

# Digipass Pack for Windows Networks



White Paper



THE AUTHENTICATION COMPANY

## Table of Contents

1	Overview .....	3
2	Problem Description .....	3
3	Solution.....	4
4	Technical Concept .....	5
4.1	Digipass Pack for Windows Networks (DPWN).....	5
4.1.1	Description.....	5
4.1.2	Architecture.....	5
4.1.3	Components .....	6
4.2	Digipass Authentication .....	11
5	Vasco Digipass within the DPWN .....	13
5.1	Digipass Import.....	13
5.2	Managing Vasco Digipass .....	15
5.2.1	Assigning Digipass .....	15
5.2.2	Unlocking Digipass.....	16
5.2.3	PIN/password assignment.....	17
5.3	Example logon .....	18
6	Features .....	19
6.1	Self enrolment.....	19
6.2	Passphrase .....	20
6.3	Role-based Management .....	24
7	Supported architectures.....	25
8	Conclusion .....	25
9	Other Resources .....	25
10	Information on VASCO products .....	25
11	Information on Protocom products .....	26
12	About VASCO Data Security .....	26

# 1 Overview

The threat for Digital networks became so critical that Vasco and Protocom joined forces to create a total security solution: **Digipass Pack for Windows Networks**.

This document will help the reader to understand the concepts of securing a Microsoft Windows® based network logon with VASCO Digipass, both for on-line use (when connected to the LAN) as for off-line use. It will offer the technical reader a better idea on how to position the Digipass Pack for Windows Networks.

## 2 Problem Description

If you rely on static password protection, you may be surprised at the risks you take everyday:

- Users tend to recycle passwords, create simple ones that they can remember easily, base them on known words or personal data, all of which make them easy to crack
- Users record their passwords somewhere accessible
- Users share their account, making identity management even more difficult
- Some programs capture keystrokes or carry out `brute force attacks` using dictionaries of potential password combinations.

Today's business is built around information applications. To ensure business workflow, productivity and enhancing client relationships, internal network resources are increasingly been made accessible from anywhere.

The weakest link in any security infrastructure, especially in a network environment is the use of static passwords. These passwords are easily stolen, guessed, reused or shared.

The future of network security resides in Strong Authentication devices that prevent credentials from being broadcasted or written down. They ensure that network access is dependent on something stored away from the network (Digipass) as much as on something stored within the network authentication service (user credentials and device specific keys). That is a defense in-depth combination that places bulletproof barrier between your data and potential intruders.

### 3 Solution

With Digipass Pack for Windows Networks (DPWN), the future of network security is already here. Software and hardware have been brought together to create a total security solution.

DPWN protects Microsoft Windows® Server and Client logon, offers a secure solution for terminal server logons, Citrix® and many other architectures where the Microsoft GINA© logon process is involved, thanks to VASCO Digipass patented technology.

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. DIGIPASS patented technology can be deployed as a small hand-held device, as a smart card reader, as software for computers, laptops, PDA's or cell phones.

As a result, users will not use static passwords anymore, but will use a Vasco Digipass turning any single logon into a highly secured process.

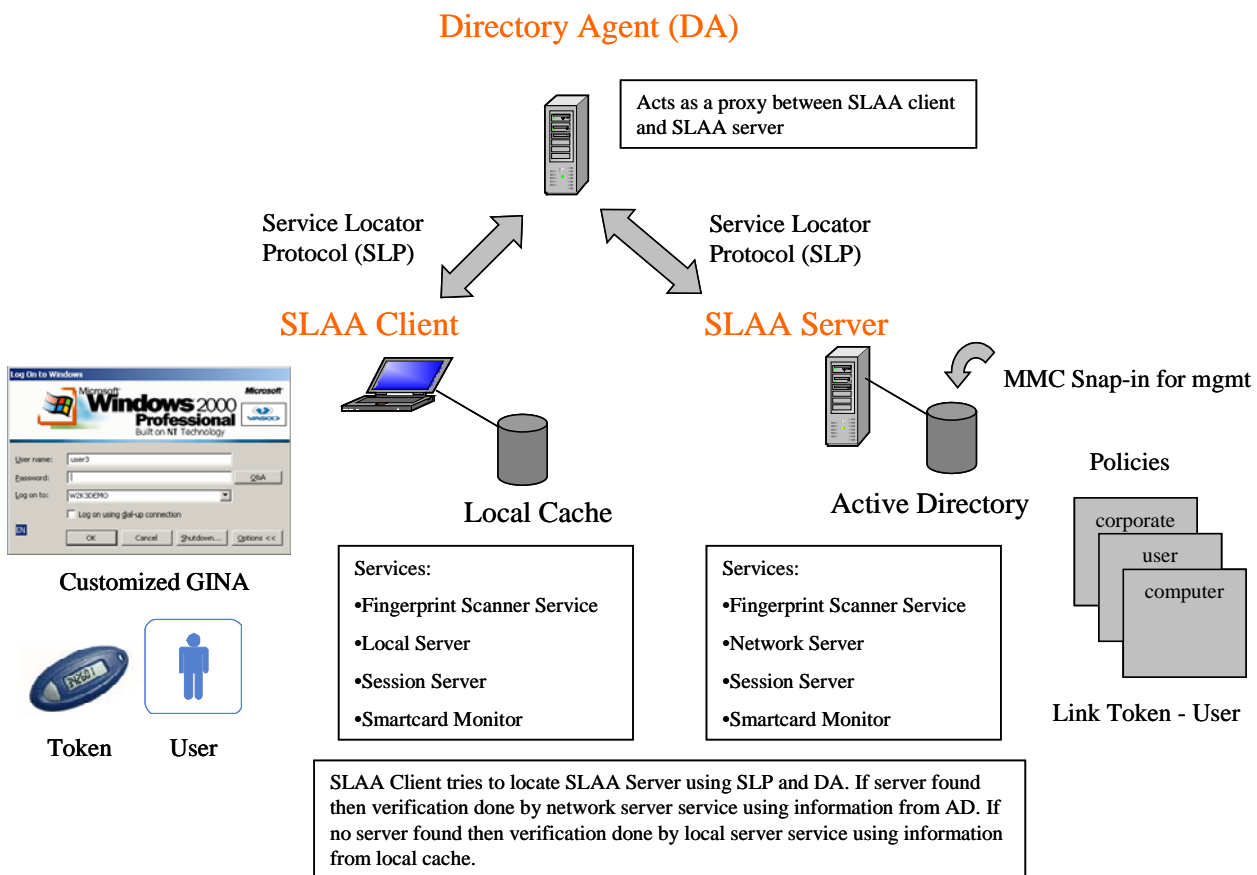
# 4 Technical Concept

## 4.1 Digipass Pack for Windows Networks (DPWN)

### 4.1.1 Description

The DPWN enforces Digipass two-factor authentication for the users accessing their workstation, both when connected to the office network, and disconnected, when using their laptop off-line. All required information such as policies; user information, Digipass information etc. are stored inside Active Directory, your central repository –maintaining one single source of information.

### 4.1.2 Architecture



## 4.1.3 Components

### 4.1.3.1 Active Directory

Digipass Pack for Windows Networks plugs into your existing Active Directory® schema. It does not interfere with your existing directory attributes, and does not change your existing profiles. The directory information and functionality you had before you installed DPWN remain the same.

DPWN does create new attributes in your directory, which are used only by DPWN and safely stored. Most of these new attributes are the DPWN policy settings, which control how a user is authenticated to your network; the others are used to control access to DPWN policy settings.

### 4.1.3.2 Users

Whenever you see the term *user* in this or any of the other DPWN guides, it indicates a user in the Microsoft® Active Directory. A user is tied to the *username*, which is used to logon to the computer.

You can set DPWN permissions for users at any level of your directory, except for the group level. For example, you could set DPWN permissions for some users at organizational unit (OU) level. Similarly, you could set permissions for other users at the individual user (object) level.

You can set or change DPWN permissions for any user, at any time. You only need to have DPWN client installed on that particular machine where the user needs to use DPWN security.

### 4.1.3.3 Policies

Policies allow a company to restrict and streamline the role and permissions of a user or device. Policies represent in a certain way the security level of a company's network administration. Allowing users to choose themselves the composition of their password offers more risks for hacking, results in more administration and is not an example of centralized management.

Setting up the policies will be the first step to start deploying your DPWN. Three policies are available:

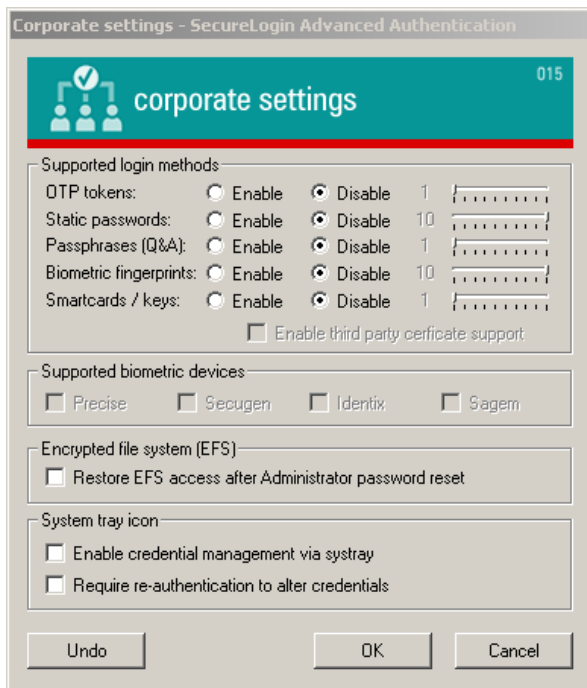
- Corporate
- Computer
- User

The scope of any will be reviewed in detail in the following sections.

## Corporate policy settings

DPWN Corporate policy settings can be implemented at the domain, organization, and organizational unit or user level.

Subordinate objects within your directory structure inherit policy settings applied at any level. However, policy settings applied to a subordinate object override inherited policy settings!

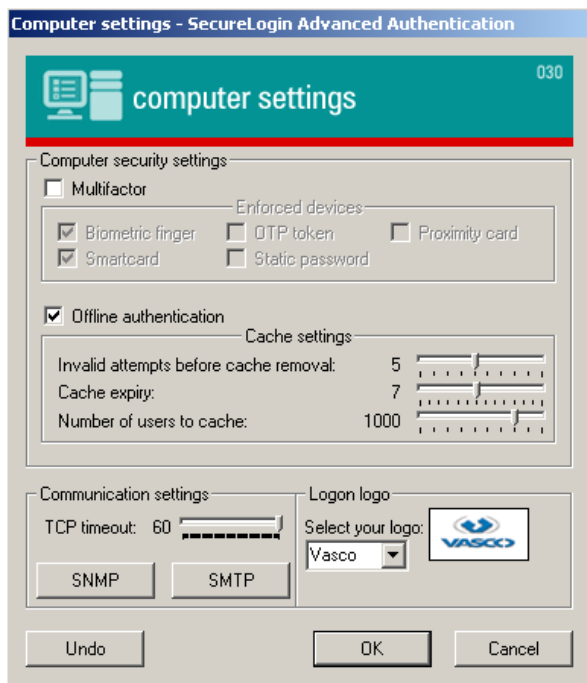


Through the corporate policy the DPWN administrator can choose to enable or disable specific authentication methods.

## Computer policy settings

You can apply a variety of policies to a computer or group of computers, rather than to users. Computer policies will take effect on the nominated computer, irrespective of which user is logged into the machine.

Before you apply a computer policy, you must ensure that the relevant computers are included as computer objects in your directory structure.



Through the computer policy the DPWN administrator can choose to enable or disable specific authentication methods. Additionally the DPWN administrator can allow 'Offline authentication'.

## User policy settings

User policies will allow to select and configure one or more authentication method for a selected user (or group) and also to setup other parameters such as self-enrolment, platform password support etc.

User policies are tied to Active Directory users, regardless the machine they will use to log on the Network.

The screenshot shows a dialog box titled "User settings - SecureLogin Advanced Authentication". The main area is titled "user settings" with a user icon and the number "010". The settings are as follows:

Authentication Method	Allow	Auto self enroll	Action
Passphrase (Q&A)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Policy
Vasco / OTP token	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Policy
Smartcard / smartkey	<input type="checkbox"/>	<input type="checkbox"/>	Policy
Biometric fingerprint	<input type="checkbox"/>	<input type="checkbox"/>	Policy
Biometric facial	<input type="checkbox"/>	<input type="checkbox"/>	Policy
Static password	<input type="checkbox"/>	<input type="checkbox"/>	Policy
Proximity card	<input type="checkbox"/>	<input type="checkbox"/>	Policy
Multifactor authentication	<input type="checkbox"/>	<input type="checkbox"/>	Settings

Below these settings, there is a "Platform password" section with a checked "Allow" checkbox and a "Grace days" slider set to 0. A "Screen unlock security" section has a "Maximum unlock attempts" slider set to 5. At the bottom are "Reset", "OK", and "Cancel" buttons.

#### 4.1.3.4 Authentication methods

The Digipass Pack for Windows Networks allows you to choose from a number of authentication methods:

- Static Password Authentication
- Digipass One Time Password authentication
- Passphrase (Question & Answer).

Especially Passphrases (Questions & Answers) have proven to be extremely effective in reducing the helpdesk calls related to password issues (forgotten passwords etc.).

Digipass One Time Password and Passphrase are explained further in this White Paper.

#### 4.1.3.5 Offline Clients

When working in online mode, when the machine is connected to the Local Area Network (LAN), the local machine connects to the server and downloads the credentials cache from the server at user logon and keeps it updated at any further logon.

Users do not access the local credentials cache if they are working online and authenticating themselves to the network.

When the user is working offline, the DPWN authentication process will use the local cache and will update the user's data at the next online authentication.

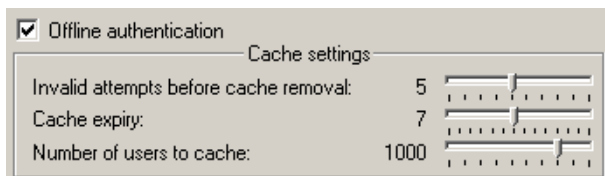
If the invalid logon attempts threshold is reached while the computer is not online, the DPWN erases the local authentication cache, making impossible any further logon attempt until it is reconnected (and successfully authenticated) to the network, then the new cache is downloaded.

If some of your users travel a lot or work from home with laptops, they still can use their regular environment without any security compromise, you just have to select and activate the Off Line Authentication support from the computer policy setting screen.

The Offline Authentication support mainly resides in a local cache of the SAM database, following the domain login genuine implementation.

You can specify the expiry, number of users to cache and invalid attempts detection.

This will ensure that your users will use the same authentication method and process as usual.



## 4.2 Digipass Authentication

Digipass products are handheld devices designed to perform two basic security functions:

- Calculate dynamic passwords, or One-Time Passwords (OTP), to provide positive authentication of a user on a remote system
- Calculate electronic signatures, or Message Authentication Codes (MAC), to protect electronic transactions and guarantee the integrity of their contents.

Digipass products calculate these OTPs and MACs based upon the publicly available Data Encryption Standard (DES) algorithm. The DES algorithm is the industry's leading encryption technology, accepted by security experts worldwide. Digipass products also support the Triple DES (3DES) algorithm and the Advanced Encryption Standard (AES), to provide an even higher level of security when required.

In general, "Strong Authentication" security can be based on three factors:

1. What you **have** (a token such as the Digipass device)
2. What you **know** (a PIN code, required to activate the Digipass)
3. Who you **are** (biometrics, voice, retina scan, fingerprint, etc.)

For most users, the third option is impractical, because the biometrics industry is still in its infancy stage, and biometric products tend to be extremely expensive. That's why the Digipass Family is based on the first two security options.

VASCO's Digipass GO1, GO3 and PRO 300 are best suited for corporate local and remote access. Most of them require a single action to retrieve the OTP. The management of Digipass is user friendly and cost-effective hence it reduces the high administration cost and overhead related to static password management.



**Digipass GO 1**




**Digipass GO 3**



**Digipass PRO 300**

When a user turns on his Vasco Digipass, it displays a One-Time Password on the token's LCD. This One-Time Password is based on time, the Vasco Digipass unique key and a combination of algorithms. When you configure the policy settings for the Vasco Digipass, you import a copy of that unique key into DPWN.



Digipass unique information is stored in a secure (encrypted) file created during the programming of the Vasco Digipass called a DPX file. This DPX file contains unique information of each of the Vasco Digipass supplied in a batch together or separate with the Digipass. In order to open that DPX file you need to supply the associated transport key that will be used to decrypt the database file.

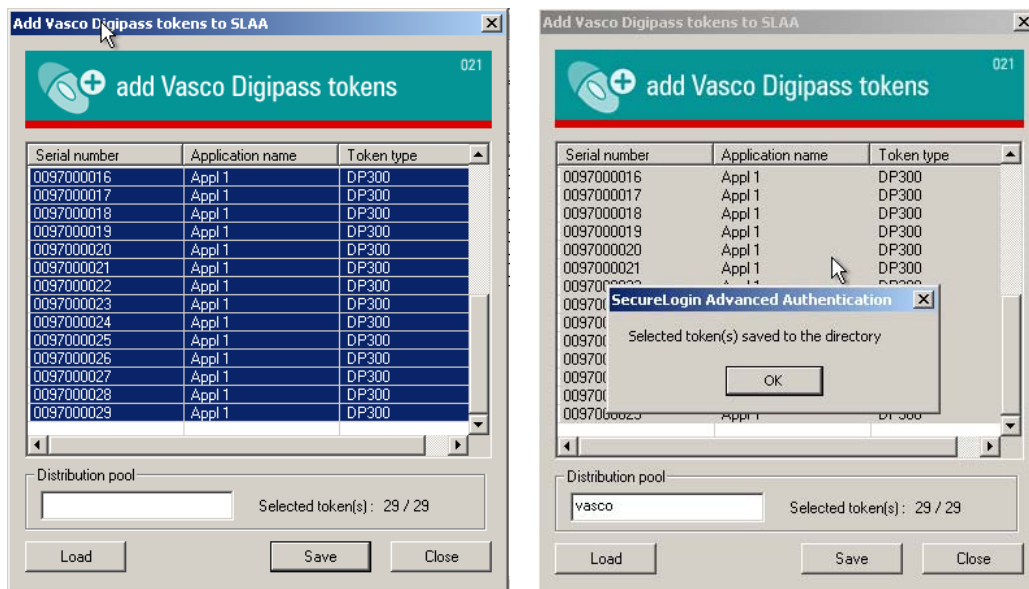
If the DPWN is installed on a network client, then the DPX import is performed via the policy configuration process, if the DPWN is installed on a standalone client, the .dpx file import may be done at enrolment.

Vasco Digipass One-Time Password generation uses time as input, the system running the authentication needs to have the correct relevant time. This DPWN will calculate the password, based on information (loaded .dpx) of a specific Vasco Digipass, and will verify a match between the presented password and its own calculated password.

## 5 Vasco Digipass within the DPWN

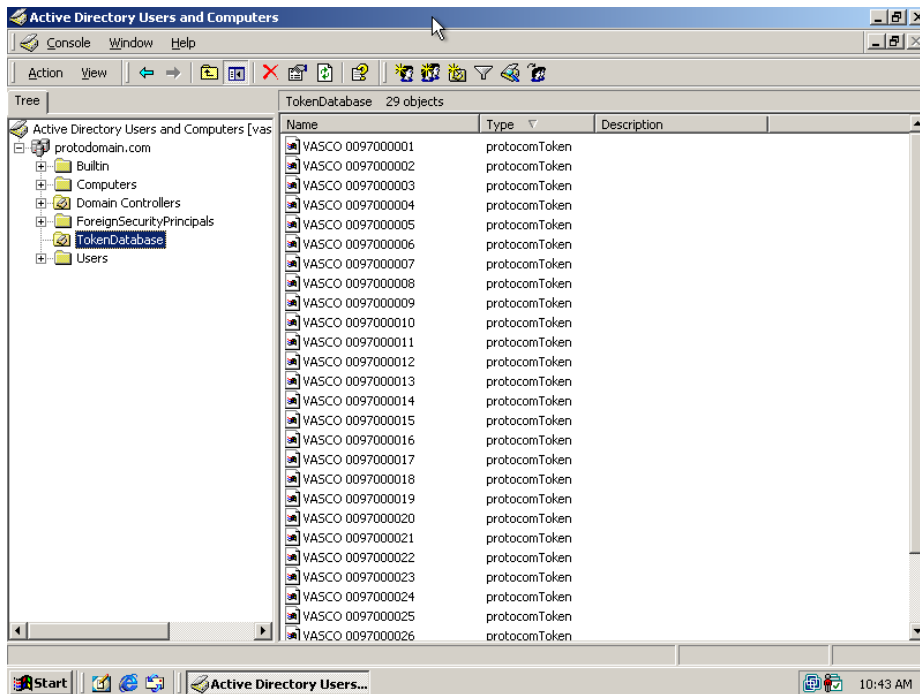
### 5.1 Digipass Import

Once Vasco Digipass secrets (in the DPX) are imported, the related information is stored in the 'TokenDatabase' container in Active Directory (automatically created). Each Vasco Digipass lists its unique serial number in the object name.



DPWN will access the Vasco Digipass information in the directory to authenticate the user; each time the user logs on with their Vasco Digipass and updates it.

DPWN manages the 'VascoDigipass' within pools. A pool name will allow an administrator to group Digipass. This feature is very useful when Digipass management needs to follow the structure of the company.

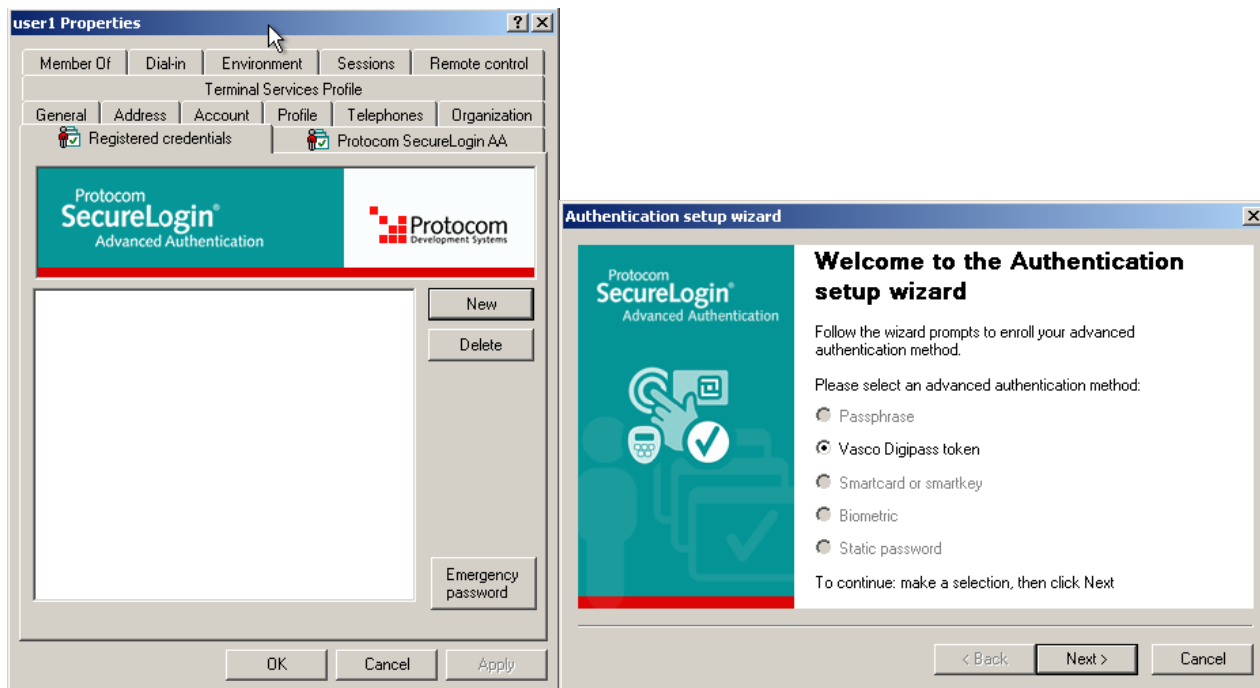


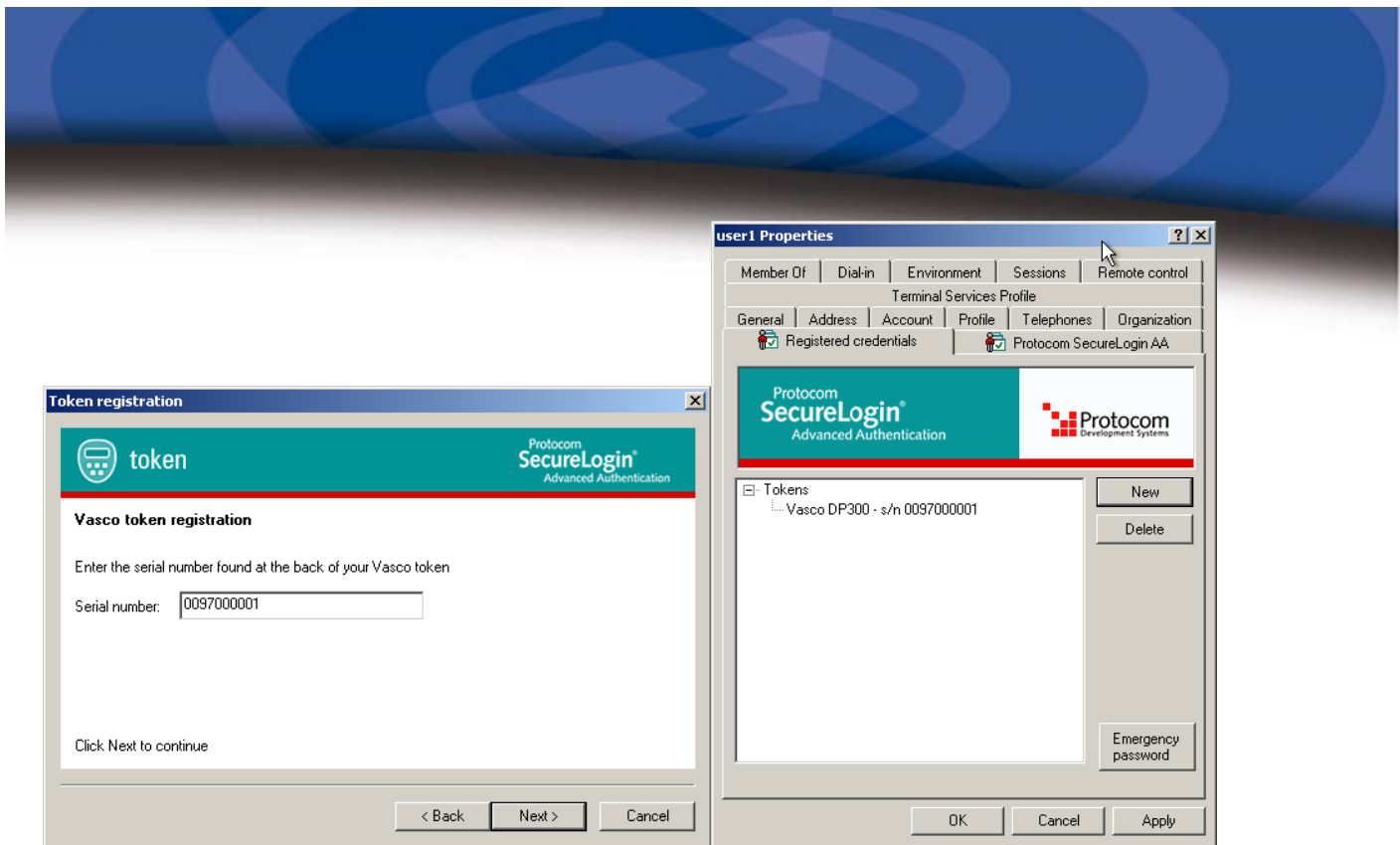
## 5.2 Managing Vasco Digipass

### 5.2.1 Assigning Digipass

Once the DPX file is loaded, the system will present you all available Digipass. At this point you get the possibility to assign a Digipass to a user.

With a simple wizard, assigning a Digipass becomes a 1-minute task.

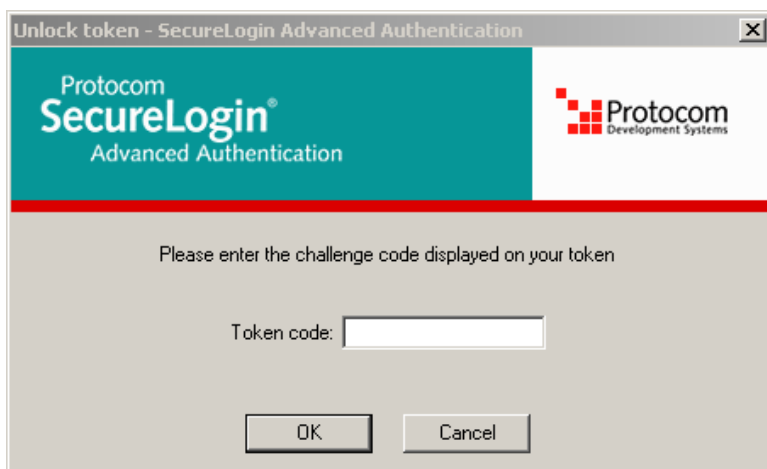




## 5.2.2 Unlocking Digipass

After several unsuccessful PIN entries, the Digipass classic behaviour is to lock itself to protect against brute force attacks.

When locked the Digipass offers a `Unlock Challenge`. The administrator of the DPWN system must enter this challenge into the `Digipass unlock` wizard. The wizard will generate an `Unlock Code` that will let the user choose a new PIN code and re-enable the Digipass.



## 5.2.3 PIN/password assignment

Certain models of Digipass do not have a keypad; Digipass GO1 and GO3 are typical examples. At first sight it seems that the Digipass is not PIN protected but they are. At user logon, the user needs to type a PIN concatenated with the One Time Password generated by the Digipass. The initial PIN for this Digipass should have been hand over to the Digipass owner. Later on you will see that the owner can change the PIN as he wishes.

With the PIN/password policy, you can manage and configure this PIN protection.

The screenshot shows a configuration window titled "PIN policy - SecureLogin Advanced Authentication". The window has a teal header with a user icon and the text "PIN/password policy" and "013". The main area is divided into three sections: "General policy", "Auto self enrollment", and "Advanced options".

**General policy:**

- Minimum uppercase characters: 0
- Minimum lowercase characters: 0
- Minimum numeric characters: 0
- Minimum special characters: 0
- Minimum length: 4

**Auto self enrollment:**

- Enforce
- Grace days: 0
- Grace logins:

**Advanced options:**

- Password history depth: 0
- Password expiry: 0
- Weak password detection:  Off  Basic  Advanced

At the bottom, there are three buttons: "Undo", "OK", and "Cancel".

## 5.3 Example logon

The users enter their Digipass One Time Password, combined with the static PIN in the password field of the logon screen.



The workstation can be unlocked by entering the Digipass One Time Password in the password field.



## 6 Features

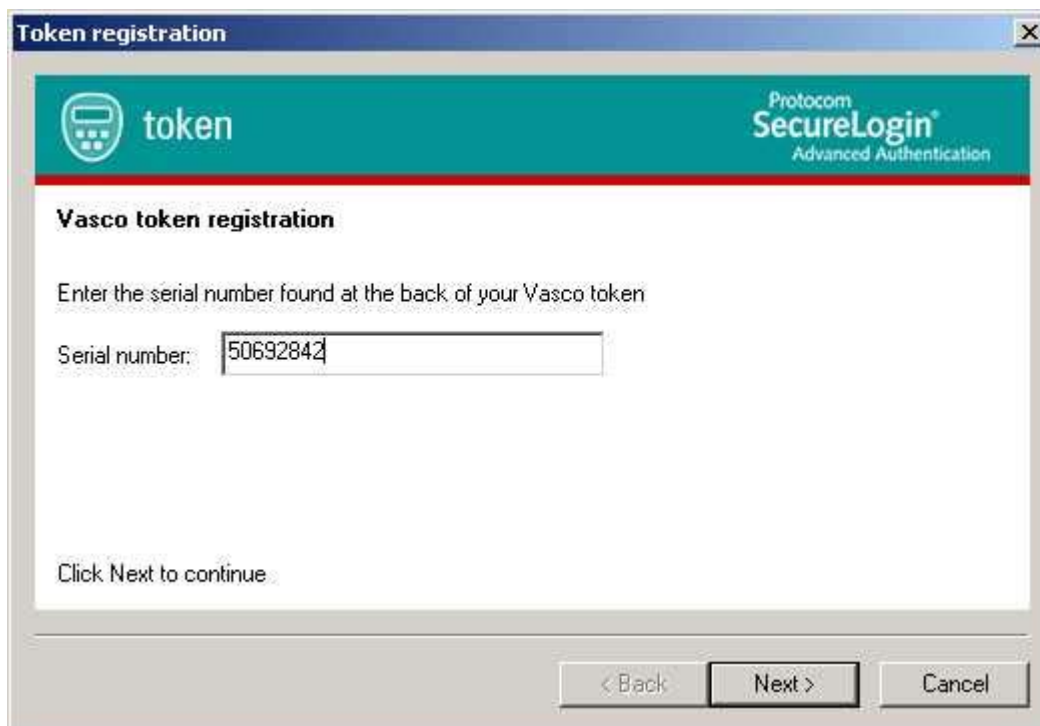
### 6.1 Self enrolment

Selecting the 'Auto Self Enrolment' function means DPWN will prompt the user to enroll his Digipass at his next logon. The user must enroll his Digipass within either the grace period or grace logon period set by the administrator.

This method is very useful when a lot of Digipass need to be distributed and the administrator does not want to handle this logistic challenge. Each user will need to register his own Digipass and the administrator will be informed about this registration.

'Auto Self Enrolment' can be set up and disabled anytime the administrator wants. It is just a matter of selecting or deselecting the check box.

During the Auto Self Enrolment process for the Digipass token, the user is prompted to enter the serial number of his/her Digipass after they have logged on with their existing username and static password.



The screenshot shows a 'Token registration' dialog box with a blue title bar and a close button. The main area has a teal header with a 'token' icon and 'Protocom SecureLogin Advanced Authentication' text. Below the header, the text reads 'Vasco token registration' and 'Enter the serial number found at the back of your Vasco token'. A text input field labeled 'Serial number:' contains the value '50692842'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The text 'Click Next to continue' is visible at the bottom left of the main content area.

Next the user is prompted to enter a valid Digipass One Time Password to confirm they have the right Digipass.

## 6.2 Passphrase

A pass phrase is a series of questions and answers. The user sees the questions appear on the screen and must enter the correct answer. The next question then appears and the user answers that question as well. This process continues until the number of answers required for authentication is reached.

Within a Vasco Digipass infrastructure, pass phrases are used as substitution for Digipass authentication. This option will also be configured in the policy settings.

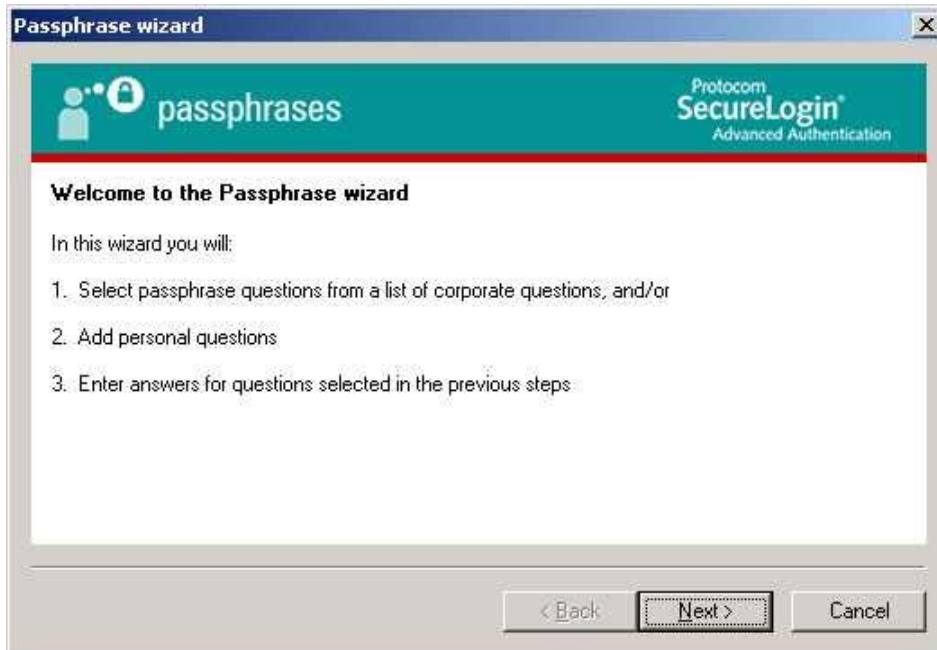
When user forgets his Digipass at home, the DPWN has a built-in solution, allowing the users to logon without the Digipass for a short period.

At logon, the pass phrase option will get active and the user will need to answer a number of questions specified on this screen. This applies to both network and standalone clients.

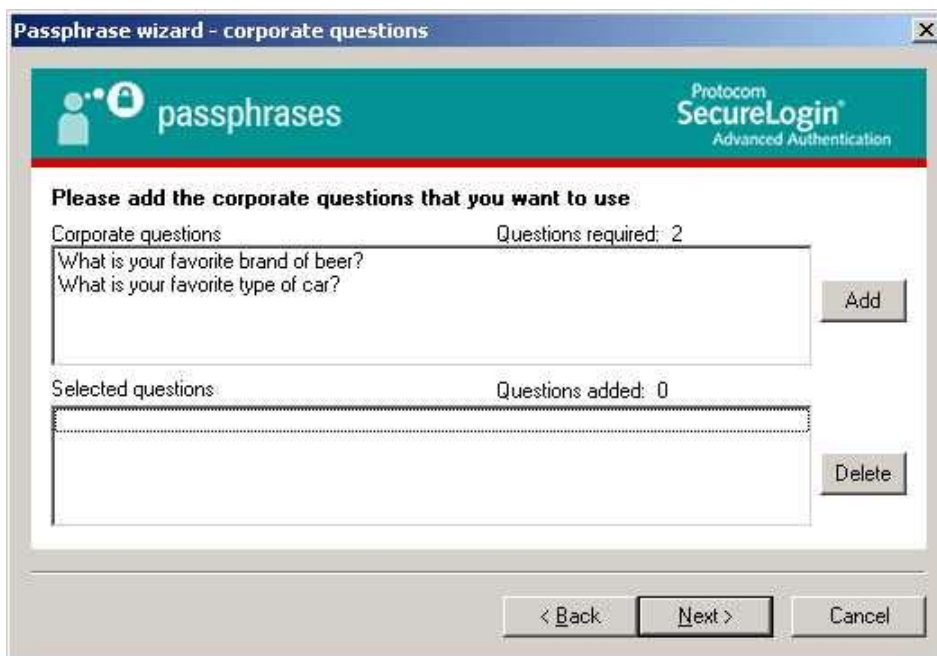
In general, pass phrases are less secure than Vasco Digipass authentication, but are more secure than simple password authentication. The idea here is that user has to enter in a certain way multiple passwords.

As already mentioned, pass phrases can be defined by the administrator, or by the user, making an exception for using pass phrases for a specific user is possible. The DPWN administration guide will offer more details on this.

When Auto Self Enrolment is enabled for a user, the user will be prompted to register the passphrases at the next logon.



The user must select which corporate questions he/she would like to use for the Q&A.



In this configuration the user must at least select 2 questions from the list of corporate questions.

Passphrase wizard - corporate questions

passphrases Protocom SecureLogin Advanced Authentication

Please add the corporate questions that you want to use

Corporate questions Questions required: 2

Add

Selected questions Questions added: 2

What is your favorite brand of beer?  
What is your favorite type of car?

Delete

< Back Next > Cancel

Next the user must provide the answers to the selected questions.

Passphrase wizard - answers

passphrases Protocom SecureLogin Advanced Authentication

Please enter an answer for the question below

Question: Questions answered: 0/3

What is your favorite brand of beer?

Answer:  Display answer

xxxxxx

Confirm answer:

xxxxxx

< Back Next > Cancel

Once all questions are answered, the Passphrase authentication method is fully operational and can be used by the user as a backup authentication method.



When clicking the Q&A button in the logon screen, the user is prompted which 'authentication method' he/she wants to substitute using the Q&A.



Next the user must provide the correct answers to the previously selected questions. If all minimum required questions are answered correctly, the user is granted access.



## 6.3 Role-based Management

DPWN configuration and management is based on specific users, groups and their related system attributes.

DPWN automatically assigns different access rights to different groups. It creates these groups in your directory during the installation on the server.

Installing the DPWN on your server or client has no effect on the existing administrator group in your directory; the new 'SecureLoginAA administrator group', does not inherit your existing administrator groups rights for example.

The 'SecureLoginAA administrator' group rights allows to configure DPWN user policy settings only.

A built-in security protection to DPWN separates 'Configuration manager' and 'administrator' roles. Security best practices recommend to assign different functions to different groups, so that one group acts as a check or constraint on the other, and *vice versa*.

This role-based separation is similar to the 'administrator' and 'security officer' separation you see in many Windows based applications.

Separating the configuration manager's role from the administrator's role allows you to centralize control of DPWN, through the configuration manager without compromising your existing hierarchical rights. You can then assign responsibility for managing and enrolling users to other people throughout your organization by adding them to the 'SecureLoginAA administrator' group.

## 7 Supported architectures

DPWN leverages current network architectures. Scalability is only limited by your current system architecture.

Architectures supported:

- ❑ Microsoft Active Directory
- ❑ Microsoft Windows Terminal server
- ❑ Citrix Metaframe

Os versions supported:

- ❑ Windows 2000 Server
- ❑ Windows 2000 Advanced Server
- ❑ Windows 2000 Professional
- ❑ Windows XP Professional
- ❑ Windows 2003 Server

## 8 Conclusion

Companies tired of searching for complex password policies to secure domain logons do not have to worry about this anymore because the Digipass Pack for Windows Networks solves all this. Making the end user life difficult searching for complex passwords, helpdesk calls for password resets, calculations of monthly costs of password management will be reduced with at least 50 percent when users, administrators, guests, backup operators, ... can logon with a Vasco Digipass managed by the Digipass Pack for Windows Networks. Vasco not only offers a solution that reduces time and the cost associated, but also safeguards the users identity and the company's identity.

## 9 Other Resources

Detailed information is available on the specific VASCO mini site for Digipass Pack for Windows Networks at this location : <http://www.vasco.com/dpwn>

For more information please send an e-mail to [dpwn@vasco.com](mailto:dpwn@vasco.com) or your local Vasco contact.

## 10 Information on VASCO products

To find more information about VASCO please visit [www.vasco.com](http://www.vasco.com) and click on "where to buy" to locate the nearest VASCO partner in your region.

## 11 Information on Protocom products

Vasco joined forces with Protocom in order to develop the Digipass Pack for Windows Networks. Protocom's Secure Logon Advanced Authentication solution and Vasco's Strong Digipass Authentication solution are two security solutions that offer infrastructure and Strong Authentication. These joined forces resulted in the `Digipass Pack for Windows Networks`

Protocom SecureLogin Advanced Authentication (SLAA) is a network authentication product suite that replaces simple password controls with stronger authentication using devices such as Vasco Digipass tokens.

SLAA is a hardware agnostic infrastructure. Protocom has developed strong partnerships with Vasco Data Security so that they can provide you with a choice in how you want to authenticate users to your network.

Protocom aims to support more devices, as and when they are released on the market. With SLAA, Protocom aims to allow their customers to purchase the latest device technology and implement the security solution that best fits their risk profile.

For more information about Protocom please visit their web site at <http://www.protocom.com>

## 12 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 11 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.