD	Azure Active Directory https://azure.microsoft.com/en-us/
IDP	Identity 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).
MSOIDSVC	Microsoft Online Services Sign-In Assistant
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] Microsoft Office 365: http://office.microsoft.com/en-us/business/

1.3 Referenced documents

[1] Mobile ID - Client reference guide v2.x.pdf
https://www.swisscom.ch/content/dam/swisscom/de/biz/mobile-id/technische-details/pdf/mobile-id-client-reference-guide-v-2-7.pdf

[2] Mobile ID - Microsoft AD FS solution guide
https://www.swisscom.ch/content/dam/swisscom/de/biz/mobile-id/technische-details/pdf/biz_mobile_id_microsoft_ADFS_solution_guide_v1.2.pdf

[3] Mobile ID – SAML and Suisse ID
https://www.swisscom.ch/content/dam/swisscom/de/biz/mobile-id/technische-details/pdf/mobileid-saml-and-suisseid-integration-guide-v1-1.pdf

2 Overview

Office customers can use Windows Active Directory, Windows Azure Active Directory or various non-Microsoft (third party) identity provider (IDP) solutions to store their user directories. By using the WS-Federation (WS-Fed) and WS-Trust protocols, Active Directory Federation Services (ADFS) 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).

Here the main topics referred and used in this document:

- SAML 2.0 enables web-based authentication and authorization scenarios including cross-domain single sign-on (SSO), which helps reduce the administrative overhead of distributing multiple authentication tokens to the user. Refer to [3] for additional documentation and information.
- The ADAL based authentication stack enables applications like Microsoft Office 2013 to engage in browser-based authentication (also known as passive authentication) where the user is directed to a web page from the identity provider to authenticate, including multi-factor authentication (MFA).
- Microsoft ADFS supports MFA, which adds additional authentication methods to the so-called primary authentication method. Immediately after a successful primary authentication, ADFS passes the primary authenticated user's identity to the additional authentication method, which performs the authentication and hands the result back to ADFS. At this point, ADFS continues executing the authentication/authorization policy and issues the token accordingly.

Mobile ID Authentication Provider for ADFS is an additional authentication method of ADFS. It implements the client interface of Mobile ID service, 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.

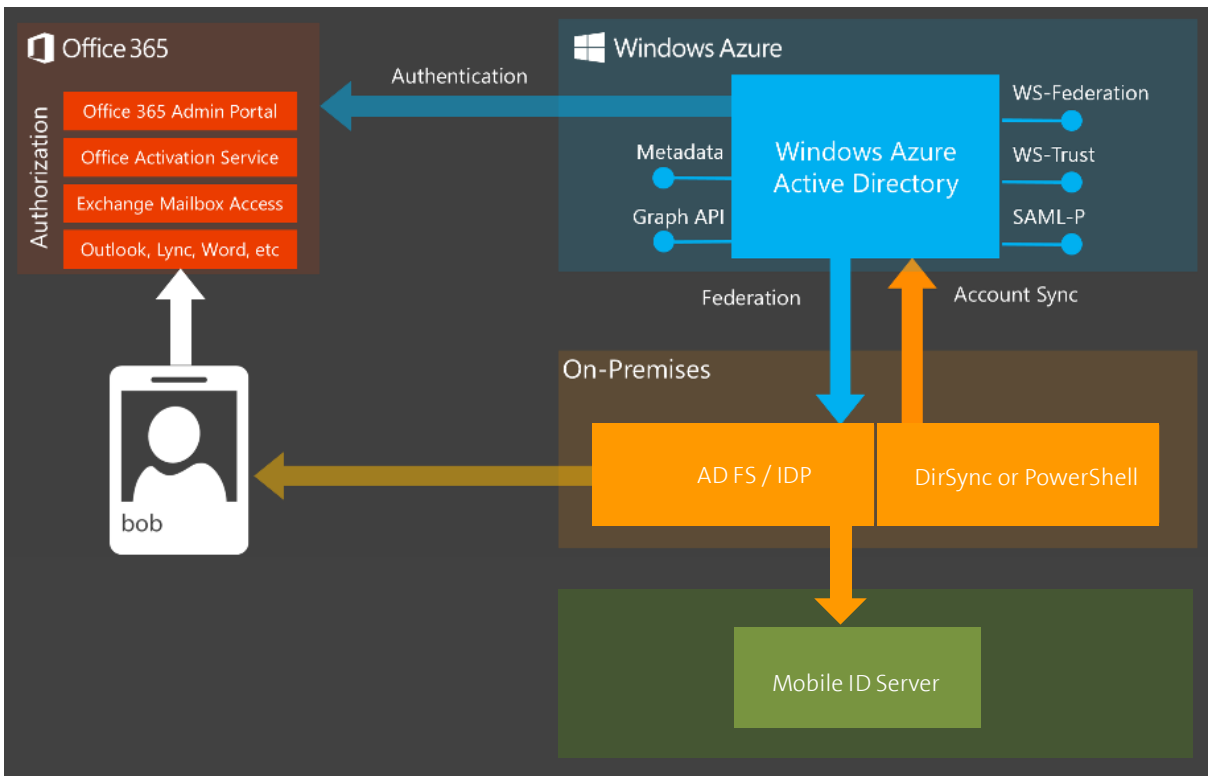

Figure 1: Identity Diagram

2.1 ADAL based sign-in into Office client apps

Modern authentication brings Active Directory Authentication Library (ADAL)-based sign-in to Office client apps across platforms. This enables sign-in features such as Multi-Factor Authentication (MFA), SAML-based third-party Identity Providers with Office client applications, smart card and certificate-based authentication, and it removes the need for Outlook to use the basic authentication protocol. Furthermore, ADAL is indicated for scenarios in which you need apps to have their own identity, without user involvement.

The chart below shows the availability of modern authentication across Office applications. Please verify the latest information on 4.1.6:

Office Client Application	Windows	OS X	Windows Phone	iOS	Android
Office clients	Available now for Office 2013 and Office 2016.	Office 2016 Mac Preview supports ADAL including Word, Excel, PowerPoint and OneNote. OneNote was released with ADAL in 2014.	Coming soon.	Word, Excel and PowerPoint are available now.	For Android phones: Word, Excel and PowerPoint are available now. For Android tablets: Word, Excel and PowerPoint are coming soon.
Skype for Business (formerly Lync)	Included in Office client	TBD	Coming soon.	Available now*.	Available now*.
Outlook	Included in Office client.	Outlook uses ADAL for licensing but not yet for mailbox access.	Coming soon.	Available now*.	Available now.
OneDrive for Business	Included in Office client.	OneDrive for Business Sync is TBD.	Available now for Windows Phone 8.1.	OneDrive for Business is available now.	OneDrive for Business is available now.
Legacy clients	There are no plans for Office 2010 or Office 2007 to support ADAL-based authentication.	There are no plans for Office for Mac 2011 to support ADAL-based authentication.	There are no plans for Office on Windows Phone 7 to support ADAL-based authentication.	There are no plans to enable older Outlook iOS clients.	There are no plans to enable older Outlook Android clients.

*Not recommended for split domain configuration that includes both Skype for Business Online and Skype for Business Server.

To address these new requirements, Azure AD provides support for the OAUTH 2.0 protocol, which is the primarily protocol for authorization and delegated authentication. Using OAuth 2.0, an application can gain access to impersonate the user, or users in his organization to access the resource. The OAuth 2.0 protocol uses JSON Web Token (JWT). Modern authentication is available to any customer running the March 2015 or later update for Office 2013 but is disabled by default. Office 2016 clients support modern authentication by default, and no action is needed for the client to use these new flows.

3 Architecture und main Scenarios

This chapter describes how to use Microsoft Solutions in Business Environments from different ways based on Multi-Factor authentication, with Mobile ID as the additional authentication method.

3.1 Strong Authentication for Microsoft Office 365

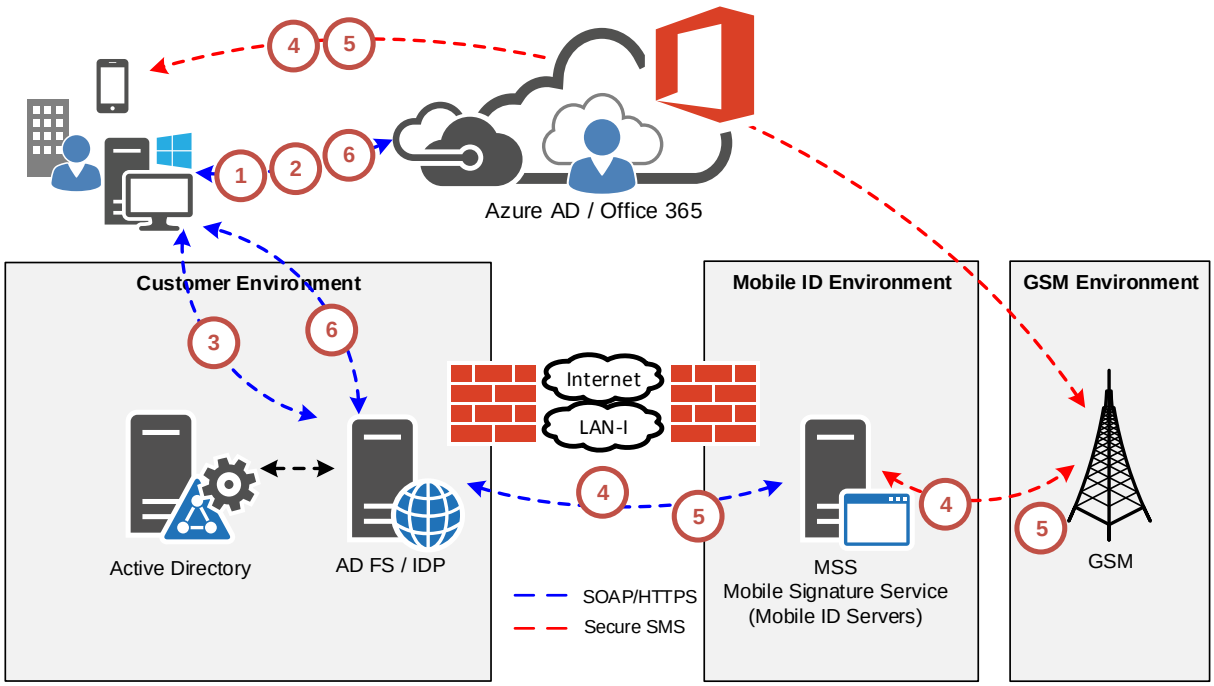

Figure 2: An example of Microsoft Office 365 over AD FS

In the above schema, the user tries to access a Web-based Office 365 service like Word, Excel, PowerPoint or SharePoint Online from an internet browser. When authenticating to Office 365 the Internet browser will establish a connection to the organization's AD FS / IDP server. The authentication flow is the following:

1. The user hits the Web-based Office 365 service. The service tells the client that it needs an authentication token signed by Azure AD, and returns the sign-in service URL of Azure AD via a HTTP 302 redirected in order to go get a ticket from there.
2. The client goes to Azure AD asking for an authentication token. The sign-in service takes the UPN the user types in and then knows if it is a federated domain. It then says it cannot sign you in; it needs a logon token signed by your on-premises claims provider, i.e. the on-premises Mobile-ID enabled AD FS server.
3. The client goes to the AD FS server to request a logon token. The AD FS server asks to user to authenticate (via Integrated Windows Authentication) against the on-premises Active Directory and to the Mobile ID authentication provider.
4. The Mobile ID authentication provider sends a SOAP/HTTP request 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.

5. The user enters his Mobile ID PIN in his mobile phone to acknowledge the login request, the mobile phone returns a signed 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. The Mobile ID Authentication Provider (optionally) verifies the signature in SOAP response, and returns the authentication outcome to AD FS.
6. AD FS builds up the claims and redirects the browser back to the application server, which then grants access to user.

3.2 Strong Authentication for Microsoft Skype for Business (Lync)

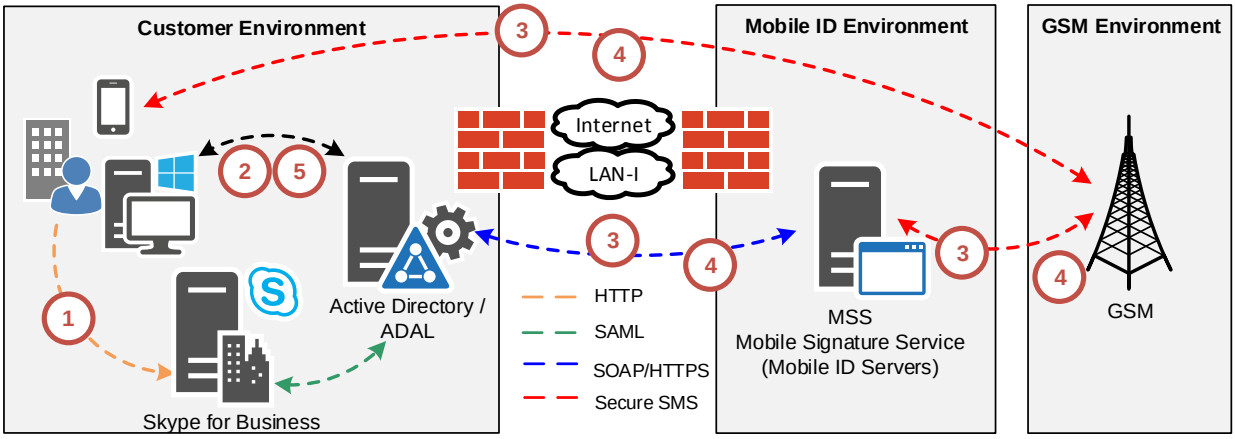

Figure 3: An example of Microsoft Skype for Business over ADAL

As Skype for Business client continues to consume services from both Skype for Business Server and Exchange, to address SSO requirements to support both Lync Online and Exchange Online connectivity, Microsoft have adopted Azure AD Authentication Library (ADAL) in Skype for Business Server. This also opens the path to enabling multi-factor authentication that expands beyond desktop client, as mobile client is now supported for multi-factor authentication.

3.3 Strong Authentication for Microsoft Office

Office 2016 can perform modern authentication through its support for MFA. The goal of strong Authentication is to create a layered defense and make it more difficult for an unauthorized person to access the data. MFA is preferable because it offers additional protection and mitigates the security risks, such as a stolen or compromised password. Check the latest Information on 4.1.6.

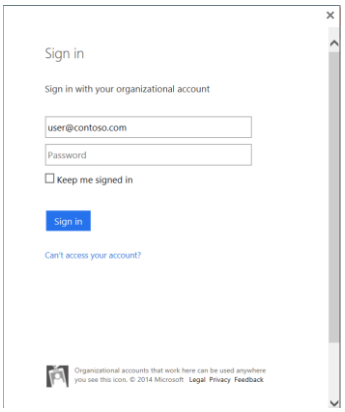

Figure 4: Modern authentication for Office 2013 Windows client

The following figure shows how the updated Office 2013 device apps (on Windows) enable users to sign in with MFA. The authentication for federated users follows these steps:

1. Azure AD redirects the user to the sign-in web page hosted by the identity provider of record for the Office 365 tenant. The identity provider is determined by the domain specified in the user's sign in name.
2. The user signs in on the sign in web page on his or her device.
3. The identity provider returns a token to Azure AD when the user is successfully signed in.
4. Azure AD returns a JSON Web Token (JWT) to the Office device app, and the device app is authenticated by using a JWT with Office 365.

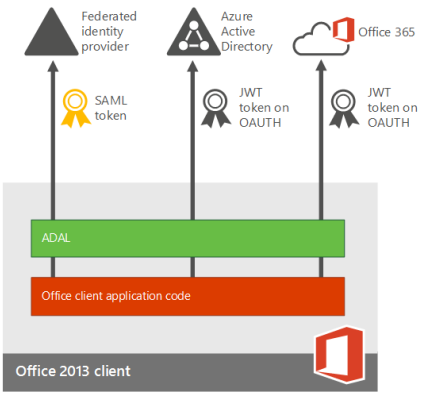

Figure 5: Microsoft Office using the ADAL component

In order for these clients to use modern authentication features, the Windows user running Office 2013 needs to have certain registry keys set.

3.4 Strong Authentication for Microsoft Windows

The MID two-factor authentication solution is designed to help Microsoft enterprise customers ensure that valuable resources are accessible only by authorized users. It delivers a simplified and consistent user login experience, virtually eliminates help desk calls related to password management, and helps organizations comply with regulatory requirements. The use of two-factor authentication instead of just traditional static passwords to access a Windows environment is a necessary critical step for information security.

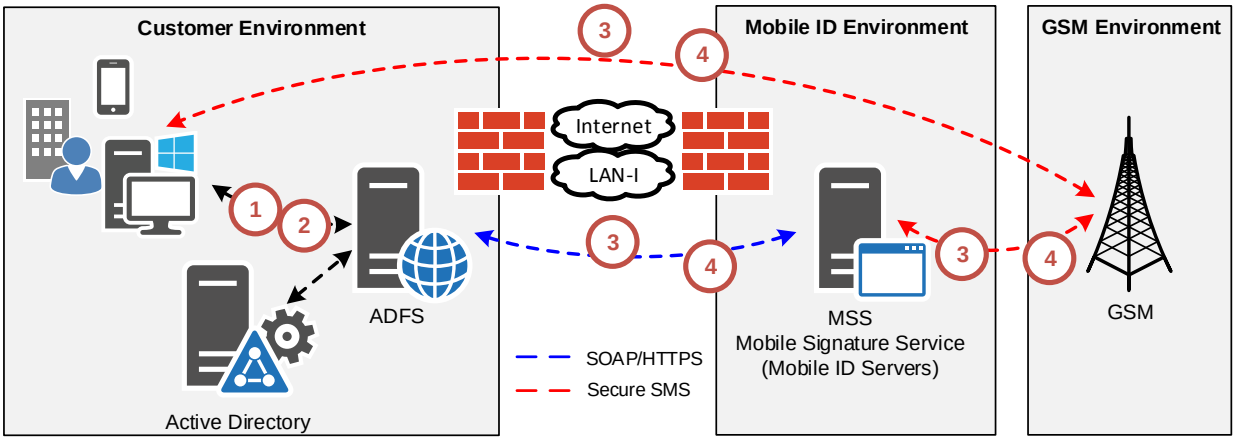

Figure 6: An example of Windows Login

In the meantime, Microsoft is making Windows ADAL enabled, alternative solutions based on the extensibility of Windows Login should be considered. Please refer to 4.1.5 that can be used in conjunction with RADIUS.

4 Setup and configuration

4.1.1 Setup Mobile ID for ADFS

Refer to [1] on how to setup and configure Mobile ID for ADFS.

4.1.2 How to setup ADFS 2012 R2 for Office 365

http://blogs.technet.com/b/rmilne/archive/2014/04/28/how-to-install-adfs-2012-r2-for-office-365.aspx

4.1.3 Enable Modern Authentication for Office 2013 on Windows devices

https://support.office.com/en-us/article/Enable-Modern-Authentication-for-Office-2013-on-Windows-devices-7dc1c01a-090f-4971-9677-f1b192d6c910

4.1.4 AD FS Configuration for Skype for Business

http://techmikal.com/2014/02/20/lync-passive-authentication-with-two-factor-authentication-part-i/

4.1.5 Windows Login with pGINA.org

http://pgina.org/docs/v3.1/radius.html

4.1.6 Office 365 modern authentication public preview

https://blogs.office.com/2015/11/19/updated-office-365-modern-authentication-public-preview/

4.2 Microsoft Technical Guides

Topic	Link
Overview of Active Directory Federation Services	https://technet.microsoft.com/en-us/windowsserver/dd448613.aspx
Supported scenarios for using AD FS to set up single sign-on in Office 365, Azure, or Intune	https://support.microsoft.com/en-us/kb/2510193
Office URLs and IP Address ranges	https://support.office.com/de-de/article/URLs-und-IP-Adressbereiche-von-Office-365-8548a211-3fe7-47cb-abb1-355ea5aa88a2?ui=de-DE&rs=de-DE&ad=DE
Description of Microsoft Online Services Sign-In Assistant (MOS SIA)	https://community.office365.com/en-us/w/sso/534
OAuth 2.0 in Azure AD	https://msdn.microsoft.com/en-us/library/azure/dn645545.aspx
How to troubleshoot sign-in issues with Office modern authentication when you use AD FS	https://support.microsoft.com/en-us/kb/3052203
Supported Token and Claim Types	https://azure.microsoft.com/en-us/documentation/articles/active-directory-token-and-claims/