Table of Contents

1 Overview........................................................................................................................................... 3
2 Problem Description .......................................................................................................................... 3
3 Solution.............................................................................................................................................. 3
4 Technical Concept............................................................................................................................ 4
  4.1 General overview .......................................................................................................................... 4
  4.2 Overview of Microsoft IAS RADIUS Authentication with VM ...................................................... 6
  4.3 Overview of RADIUS IP and Port Settings .................................................................................. 6
  4.4 Overview of RADIUS IP and Port Settings .................................................................................. 7
5 Configuration of the Microsoft IAS ................................................................................................. 8
  5.1 Installation of the IAS ................................................................................................................... 8
  5.2 IAS Server Configuration ............................................................................................................. 10
  5.3 IAS RADIUS Client configuration ............................................................................................... 12
6 Configuration of VACMAN Middleware........................................................................................ 15
  6.1 Set time and date .......................................................................................................................... 15
  6.2 Configure VACMAN Middleware ................................................................................................. 16
  6.3 Configure RADIUS Proxy .......................................................................................................... 17
  6.4 Configure RADIUS Client .......................................................................................................... 18
  6.5 Import Demo DIGIPASS token secret ......................................................................................... 19
  6.6 Changing PINs ............................................................................................................................ 21
7 Sample logon with VASCO RADIUS Client Simulator .............................................................. 22
  7.1 Dynamic User Registration (DUR) ............................................................................................ 22
8 VACMAN Middleware features ..................................................................................................... 33
  8.1 Installation ................................................................................................................................... 33
  8.2 Deployment ................................................................................................................................ 33
  8.3 Administration ............................................................................................................................. 35
  8.4 Advanced Features ...................................................................................................................... 35
9 Conclusion......................................................................................................................................... 36
10 For more information on Microsoft ............................................................................................. 36
11 For more information on VASCO ................................................................................................. 36
12 About Microsoft............................................................................................................................. 36
13 About VASCO Data Security ....................................................................................................... 37
1 Overview

Vasco Data Security has a long history with delivering strong authentication through our DIGIPASS Family of tokens that delivers the comfort of using One Time Passwords (OTP).

DIGIPASS authentication for Microsoft IAS is the result of the open market approach delivered through VACMAN Middleware technology.

VACMAN Middleware and Microsoft IAS gives the possibility to utilize the strength of the DIGIPASS Token Family concept (One Time Password login as Time Based Response Only or Challenge/Response) into their solid existing technology.

2 Problem Description

Since static passwords are generally known as non-secure and easy to compromise, the challenge was to introduce OTP’s into the remote access market to strongly secure the corporate LAN. Additionally it would be nice to easily track and manage incoming users of the NAS/RAS devices.

The following pages present how to solve these issues via an overview of how to setup an easy configuration.

3 Solution

Microsoft® Windows Internet Authentication Service (IAS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server. IAS performs centralized connection authentication, authorization, and accounting for dial-up and virtual private network (VPN) remote access and for router-to-router connections. It can be used in conjunction with Windows Routing and Remote Access service. IAS enables the use of a single- or multiple-vendor network of remote access or VPN equipment

VASCO’s DIGIPASS enables users to generate One-Time Passwords that safeguard access to e-business and e-banking applications, to corporate networks and allow for more secure transactions. By using DIGIPASS patented technology, you eliminate the weakest link in any security infrastructure; the use of static passwords that are easily stolen, guessed, reused, or shared. It can be deployed as a small hand-held device, as a smart card reader, as software for computers, laptops, PDA’s or cell phones.
4 Technical Concept

4.1 General overview

The concept is very easy: the VACMAN Middleware (VM) is installed as front-end of the Microsoft IAS. This means that the VM will interfere each authentication request on the Microsoft IAS. This One Time Password (OTP) of the authentication request will be verified on the VM. After VM verification, a RADIUS authentication request is asked to the Microsoft IAS for the Authorization and Accounting part.

Two setups are possible:
- VM and Microsoft IAS are running on the same machine
- VM and Microsoft IAS are running on different machines.

The basic architecture is the same for both. The difference is that the RADIUS ports need to be different when VM and Microsoft IAS is installed on the same machine.

Special features as DUR, Passthru makes the VM a very easy deployable authentication server system. (please see further).

VM and Microsoft IAS running on one machine
VM and Microsoft IAS running on two machines
4.2 Overview of Microsoft IAS RADIUS Authentication with VM

The following is a description on the RADIUS authentication sequence WITHOUT DIGIPASS assigned:

- A remote user initiates a (dial-up) connection to the NAS (Network Access Server).
- NAS gathers the remote user’s ID and password, and then submits a RADIUS authentication request to the VM.
- VM performs its verification, and then proxies the request to Microsoft IAS.
- Microsoft IAS performs its verification, and then returns the results.
- VM forwards the Microsoft results to NAS.
- The NAS takes an appropriate action based on returned RADIUS results from Microsoft IAS via VM.

The following is a description on the RADIUS authentication sequence WITH DIGIPASS Assigned:

- A remote user initiates a (dial-up) connection to the NAS (Network Access Server).
- NAS gathers the remote user’s ID and one time password generated by the DIGIPASS, and then submits a RADIUS authentication request to the VM.
- VM performs the OTP verification, and then proxies an authentication request to Microsoft IAS with the static password found in the VM database.
- Microsoft IAS performs its verification and then returns the results.
- VM forwards the Microsoft IAS results to NAS.
- The NAS takes an appropriate action based on returned RADIUS results from Microsoft IAS via VM.

4.3 Overview of RADIUS IP and Port Settings

In most installations, only a few products manage many NAS and firewall RADIUS clients. Therefore, the recommended setup is to change the limited number of VM and Microsoft IAS settings rather than the many RADIUS client settings. The alternate setup is to change those RADIUS clients to point to the VM.

In either case, the RADIUS settings must result in the following relationships as detailed below. Also, see VM Configuration and Microsoft IAS Configuration sections in this document on how to configure these settings.

<table>
<thead>
<tr>
<th>Required RADIUS Setting Relationships</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS and Firewall RADIUS Clients</td>
<td>VM</td>
<td>Microsoft IAS</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address in Server settings &amp; IP address in Client settings</td>
<td></td>
</tr>
<tr>
<td>Port numbers</td>
<td>Port numbers in Server settings</td>
<td></td>
</tr>
<tr>
<td>Shared-Secret</td>
<td>Shared-Secret in Client settings</td>
<td></td>
</tr>
<tr>
<td>IP address in Proxy settings</td>
<td>IP address in Client settings</td>
<td>IP address in Server settings</td>
</tr>
<tr>
<td>Port numbers in Proxy settings</td>
<td>Port number in Server settings</td>
<td></td>
</tr>
<tr>
<td>Shared-Secret in Proxy settings</td>
<td>Shared-Secret in Client settings</td>
<td></td>
</tr>
</tbody>
</table>
4.4 Overview of RADIUS IP and Port Settings

The following diagram shows actual RADIUS settings. This is an installation with VM and Microsoft IAS installed on the same machine. The numbers are examples.

**Network Access Server**

- **NAS IP**: 192.168.10.1
- **Radius settings**:
  - Server IP: 192.168.10.10
  - Auth Port: 1645
  - Acct Port: 1646
  - Secret = vasco

- **VM Server Settings**
  - VM IP: 192.168.10.10
  - Auth Port: 1645
  - Acct Port: 1646

- **VM Client Settings**
  - Client IP: 192.168.10.1
  - Secret = vasco

- **VM Proxy Settings**
  - VM IP: 192.168.10.10
  - Auth Port: 1812
  - Acct Port: 1813

- **IAS Server settings**:
  - IAS IP: 192.168.10.10
  - Radius Port: 1812

- **IAS Client settings**:
  - Client IP: 192.168.10.10
  - Secret = vasco

- **Network Access Server**
5 Configuration of the Microsoft IAS

5.1 Installation of the IAS

IAS (Internet Authentication Service) is a part of Windows 2000. To install it, go to the control panel and click on Add/Remove Software:
Next, select Add/Remove Windows Components and look for Networking Services. Then, click on details:

Select Internet Authentication Services from the list
Insert your W2K CDROM, click “OK”, click next...

Now go on to the next section to configure your IAS

5.2 IAS Server Configuration

First you have to change the policy so the IAS accepts PAP as an authentication method

START -> admin tools -> Internet Authentication Server
The following window will open when starting IAS (see screenshot)

1. Click on REMOTE access policy’s (1)
2. Select your policy and open it’s properties (2)
3. Click on “edit profile” (3)
4. Authentication tab (4)
5. Enable PAP authentication (5)
6. Apply / OK

Remark: Maybe you should change your policies. This is very site specific.
5.3 IAS RADIUS Client configuration

- START -> admin tools -> Internet Authentication Server
- Click on clients and add a new client
- Choose a friendly name
- Click Next

![Add Client Dialogue Box]

Name and Protocol
Assign a name and protocol for the client.

Type a friendly name and protocol for the client.

- Friendly name: VM
- Protocol: RADIUS
- As IP choose the Middleware-server-to-be (this can be the same or different machine)
- Fill in the shared secret between the VACMAN Radius Middleware and your IAS server
- Apply
If you are installing VM and IAS on the same machine, you have to alter the port settings of your IAS server.

START -> admin tools -> Internet Authentication Server
Right-click on "Internet Authentication Service (local)" and open properties

Click on the RADIUS field and change the port settings to something else than the default RADIUS ports.
These ports should be unused UDP port numbers, (in the example: 1647, 1648)
6 Configuration of VACMAN Middleware

6.1 Set time and date

The DIGIPASS token is based on Time Synchronization. All tokens are created with its internal real time clock set to GMT. As such, it is important to set the date, time and time zone of the server running the VACMAN Middleware to correctly so that GMT can be local derived correctly.
6.2 Configure VACMAN Middleware

Start the VACMAN Middleware and select the Admin Console. And set there the following configurations as shown below. The ‘Server IP’ refers to the IP address of the server running the VACMAN Middleware and thus it is set to 192.168.10.10.

Assuming that there is no third party RADIUS Server in this setup, and that the VACMAN Middleware is used to handle authentication only, you can then select the ‘Authenticator’ as ‘Local Server’.

The RADIUS Client is using the RADIUS port for authentication and accounting and thus ‘Incoming RADIUS Authentication Port’ and ‘Incoming RADIUS Accounting Port’ should be set to 1645 (1812) and 1646 (1813) respectively.

To save the VACMAN Middleware setting, click on the ‘Diskette’ button or the ‘File’->‘Save’ menu as shown.
6.3 Configure RADIUS Proxy

Now we will define the proxy settings. We will only define Primary Server. Secondary Server is for backup. In the fields Authentication IP and Accounting IP, you put your local IP in. In this sample is this thus 192.168.1.24. Authentication Port is 1812 and Accounting Port is 1813. Save the settings.
6.4 Configure RADIUS Client

Select the RADIUS Client and set in the configurations as shown below. Click on the ‘New’ button to enter the IP address and shared secret of a new RADIUS Client as shown. The ‘IP Address’ refers to that of the RADIUS Client used in the setup and thus it is set to 192.168.10.1. The ‘Shared Secret’ is set to ‘vasco’. Note that the corresponding shared secret will have to be set at the RADIUS Server configuration within the RADIUS Client Simulator later on. Click on ‘Save’ button to save the configuration.
6.5 Import Demo DIGIPASS token secret

Right click on the ‘Token’ and select ‘Import Tokens’ or click on ‘Import New Tokens’ button as shown below.

Enter the encryption key to decrypt the content of a DPX file.
The DPX file contains secret information relating to the token and thus it is encrypted. In order for VACMAN Middleware to decrypt such DPX file, you will have to enter the key. In order to decrypt a demo DPX file that contains secret information relating to a demo token, the encryption key is 32 digits of ‘1’ as shown above.

Click on the Folder button to select the path for the DPX file. The name for demo DPX file for DIGIPASS Pro 300 token is typically ‘demo.dpx’ while the demo DPX file for DIGIPASS GO 1 is typically ‘demoGO1.dpx’ and it can be found under the VACMAN Middleware program directory.

Select ‘APPL 1’ for onetime password application of either the demo DIGIPASS Pro 300 token or DIGIPASS GO1 token and click the ‘Import’ button as shown.

Upon successful import, a message will be displayed, click on ‘OK’ button. Check the number of ‘Token Application Read’, ‘Token Record Read’ and ‘Token Records Imported’ to ensure that 1 token has been successfully imported into the VACMAN Middleware. Click on the ‘Close’ button after finishing importing the token.
6.6 Changing PINs

The DIGIPASS Pro series of tokens have a small keyboard so a PIN is changed on the physical token. With a DIGIPASS Go-1 and Go-3, a user’s PIN is entered in the password field before the DIGIPASS code (eg. MyPIN896321). A Go-1 or Go-3’s PIN can be alphanumeric (any combination of 0-9, A-Z and a-z) if desired. For simplicity it is still referred to as a PIN. A space cannot be used in the PIN. If you are using Go-1/3’s and you decide to use the DIGIPASS record that has a PIN you obviously must allow the user and/or administrator to change the PIN. There are 2 methods to change the PIN. The user can change a PIN by entering the following in their logon page’s password field.

Password = Existing PIN + One Time Password + New PIN + New PIN

Please note: If any of the supplied information is incorrect the PIN will not be updated. The new PIN must fit the PIN length parameters when the DIGIPASS is programmed.

An administrator can change a PIN via the Administration Interface by going to the Token tab on the left hand side of the administration interface screen. On your right you click on Set PIN. There you write the New PIN and confirm it. Then you click on Set New PIN.
7 Sample logon with VASCO RADIUS Client Simulator

7.1 Dynamic User Registration (DUR)

First we have to create a new user. Therefore we go to administrative tools local user manager. Here we can create users. For creating the user you have to right click and then select 'new user'
Then you have to define the user's name and his password.

Now we have to change his properties so the user is allowed to dial in. This can be done by right clicking on the created user and selecting properties.
In the properties menu we have to go to the 'Dial-in' tab. Here you have to enable the option ‘Allow access’ in the ‘Remote Access Permission field’. 

User is properly created now.
Now we will test the created user with Radius Client Simulator.
The VACMAN RADIUS Client Simulator (RCS) is a program that simulates RADIUS Authentication and Accounting processing in a similar fashion to RADIUS enabled NAS and Firewall devices. The RCS can be used to test user (and static-password) authentication, (DIGIPASS) token password authentication, estimate RADIUS server performance, system overload, and assist in detection of resource (memory, handle, etc.) leakage.

When we open the Radius Client Simulator we have to change some things first. Server IP should be the same IP of the VM. The Auth. Port should be define as 1645 and the Acct. port as 1646. Then you fill the Shared secret in.
Then you click one of the yellow ports, allowing you to enter User ID and password. In the User ID field you enter VascoDemo. (The test user we have created.) In the password field you give the password of the created user in.

Click ‘Login’. Now you will see the prove that the user is successfully logged in.
When the user VascoDemo logged in successfully. He will automatically been added in the VACMAN Middleware. So now you have to open the Admin GUI of the VACMAN Middleware. Then right click on ‘User’ and select ‘Search list’.

In the ‘Token Assign status’ you select ‘Both’ and click on the search button. And now on your left under ‘User’ we see our created user.
Now we have to assign a Demo DIGIPASS token to the demo user.

Right click on the ‘Token’ menu and select ‘Search List…’ as shown.

Select ‘Both’ to search all tokens within VACMAN Middleware and click on ‘Search’ button.
The serial number of the imported token should be displayed under the Token as shown. The ‘0097123456’ refers to the serial number of the demo token that is imported from the DPX file.

Click on the ‘Assign’ button to assign the token to user. In order to search for all users available, click on the ‘Search’ button as shown below.
Select user ‘VascoDemo’ and click on ‘Assign’ button and see that demo token serial ‘0097123456’ has been assigned to user ‘VascoDemo’.
At this stage, the VACMAN Middleware has been successfully installed and configured to communicate with the IAS at IP address 192.168.10.10 and the user ‘VascoDemo’ has been successfully created and assigned with a demo DIGIPASS Pro 300 token.

Now open again the Radius Client Simulator. Then you click one of the yellow ports, allowing you to enter User ID and password. In the User ID field you enter VascoDemo. (The test user we have created.) In the password field you enter the One Time Password (OTP) generated by the 1st application of the DIGIPASS. If you do not have a demo DIGIPASS you can get one by downloading from the VASCO website the DIGIPASS for Windows. This you can find here: http://www.vasco.com/support/download.html?download=23. Install it properly and run it. Go to Internet Banking. In “Authentication” you will find your password. As an alternative you can also go to http://demotoken.vasco.com.
Then click on the ‘Login button’ and you are successfully logged in with the One Time Password.
8 VACMAN Middleware features

8.1 Installation
The VACMAN Middleware (VM) installation is very easy and straightforward. VM runs on Windows platforms, supports a variety of databases and uses an online registration. Different authentication methods allow a seamless integration into existing environments.

Support for Windows 2003 and IIS6
Support for ODBC databases and Active Directory
Any ODBC compliant database can be used instead of the default MS Access Database (MS SQL Server, Oracle). Active Directory can also be used as a repository. This option requires an AD schema update.

Online Licensing
An online licensing mechanism is used to allow automatic delivery of a license file by e-mail.

Authentication Methods
Different authentication methods can be set on server level and on user level: local (VM only), proxy (back-end RADIUS server only), Windows (Windows domain controller only), local and proxy, local and Windows. On top of that Default (server level authenticator will be used) and Disabled (user can not log on) can be used on user level. Using proxy or Windows is also known as pass-through.

8.2 Deployment
Several VACMAN Middleware features exist to facilitate deployment. Combining these features provides different deployment scenarios from manual to fully automatic.

Dynamic User Registration (DUR)
This feature allows VM to check a username and password not in the database with a back-end RADIUS server or a Windows domain controller and, if username and password are valid, to create the username in the VM database.

Autolearn Passwords
Saves administrators time and effort by allowing them to change a user’s password in one location only. If a user tries to log in with a password that does not match the password stored in the VM database, VM can verify it with the back-end RADIUS server or the Windows domain controller and, if correct, store it for future use.
**Stored Password Proxy**
Allows VM to save a user’s RADIUS server password or Windows domain controller password in the database (static password). User’s can then log in with only username and dynamic one-time password (OTP). If this feature is disabled, users must log in with username and static password immediately followed by the OTP.

**Token Self Assign**
Allows users to assign tokens to themselves by providing the serial number of the token, the static password and the OTP.

**Token Auto Assign**
Allows automatic assignment of the first available token to a user on user creation. An e-mail with the serial number of the token and the name of the user can be sent to an administrator.

**Grace Period**
Supplies a user with a certain amount of time (7 days by default) between assignment of a token and the user being required to log in using the OTP. The Grace Period will expire automatically on first successful use of the token.

**Bulk Management**
Allows administrators to quickly administer multiple users and tokens with a single mouse click.

**CSV File Import**
A comma separated file (.csv) can be created containing users, serial numbers of DIGIPASSes and other information. By importing this file into the VACMAN Middleware, the users are created, the DIGIPASSes are assigned and other settings are determined.

User Self Management Web Site - A web site running on IIS has been developed to allow users to register themselves to the VM with their username and back-end (RADIUS or Windows) password, to do a token self assign, to update their back-end password stored in the VM database, to do a change PIN (Go-1/Go-3 token), to do a token test.
8.3 Administration

A highly intuitive graphical user interface (GUI) exists to administer the product. An Audit Console is available to give an instant view on all actions being performed on the VM. Both can be installed on the VM server itself or on a separate PC and require a Java Runtime Environment (JRE) to be installed.

8.4 Advanced Features

Protocol Support - PAP, CHAP, MS-CHAP v1, MS-CHAP v2, MPPE are supported by the VM. This means that PPTP is also supported. Some features of VM are not or only partially supported when using CHAP or MS-CHAP: Windows Authentication, Password Autolearn, Token Self Assign, Change PIN, Stored Password Proxy, Challenge/Response. The User Self Management Web Site can be used to overcome these drawbacks.

Redundancy, Failover and Replication - A Primary and a Backup VM can be installed and a built-in database replication feature assures databases are in sync. This allows for some form of redundancy – failover. The replication process will automatically attempt re-connection until connection is restored. When using the Active Directory option the AD replication can be used instead of the built-in VM database replication. The same is true for ODBC compliant databases (SQL Server, Oracle).
9  Conclusion

Today’s Microsoft IAS solution can be very easily upgraded for using dynamic passwords as user authentication method. Due to the straightforward management tools like DUR, AutoLearn, AutoAssign, Vasco’s VM gives IT-managers the possibility to increase the level of security in a minute. VM supports all Vasco’s DIGIPASS models.

10  For more information on Microsoft

To find your nearest Microsoft partner or to contact Microsoft please go to:

www.microsoft.com

11  For more information on VASCO

To find more information about VASCO please visit www.vasco.com and click on “where to buy” to locate the nearest VASCO partner in your region.

12  About Microsoft

At Microsoft, we’re motivated and inspired every day by how our customers use our software to find creative solutions to business problems, develop breakthrough ideas, and stay connected to what’s most important to them.

We run our business in much the same way, and believe our seven core business units offer the greatest potential to serve our customers in the coming decade. They include:

- **Windows Client**, including the Microsoft® Windows® XP desktop operating system, Windows 2000, and Windows Embedded operating system.

- **Information Worker**, including Microsoft Office, Microsoft Publisher, Microsoft Visio®, Microsoft Project, and other stand-alone desktop applications.

- **Microsoft Business Solutions**, encompassing Great Plains and Navision business process applications, and bCentral™ business services.

- **Server and Tools**, including the Microsoft Windows Server System™ integrated server software, software developer tools, and MSDN®.

- **Mobile and Embedded Devices**, featuring mobile devices including the Windows Powered Pocket PC, the Mobile Explorer microbrowser, and the Windows Powered Smartphone software platform.
**MSN**, including the MSN® network, MSN Internet Access, MSNTV, MSN Hotmail® and other Web-based services.

**Home and Entertainment**, including Microsoft Xbox®, consumer hardware and software, online games, and our TV platform.

We are committed long term to the mission of helping our customers realize their full potential. Just as we constantly update and improve our products, we want to continually evolve our company to be in the best position to accelerate new technologies as they emerge and to better serve our customers.

### 13 About VASCO Data Security

VASCO designs, develops, markets and supports patented Strong User Authentication products for e-Business and e-Commerce.

VASCO’s User Authentication software is carried by the end user on its DIGIPASS products which are small “calculator” hardware devices, or in a software format on mobile phones, other portable devices, and PC’s. At the server side, VASCO’s VACMAN products guarantee that only the designated DIGIPASS user gets access to the application.

VASCO’s target markets are the applications and their several hundred million users that utilize fixed password as security.

VASCO’s time-based system generates a “one-time” password that changes with every use, and is virtually impossible to hack or break.

With over 10 million current users of its DIGIPASS products, VASCO has established itself as a world leader for Strong Authentication with over 250 international financial institutions, approximately 1200 blue-chip corporations, and governments representing more than 60 countries.