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 © 2013 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** .......................................................................................................................... 3

2  **Technical Concepts** ......................................................................................................... 4

   2.1  Manage Engine .................................................................................................................. 4

      2.1.1  Password Manager Pro ........................................................................................... 4

   2.2  VASCO ............................................................................................................................ 4

      2.2.1  IDENTITY Authentication server ............................................................................ 4

3  **Password Manager Pro setup** ............................................................................................ 5

   3.1  Architecture ..................................................................................................................... 5

   3.2  Prerequisites .................................................................................................................... 5

   3.3  Password Manager Pro .................................................................................................... 5

   3.4  Test the setup ................................................................................................................ 7

4  **Solution** ............................................................................................................................. 8

   4.1  Architecture ..................................................................................................................... 8

   4.2  IDENTITY Authentication Server ................................................................................... 8

      4.2.1  Policies .................................................................................................................... 8

      4.2.2  Client ..................................................................................................................... 9

      4.2.3  Domain ................................................................................................................... 10

      4.2.4  User ..................................................................................................................... 10

      4.2.5  DIGIPASS ............................................................................................................. 11

   4.3  Password Manager Pro ................................................................................................... 13

   4.4  Test the Solution ........................................................................................................... 15
1 Overview

192.168.20.2
Active Directory

192.168.20.3
Password Manager Pro

192.168.20.4
IDENTIKEY Authentication Server

Overview
2 Technical Concepts

2.1 Manage Engine

2.1.1 Password Manager Pro

Password Manager Pro is a secure vault for storing and managing shared sensitive information such as passwords, documents and digital identities of enterprises. It can integrate with your Active Directory systems to ease the management of all your password.

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.
3 Password Manager Pro setup

Before adding 2 factor authentication it is important to validate a standard configuration without One Time Password (OTP).

3.1 Architecture

![Architecture Diagram]

3.2 Prerequisites

- A default installation of Password Manager Pro is required.
- A Demo user with credentials: Demo, Test1234

3.3 Password Manager Pro

Log into Password Manager Pro using the web service (in our example we use the local host).

For the first login use **admin** as both password and username.
Navigate to **Admin, Active Directory**.

Import users from Active Directory:

Click on **Import now** and the following screen will appear:

- **Select Domain Name**: Click **New Domain**
  - Enter: **vdsi.local**
- **Primary Domain Controller**: **192.168.20.2**
- **Select**: **Specify User Name and Password manually**
- **User Name**: **Administrator**
- **Password**: **ADPassword**
- **Select 2 hours**
• Click **Import**

Click **Enable**.

### 3.4 Test the setup

When you are still logged in as “admin”, log out and try a login with one of your users in the Active Directory.

Log in using **Demo** and **Test1234**.

Login was successful.
4 Solution

4.1 Architecture

4.2 IDENTIKEY Authentication Server

There are lots of possibilities when using IDENTIKEY Authentication Server. We can authenticate with:

- Local users (Defined in IDENTIKEY Authentication Server)
- Active Directory (Windows)

In this whitepaper we will use Local users to authenticate.

4.2.1 Policies

In the Policy the behavior of the authentication is defined. It gives all the answers on: I have got a user and a password, what now?

- **Create** a new Policy
• **Policy ID:** **Test**
• **Inherits From:** **Base Policy**

Inherits means: The new policy will have the same behavior as the policy from which he inherits, except when otherwise specified in the new policy.

**Example:**

<table>
<thead>
<tr>
<th></th>
<th>Base Policy</th>
<th>New Policy</th>
<th>Behaviour</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>a</td>
<td></td>
<td>New policy will do a</td>
</tr>
<tr>
<td>2</td>
<td>b</td>
<td></td>
<td>New policy will do b</td>
</tr>
<tr>
<td>3</td>
<td>c f</td>
<td></td>
<td>New policy will do f</td>
</tr>
<tr>
<td>4</td>
<td>d</td>
<td></td>
<td>New policy will do d</td>
</tr>
<tr>
<td>5</td>
<td>e g</td>
<td></td>
<td>New policy will do g</td>
</tr>
</tbody>
</table>

The new policy is created, now we are going to edit it.

• **Click** **edit**

• **Local Authentication:** **Digipass/Password**
• **Click** **Save**

**4.2.2 Client**

In the clients we specify the location from which IDENTIKEY Authentication Server will accept requests and which protocol they use.

We are going to add a new RADIUS client.
• Client Type: select **Radius Client** from **select from list**
• Location: **192.168.20.2**
• Policy ID: Select the Policy that was created in **Policies**
• Protocol ID: **RADIUS**
• Shared Secret: **Test123**
• Confirm Shared Secret: reenter the **shared secret**
• Click **Save**

**4.2.3 Domain**

Navigate to **Organization, Add Domain**.

• Domain name: **VDSI.LOCAL**
• Click **Save**

**4.2.4 User**

We are going to create a user.
• User ID: demo
• Domain: vdsi.local

4.2.5 DIGIPASS

The purpose of using IDENTIKEY Authentication Server, is to be able to log in using One Time Passwords (OTP). To make it possible to use OTP we need to assign a DIGIPASS to the user. The Digipass is a device that generates the OTP's.

• Open the user by clicking on its name
• Select Assigned Digipass

• Click ASSIGN
• Click **Next**

![Assign Digipass](image)

• **Grace period: 0 Days**

Grace period is the period that a user can log in with his static password. The first time the user uses his DIGIPASS the grace period will expire.

• Click **ASSIGN**

![Assigning Digipass](image)

• Click **Finish**
4.3 Password Manager Pro

Go to Password Manager Pro and login as the local administrator \texttt{admin}.

Navigate to \textbf{Admin, RADIUS}.

Click \textbf{Configure}.
• IP address: 192.168.20.2
• Server Authentication Port: 1812
• Server protocol: PAP
• Authentication Retries: 3
• Check: Specify Server Secret Manually
• Server Secret: Test123
• Click Save

Navigate to Admin, Active Directory.

Disable Active Directory authentication.

Navigate to Admin, RADIUS.

Enable RADIUS authentication.
4.4 Test the Solution

To test this login take the DIGIPASS assigned to the demo

Login with username and One Time Password

- Username: `<DOMAIN>\User` (in our example this is `LABS.VASCO.COM\Demo`)
  - The Domain needs to be in capital letters. PMP stores the domain always in capital. This means that you must enter the DOMAIN in capital to pass the first user check of PMP itself. If you do not place it in capital the login will get rejected and not even generate an OTP.
- Password: `OTP` (The demo uses DEMO DIGIPASSes to get these you can find a DEMO DIGIPASS here: `http://demotoken.vasco.com/go3.html`
DIGIPASS Authentication for Password Manager Pro

Password Manager Pro

Auto Logon Explorer

My Favorite Passwords

Your list of favorite passwords is empty. Click the icon against the passwords in the 'My Passwords' view to add them to your list of favorite passwords.
5 Challenge/Response

The easiest way to test challenge/response is to use (Back-Up) Virtual DIGIPASS. Virtual DIGIPASS is a solution where an OTP is sent to your E-mail account or mobile phone, after it was triggered in a user authentication. The trigger mechanism is configured in the policy (see later).

- Virtual DIGIPASS is a DIGIPASS that needs to be ordered like a Hardware DIGIPASS
- Back-Up Virtual DIGIPASS is a feature that must be enabled while ordering other DIGIPASS (Hardware, DIGIPASS for Mobile, DIGIPASS for Web or DIGIPASS for Windows)

Availability of Back-Up virtual DIGIPASS can be checked in the IDENTIKEY web administration.
Select a DIGIPASS > Click on the first application and scroll down.

For test purposes a demo DPX file (named Demo_VDP.DPX) with Virtual Digipass is delivered with every IDENTIKEY Authentication Server

5.1 Architecture

This solution makes use of an SMS-gateway (for SMS or text messages) or SMTP-server (for mail). The first step is to configure one of the servers. This is done in the Message Delivery Component (MDC) configuration. For more information see the IDENTIKEY Authentication Server manuals.
5.2 IDENTIKEY Authentication Server

5.2.1 Policy

The configuration virtual Digipass can be used is done in the policy. Select the policy created in Policies. This should be Test.

Select Test

Go to Virtual Digipass

Click Edit

- Delivery Method: SMS
- BVDP Mode: Yes – Permitted
- Request Method: KeywordOnly
- Request Keyword: IwantOTP

Click Save

The request method is the trigger to send the message. The trigger can be:
- Static password: as stored inside IDENTIKEY Authentication Server (different for each individual user)
- Keyword: a text message (the same for all users)

5.2.2 User

IDENTIKEY Authentication Server needs to know, where to send the mail or SMS. Therefor the User should be added.

Select a user: Demo

Click User Info

Click Edit
• Mobile: +32... (for the sms)
• Email Address: mail@server.com (for mail)

Click **save**

### 5.3 Test the Solution

PMP can support Backup Virtual DIGIPASS as two one step challenge response steps. This translates into logging in with your username and keyword and being rejected.

You will receive a One Time Password and you can log in again with username and password + OTP.

- Username: `<DOMAIN>\User` (in our example this is `LABS.VASCO.COM\Demo`)
  - The Domain needs to be in capital letters. PMP stores the domain always in capital. This means that you must enter the DOMAIN in capital to pass the first user check of PMP itself. If you do not place it in capital the login will get rejected and not even generate an OTP.
- Password: **IwantOTP**
You will get rejected but even so, if the credentials were correct you will receive an OTP.

- Username: `<DOMAIN>\User` (in our example this is LABS.VASCO.COM\Demo)
- Password: `Password + OTP` (in this example: `Test1234xxxxxx`)

You are successful logged in.