VASCO
THE AUTHENTICATION COMPANY

IDENTIKEY

DIGIPASS Authentication for Windows Logon

DIGIPASS Authentication for Windows Logon, an extension to IDENTIKEY Server 3.1., is a cost-effective solution for enterprises wanting to protect their Windows PCs connected to the corporate network against unauthorised access.

The traditional use of static passwords for logon is considered very unsafe. Not only for remote access over the Internet, but also for the local connection to the corporate network in the office. By replacing static passwords with VASCO's strong authentication, companies can uplift their level of security.

DIGIPASS® Authentication for Windows Logon offers companies of all size a cost-effective way of protecting their Windows PCs - connected to the corporate network - against unauthorised access. Even when laptops are not connected to the LAN, they remain secure, increasing the security of stored data in case they go missing or get stolen.

'DIGIPASS Authentication for Windows Logon' is an extension to IDENTIKEY® Server 3.1. It allows users to logon to their Windows desktop on the network via a DIGIPASS-generated one-time password (OTP).

HOW DOES IT WORK?

'DIGIPASS Authentication for Windows Logon' is installed as a small software module on the end-user's Windows environment. It can be installed on desktop PCs and laptops that are connected to the corporate network. As soon as 'DIGIPASS Authentication for Windows Logon' is setup, it replaces the original login window by a version that will send the login credentials to IDENTIKEY Server for verification. When the authentication request is positively validated, the original static password is sent back to the desktop and used for domain login.

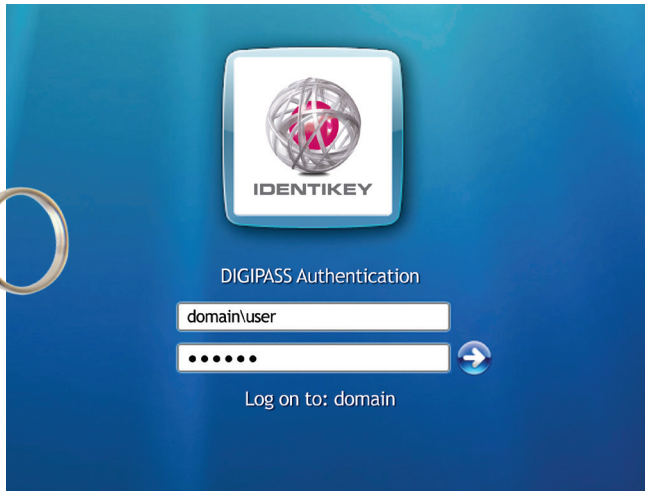
SECURE IN CONNECTED AND UNCONNECTED MODE

When laptops are used outside the corporate network, for instance on the road or at home, the log-on module will work in unconnected mode, allowing the same strong authentication functionality as in connected mode. This prevents unauthorised access even when these laptops are unsupervised or stolen.

If the computer works in unconnected mode, the login credentials are validated against a local database of one-time passwords. These OTPs are generated when the PC is working in connected mode, and they are securely encrypted and stored. With thousands of OTPs generated upfront, the user can work for several weeks in unconnected mode.

AUTOMATIC DETECTION OF AUTHENTICATION SERVER

Behind-the-scene mechanisms have been implemented to ensure that the correct IDENTIKEY Server is detected on the network when a user reconnects and that the static password in the IDENTIKEY database is always up-to-date. The communication between the desktop logon module and IDENTIKEY is done over a security certificate-based SSL connection.



COMPLIANCE

IDENTIKEY Server supports the randomization of the user's Active Directory static password as part of the authentication process. This is an often requested feature in environments where regulations and compliance are crucial. It addresses the need of complex, unguessable and unhackable static passwords and prevents any circumvention of the security system by users such as disabling, uninstalling or bypassing the DIGIPASS Authentication for Windows Logon module.

FEATURES

Based on VASCO's proven strong authentication technology, the Windows Logon module offers many benefits in real business situations, such as:

- Microsoft Windows Logon with DIGIPASS strong user authentication
- Seamless integration into an existing Microsoft Active Directory environment
- Supports connected and unconnected mode (for up to 30 days - configurable)
- Supports login to desktop, laptop, server, terminal Server 2003/2008
- Works with VASCO's Password Synchronisation Module to keep static passwords up-to-date
- Supports automatic IDENTIKEY discovery on the network through DNS lookup
- SSL (Certificate) based secure communication
- Requires static password randomization enabled for optimized security
- Offered as part of IDENTIKEY Server Enterprise Edition

SUPPORT FOR SECURE ADMINISTRATOR LOGON

DIGIPASS Authentication for Windows Logon also supports the protection of administrators' login on Windows Server login, as well as for Terminal Server 2003/2008 login by using DIGIPASS on the standard RDP client.

SUPPORTED ENVIRONMENTS

Operational Modes:

- Connected to the corporate network
- Unconnected for up to 30 days (configurable parameter)

Desktop OS:

- Windows XP (SP3+) (32 bits & 64 bits)
- Windows Vista (SP1+) (32 bits & 64 bits)
- Windows 7 (32 bits & 64 bits)

Server OS:

- Windows Server 2003 (R2, SP2+) (32 bits & 64 bits)
- Windows Server 2008 (R2, SP2+) (32 bits & 64 bits)
- Terminal Server 2003, 2008

DIGIPASS:

- All models, 1 per user, Time Based or Event Based, Response-Only
- User License through DIGIPASS DPX file

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