DIGIPASS for Windows

Adding strong authentication when hardware or mobile authentication devices cannot be deployed

For companies which have a need for strong authentication but where hardware based devices or mobile phones cannot be used as authentication device and where transparent deployment to end-users is required.

DIGIPASS for Windows has been designed for companies which have a need to add strong authentication to secure their networks and applications but where it is not possible to use hardware based devices or mobile phones as authentication device.

DIGIPASS for Windows is ideally suited for securing remote access or online applications. Application providers, e-gaming platforms and SaaS-vendors often want to increase the security of their applications without impacting the end-user. DIGIPASS for Windows can easily be deployed to vast numbers of end-users, especially in environments where the ease of implementation is the major requirement. DIGIPASS for Windows has a silent install option which allows pushing the customized authentication application to the end-user without having to ask the end-user to set up the application.

Strong authentication, using DIGIPASS for Windows, can be used with virtually any application in a Windows environment. DIGIPASS for Windows is multi-purpose: adding strong authentication to VPN for remote access and any web-based application and adding electronic signature to online transactions.

HOW DOES IT WORK?
DIGIPASS for Windows is very straightforward in use. The application resides on the end-user's desktop and a one-time password (OTP) will be generated after PIN-code insertion. For an electronic signature, the PIN-code will be requested, after which transaction data will need to be entered into the data fields. The e-signature will be calculated using the data field entries. DIGIPASS for Windows also provides the possibility to open the protected web application directly from the DIGIPASS for Windows application. Once your OTP has been generated you can click next to immediately access the application.

DIGIPASS for Windows operates with VACMAN Controller, IDENTIKEY and aXsGUARD Identifier, the full range of VASCO server-side authentication platforms and can be used in conjunction with any other device from the DIGIPASS family.

FULLY CUSTOMIZABLE
The authentication interface the end-user will see can fully be customized. Menus, messages, corporate colors, logos, fonts can be adapted to reflect the company's corporate image. The customer will be able to fully customize the look-and-feel himself thanks to the customization tool provided by VASCO.

Customization options:
- Customizable GUI (menus, messages, logos, colors)
- Operating modes (user authentication and/or e-signature) can be adjusted to best fit the customer's requirements
- Menus can be extended to immediately link to predefined applications
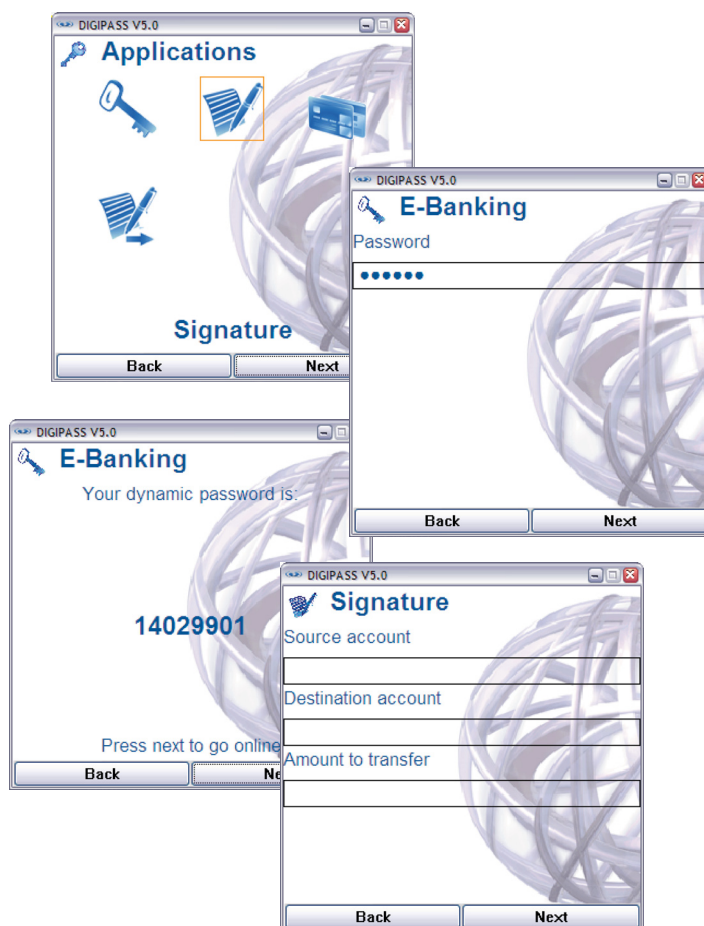
TRANSPARENT DEPLOYMENT TO END-USERS & EASE OF MANAGEMENT

DIGIPASS for Windows is the ideal solution for companies which consider the transparent deployment to the end-user as the major hurdle for adding two-factor authentication to their environment and/or applications. The silent install option of DIGIPASS for Windows pushes the authentication application to the end-users laptop thus avoiding an installation process to be executed by the end-user.

Furthermore DIGIPASS for Windows allows to directly open the protected web application from the DIGIPASS for Windows application, thus making the authentication process part of the access to the application and thus avoiding that authentication is considered as a burden to the end-user. This functionality is available to all applications which use a a web frontal. It does not require any server integration, DIGIPASS for Windows simply takes over the browser behavior when launching the application.

DIGIPASS for Windows has an unlock and re-activate function, allowing end-user to re-activate their DIGIPASS, thus reducing helpdesk and support costs.

SOFTWARE DEVELOPMENT KIT

DIGIPASS for Windows is also available as an SDK for integrators. It allows them to natively integrate DIGIPASS behavior into virtually any Windows application. DIGIPASS strong authentication thus becomes part of the application or VPN client.

AUTO-UPDATE

DIGIPASS for Windows has an auto-update function thanks to which updates are automatically executed in the application. Thanks to the auto-update functionality, DIGIPASS for Windows does not require any deployments when upgrading to a new version, thus facilitating product life-cycle management.

SINGLE LICENSE SYSTEM

DIGIPASS for Windows uses the same licence system as the other software-based DIGIPASS solutions (DIGIPASS for Mobile, DIGIPASS SDK, DIGIPASS for Web). The end-user can for instance use DIGIPASS for Windows to log-on to the VPN and use DIGPASS for Mobile to log on a web application. All software based DIGIPASS use the same license model to facilitate IT administration. All software based DIGIPASS require a single activitation independently from which DIGIPASS software is used.

TIME SYNCHRONIZATION

DIGIPASS for Windows provides time synchronization and daylight saving time. As a result, frequent travellers can effortlessly access their confidential data using VASCO authentication while traveling anywhere in the world.

About VASCO

VASCO designs, develops, markets, and supports patented DIGIPASS®, DIGIPASS PLUS®, VACMAN®, IDENTIKEY® and aXs GUARD® authentication products for the financial world, remote access, e-business, and e-commerce. With tens of millions of products sold, VASCO has established itself as the world leader in Strong User Authentication for e-Banking and Enterprise Security for blue-chip corporations and governments worldwide.

www.vasco.com

BRUSSELS (Europe)
phone: +32.2.609.97.00
email: info-europe@vasco.com

BOSTON (North America)
phone: +1.508.366.3400
email: info-usa@vasco.com

SYDNEY (Pacific)
phone: +61.2.8061.3700
email: info-australia@vasco.com

SINGAPORE (Asia)
phone: +65.6323.0906
email: info-asia@vasco.com