Disclaimer

Disclaimer of Warranties and Limitation of Liabilities

All information contained in this document is provided 'as is'; VASCO Data Security assumes no responsibility for its accuracy and/or completeness.

In no event will VASCO Data Security be liable for damages arising directly or indirectly from any use of the information contained in this document.

Copyright

Copyright © 2014 VASCO Data Security, Inc, VASCO Data Security International GmbH. All rights reserved. VASCO®, Vacman®, IDENTIKEY AUTHENTICATION®, aXsGUARD™ and DIGIPASS® logo are registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH in the U.S. and other countries. VASCO Data Security, Inc. and/or VASCO Data Security International GmbH own or are licensed under all title, rights and interest in VASCO Products, updates and upgrades thereof, including copyrights, patent rights, trade secret rights, mask work rights, database rights and all other intellectual and industrial property rights in the U.S. and other countries. Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation. Other names may be trademarks of their respective owners.
# Table of Contents

1 Overview......................................................................................................................... 4
   1.1 Two factor authentication............................................................................................ 4
   1.2 Scope ........................................................................................................................... 4

2 Components...................................................................................................................... 5
   2.1 Microsoft ...................................................................................................................... 5
      2.1.1 Office 365 .............................................................................................................. 5
      2.1.2 Active Directory Federation Server ........................................................................ 5
   2.2 VASCO ......................................................................................................................... 5
      2.2.1 IDENTIKEY Authentication Server ..................................................................... 5
      2.2.2 DIGIPASS Authentication for Outlook Web Access ............................................. 5
      2.2.3 IDENTIKEY Federation Server ........................................................................... 5

3 Solutions......................................................................................................................... 7
   3.1 Method 1: DIGIPASS Authentication for Outlook Web Access ................................. 7
      3.1.1 Architecture ........................................................................................................... 7
      3.1.2 Pre-requisites ........................................................................................................ 7
   3.2 Method 2: Microsoft UAG or similar with IDENTIKEY Authentication Server .......... 8
      3.2.1 Architecture .......................................................................................................... 8
      3.2.2 Pre-Requisites ....................................................................................................... 8
   3.3 Method 3: IDENTIKEY Federation Server with AD FS solution .............................. 9
      3.3.1 Architecture ......................................................................................................... 9
      3.3.2 Pre-requisites ..................................................................................................... 9
   3.4 Method 4: IDENTIKEY Federation Server solution .................................................. 10
      3.4.1 Architecture ....................................................................................................... 10
      3.4.2 Pre-requisites ..................................................................................................... 10

4 Differences ..................................................................................................................... 11
   4.1 Method 1: DIGIPASS Authentication for Outlook Web Access ............................... 11
4.1.1 Installation ................................................................................................................. 11
4.1.2 Configuration ............................................................................................................ 11
4.1.3 Workings ................................................................................................................... 11
4.1.4 Application support ................................................................................................ 11
4.1.5 Supported back-end authentication ......................................................................... 11
4.2 Method 2: Microsoft UAG or similar with IDENTIKEY Authentication Server .......... 12
  4.2.1 Installation ................................................................................................................. 12
  4.2.2 Configuration ............................................................................................................ 12
  4.2.3 Workings ................................................................................................................... 12
  4.2.4 Application support ................................................................................................ 12
  4.2.5 Supported back-end authentication ......................................................................... 12
4.3 Method 3: IDENTIKEY Federation Server with AD FS solution .................................. 13
  4.3.1 Installation ................................................................................................................. 13
  4.3.2 Configuration ............................................................................................................ 13
  4.3.3 Workings ................................................................................................................... 13
  4.3.4 Application support ................................................................................................ 13
  4.3.5 Supported back-end authentication ......................................................................... 13
4.4 Method 4: IDENTIKEY Federation Server solution ....................................................... 14
  4.4.1 Installation ................................................................................................................. 14
  4.4.2 Configuration ............................................................................................................ 14
  4.4.3 Workings ................................................................................................................... 14
  4.4.4 Application support ................................................................................................ 14
  4.4.5 Supported back-end authentication ......................................................................... 14
5 Conclusions ...................................................................................................................... 15
1 Overview

1.1 Two factor authentication

Many organizations still rely on a username and password to protect their data or external access. However passwords are often very simple and very easy guessed, cracked or even stolen. Once it is compromised it can take quite a lot of time before anyone notices that it has been compromised. Recently a lot of services are being moved to the “cloud” where anyone can access the service from anywhere. This means that the users are often accessing it from outside the safe network, making password protection even more important and harder.

Two factor authentication of VASCO Data Security will add an additional factor, called DIGIPASS, to your password. The DIGIPASS will generate a One Time Password, or OTP, which you can use in combination with your password. This means that people will need a specific device and password if they want to gain access. Imagine if the device were to be stolen, this will be noticed quickly and that way access using that device can be denied, stopping any attacker quickly.

With this in mind you can secure your Office 365 accounts, granting you the freedom of Office 365 with the hardened security of two factor authentication.

1.2 Scope

This paper handles the four ways tested by VASCO Data Security to connect two factor authentication, by VASCO Data Security, with Office 365.

The four ways which will be discussed involve two factor authentication integration using an IDENTIKEY Federation Server (this can be done with two methods), IDENTIKEY Authentication Server web filter or a Microsoft UAG or similar. All methods have a DIGIPASS and IDENTIKEY Authentication Server as two factor authentication solution in common.

These methods are:

- Method 1: DIGIPASS Authentication for Outlook Web Access
- Method 2: Microsoft UAG or similar with IDENTIKEY Authentication Server
- Method 3: IDENTIKEY Federation Server with AD FS solution
- Method 4: IDENTIKEY Federation Server solution

This paper will not cover the setup for Office 365 with your local Active Directory database. This is mandatory to add two factor authentication. Neither will the setup of the IDENTIKEY Authentication Server be discussed, this setup is the same for all solutions. The information to create these setups is readily available in whitepapers on the VASCO website.

This paper focuses on the essential differences in these solutions and sketches the environment used for these solutions.
2 Components

2.1 Microsoft

2.1.1 Office 365
Office 365 refers to the Microsoft Office collaboration and productivity tools that are delivered to you through the Internet. This enables your work force to access and store documents, access email and even web conference from nearly any device that has an Internet connection.

2.1.2 Active Directory Federation Server
Active Directory Federation Services (AD FS) is based on the emerging, industry-supported Web Services Architecture, which is defined in WS-* specifications. AD FS helps you use single sign-on (SSO) to authenticate users to multiple, related Web applications over the life of a single online session. AD FS accomplishes this by securely sharing digital identity and entitlement rights across security and enterprise boundaries.

2.2 VASCO

2.2.1 IDENTIKEY Authentication Server
IDENTIKEY Authentication Server is an off-the-shelf centralized authentication server that supports the deployment, use and administration of DIGIPASS strong user authentication. It offers complete functionality and management features without the need for significant budgetary or personnel investments.

IDENTIKEY Authentication Server is supported on 32bit systems as well as on 64bit systems.

IDENTIKEY Appliance is a standalone authentication appliance that secures remote access to corporate networks and web-based applications.

⚠️ The use and configuration of an IDENTIKEY Authentication Server and an IDENTIKEY Appliance is similar. The IDENTIKEY Appliance is Linux based.

2.2.2 DIGIPASS Authentication for Outlook Web Access
The DIGIPASS Authentication for Outlook Web Access is an add-on for Internet Information Services (IIS) and can be configured to intercept authentication requests to Web sites using the HTTP forms based authentication mechanism. It allows users to use one-time passwords (OTPs) instead of static passwords. The plug-in intercepts authentication requests, validates the OTP, and replaces it with the static password expected by the back-end. The OTPs are validated using an IDENTIKEY Authentication Server or IDENTIKEY Appliance.

2.2.3 IDENTIKEY Federation Server
IDENTIKEY Federation Server is a virtual appliance which offers a federated login and provides Single Sign-On for web applications. The IDENTIKEY Federation Server accepts incoming authentication requests using SAML2, A-Select or Microsoft WS-Federation. The authentication requests can be forwarded via RADIUS, LDAP, SAML2 and OAuth.

Since version 1.4 of the IDENTIKEY Federation Server, the Microsoft Office 365 applications are directly supported.

The following products are fully supported with two factor authentication:
<table>
<thead>
<tr>
<th>Product</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office 365 web</td>
<td>Web</td>
</tr>
<tr>
<td>Lync 2013</td>
<td>Desktop</td>
</tr>
<tr>
<td>Outlook 2013</td>
<td>Desktop</td>
</tr>
<tr>
<td>Outlook Web App</td>
<td>Web</td>
</tr>
<tr>
<td>Exchange ActiveSync</td>
<td>Mobile</td>
</tr>
<tr>
<td>Exchange Online</td>
<td>Web</td>
</tr>
<tr>
<td>Sharepoint</td>
<td>Web</td>
</tr>
</tbody>
</table>

The following products are supported using username/password combination:

<table>
<thead>
<tr>
<th>Product</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lync 2013</td>
<td>Desktop</td>
</tr>
<tr>
<td>Outlook 2013</td>
<td>Desktop</td>
</tr>
<tr>
<td>Exchange ActiveSync</td>
<td>Mobile</td>
</tr>
</tbody>
</table>
3 Solutions

3.1 Method 1: DIGIPASS Authentication for Outlook Web Access

There are several types of DIGIPASS Authentication for web interface but for this setup an DIGIPASS Authentication for Outlook Web Access using Forms was used.

3.1.1 Architecture

3.1.2 Pre-requisites

- Active Directory Federation Service
- Active Directory Federation Service – Office 365 connection
- DIGIPASS Authentication for Outlook Web Access using forms
- IDENTIKEY Authentication Server running
3.2 Method 2: Microsoft UAG or similar with IDENTIKEY Authentication Server

3.2.1 Architecture

3.2.2 Pre-Requisites

- Active Directory Federation Service
- Active Directory Federation Service – Office 365 connection
- Microsoft UAG or similar or similar – Active Directory Federation Server connection
- IDENTIKEY Federation Server with basic setup
- IDENTIKEY Authentication Server running
3.3 Method 3: IDENTIKEY Federation Server with AD FS solution

3.3.1 Architecture

3.3.2 Pre-requisites

- Active Directory Federation Service
- Active Directory Federation Service – Office 365 connection
- IDENTIKEY Federation Server with basic setup
- IDENTIKEY Authentication Server running
3.4 Method 4: IDENTIKEY Federation Server solution

3.4.1 Architecture

3.4.2 Pre-requisites
- Office 365 with federated domain
- IDENTIKEY Federation Server with basic setup
- IDENTIKEY Authentication Server running
4 Differences

These solutions accomplish the same goal; they add two factor Authentication to your Office 365 login process. Even as both solutions have the same outcome, their method of achieving this is very different.

4.1 Method 1: DIGIPASS Authentication for Outlook Web Access

4.1.1 Installation

The installation of the DIGIPASS Authentication for Outlook Web Access is short and straightforward. It can swiftly be executed as you can turn the filter off and on with no downtime. For the installation of the filter you must allow traffic from the web server to the IDENTIKEY Authentication Server over TCP port 20003 (or TCP 20004 when using the secure option).

4.1.2 Configuration

The DIGIPASS Authentication for Outlook Web Access has only the capability to capture GET and POST requests on the IIS web server. As a result the configuration is very simple and straightforward.

Additional configuration to the IDENTIKEY Authentication Server can be required depending on the selected login method.

- User login with: username and Active Directory password + OTP, there is no additional configuration required.
- User login with: username and OTP or username and pin + OTP, the IDENTIKEY will need to know the Active Directory password of the user and an additional tool to synchronize the password is required.

4.1.3 Workings

Once installed, the DIGIPASS Authentication for Outlook Web Access works transparent and fast. This is because of the method the IDENTIKEY web filter uses. The filter will capture the credentials the user has entered and send these to the IDENTIKEY Authentication Server for verification. If successful the filter will receive the username and Active Directory password. It will then pass these credentials to the IIS server to continue the login procedure. The DIGIPASS Authentication for Outlook Web Access only works on an IIS application server.

The user will not even notice the filter is there.

4.1.4 Application support

The IDENTIKEY Authentication Server web filter is installed on the Internet and Information Service from Microsoft and is only able to capture forms based authentication requests. This translates that you are limited to only in-house web sites.

4.1.5 Supported back-end authentication

The web filter can use IDENTIKEY Authentication Servers and IDENTIKEY Appliances as authentication servers.
4.2 Method 2: Microsoft UAG or similar with IDENTIKEY Authentication Server

4.2.1 Installation
Except for the basic installation of an IDENTIKEY Authentication Server there are no additional installations to be done.

4.2.2 Configuration
You will need to configure the Microsoft UAG or similar to use the IDENTIKEY Authentication Server as a RADIUS back-end for authentication.

In this setup the difficulty is not in the configuration of the Vasco solution but the setup of the entire system with Microsoft’s UAG or similar.

4.2.3 Workings
In this setup the user trying to login Office 365 will be redirected to the AD FS. The AD FS will then connect to the UAG or similar for authentication, while the UAG or similar will use IDENTIKEY Authentication Server for the two factor authentication.

4.2.4 Application support
With the connection to the Microsoft UAG or similar you can secure most connections managed by Microsoft.

4.2.5 Supported back-end authentication
Microsoft’s UAG or similar supports the RADIUS connection to our systems so it can connect to IDENTIKEY Authentication Server and the IDENTIKEY Appliance.
4.3 Method 3: IDENTIKEY Federation Server with AD FS solution

4.3.1 Installation
The installation of the IDENTIKEY Federation Server on the other hand requires a bit more planning. This is an additional appliance and needs to be planned. This includes the planning of an IP address and additional resources (as the IDENTIKEY Federation Server is a virtual appliance). The IDENTIKEY Federation Server needs to be accessible from the internet so this needs to be placed in the Demilitarized Zone to be functioning optimally. When the IDENTIKEY Federation Server is placed in the DMZ, ports have to be opened between the federation server and the internal network depending on the required services (RADIUS port to your IDENTIKEY Authentication Server, LDAP port to your Active Directory).

4.3.2 Configuration
The IDENTIKEY Federation Server will require more of your time to configure. Mainly the additional configuration is related to connecting the IDENTIKEY Federation Server with third parties and all the extra options it offers.

One part of the additional configuration relates to the fact that this is a separate server that is accessible from the internet. Therefore you must ensure that the connections are secure, using HTTPS. In short you will need to configure certificates.

You are also required to perform additional settings on the Active Directory Federation Service Server. To make the configuration on the Active Directory side a bit easier, an attribute store has been created.

4.3.3 Workings
Once installed, the IDENTIKEY Federation Server will be placed between the Active Directory Federation Service server and the IDENTIKEY Authentication Server. This will have little impact on request processing speed but will stay noticeable, even just for mere moments.

This is because of the different approach in authentication process. The IDENTIKEY Federation Server will act as the identity provider and additionally provide Single Sign-On for web applications. Alongside this different approach the IDENTIKEY Federation Server supports plenty of additional methods to connect to it and enjoy the Single Sign-On for web applications it offers. The additional methods are SAML2 (a very universal authentication method) and A-Select.

The extra functionality to add applications using SAML2 means that the timing of the IDENTIKEY Federation Server needs to be synchronized with a global NTP server. This must ensure that the timing in the SAML2 messages are within margin (1 minute).

4.3.4 Application support
The IDENTIKEY Federation Server supports any application that can use A-Select or SAML2 as authentication protocol. This means that it can be any internal or external website or application. In addition the IDENTIKEY Federation Server provides Single Sign-On for web applications so only one login is required to access all the websites or applications.

4.3.5 Supported back-end authentication
The IDENTIKEY Federation Server supports several back-end authentication protocols. It supports RADIUS, SAML2, LDAP and OAuth.
4.4 Method 4: IDENTIKEY Federation Server solution

4.4.1 Installation

The installation of the IDENTIKEY Federation Server on the other hand requires a bit more planning. This is an additional appliance and needs to be planned. This includes the planning of an IP address and additional resources (as the IDENTIKEY Federation Server is a virtual appliance). The IDENTIKEY Federation Server needs to be accessible from the internet so this needs to be placed in the Demilitarized Zone to be functioning optimally. When the IDENTIKEY Federation Server is placed in the DMZ, ports have to be opened between the federation server and the internal network depending on the required services (RADIUS port to your IDENTIKEY Authentication Server, LDAP port to your Active Directory).

4.4.2 Configuration

The configuration to be done on the IFS is quite small. Enable a checkbox and the device will listen to WS-Fed protocol from Office 365.

Additionally you will be required to configure certificates as this is a separate server that is accessible from the internet. Therefore you must ensure that the connections are secure, using HTTPS.

There is also a small part of the configuration that needs to happen from a machine running a Microsoft OS connected to the domain. From this device you will need to open a PowerShell prompt and execute three commands to make sure that the Office 365 environment will connect to the IFS.

4.4.3 Workings

In this setup Office 365 will build up a WS-Federation trust with the IFS directly. This kicks out the possibility of additional problems that may occur with AD FS. The IFS will translate the WS-Federation messages for the IDENTIKEY server which will do the actual authentication.

The IFS will act as the identity provider directly for Office 365 and additionally provide Single Sign-On for web applications. Alongside this different approach the IDENTIKEY Federation Server supports plenty of additional methods to connect to it and enjoy the Single Sign-On for web applications it offers. The additional methods are SAML2 (a very universal authentication method) and A-Select.

The extra functionality to add applications using SAML2 means that the timing of the IDENTIKEY Federation Server needs to be synchronized with a global NTP server. This must ensure that the timing in the SAML2 messages are within margin (1 minute).

4.4.4 Application support

The IDENTIKEY Federation Server supports any application that can use A-Select or SAML2 as authentication protocol. This means that it can be any internal or external website or application. In addition the IDENTIKEY Federation Server provides Single Sign-On for web applications so only one login is required to access all the websites or applications.

This type of integration with Office 365 enables the support of Office 365’s rich clients, Outlook and Lync.

4.4.5 Supported back-end authentication

The IDENTIKEY Federation Server supports several back-end authentication protocols. It supports RADIUS, SAML2, LDAP and OAuth.
## Conclusions

<table>
<thead>
<tr>
<th>Method 1: DIGIPASS Authentication for Outlook Web Access</th>
<th>Method 2: Microsoft UAG or similar with IDENTIKEY Authentication Server</th>
<th>Method 3: IDENTIKEY Federation Server over AD FS solution</th>
<th>Method 4: IDENTIKEY Federation Server solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning</td>
<td>Planning for an additional machine</td>
<td>Planning for an additional machine</td>
<td>Planning for an additional machine</td>
</tr>
<tr>
<td>Installation</td>
<td>Simple wizard</td>
<td>Only IAS</td>
<td>Plug and play</td>
</tr>
<tr>
<td>Configuration</td>
<td>Easy and straight-forward</td>
<td>Setting up a RADIUS back-end</td>
<td>More complex</td>
</tr>
<tr>
<td>Application support</td>
<td>Only supports IIS password replacement</td>
<td>Internal Microsoft applications</td>
<td>In addition to Office 365 supports plenty of other applications as long as they support SAML2 or A-Select.</td>
</tr>
<tr>
<td>Web SSO</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Secure connection</td>
<td>The IIS takes care of this</td>
<td>Is handled by the Microsoft products</td>
<td>Needs a certificate to provide a secure connection</td>
</tr>
<tr>
<td>Back-end authentication</td>
<td>Only IDENTIKEY Authentication Server</td>
<td>Only IDENTIKEY Authentication Server</td>
<td>IDENTIKEY Authentication Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OAuth and MDP</td>
<td>OAuth and MDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IDENTIKEY Federation Server</td>
<td>IDENTIKEY Federation Server</td>
</tr>
</tbody>
</table>

Looking at difficulty of implementation between Office 365 - IDENTIKEY Federation Server (starting from version 1.4) and Office 365 – IDENTIKEY Federation Server with AD FS as intermediate, it is advised to aim for the installation Office 365 – IDENTIKEY Federation Server. This will eliminate any problems in regards to AD FS.
Securing your connection to Office 365 using Microsoft’s UAG or similar is no simple matter. Securing the UAG or similar login with IDENTIKEY Authentication Server is quite easy. However setting up UAG or similar and connecting it with all other services is more difficult. Unless you have the complete setup running, this setup is not advised.

The IDENTIKEY Federation Server requires a bit more configuration to install. Even so, unless you already have a working setup with Office 365 – AD FS, connecting Office 365 directly to IDENTIKEY Federation Server will bear a simpler environment with more possibilities.

The IDENTIKEY Federation Server really shines when you use it for Office 365 and your other internal or external sites. Once you combine multiple services to use the IDENTIKEY Federation Server as your identity provider, you can use the full power of the Single Sign-On for web applications, alternative back-end and account linking.

In short: to secure your Office 365 applications it is always advised to install an IDENTIKEY Federation Server to connect Office 365 directly to it even over the simpler WEB filter DIGIPASS Authentication for Outlook Web Access. Unless they only wish to secure Office 365 and already have an active Office 365 – AD FS setup.