Password Synchronization Manager

Automatically updates renewed passwords and lowers maintenance cost

With the growing number of remote users requiring access to client data, confidential documents, account records and other sensitive information, the issue of security has been a top priority for the business community. VASCO's solution for secure user authentication replaces the weak static password with a short-lived One-Time Password (OTP). Stealing and re-using someone's login credentials becomes impossible: the static password never crosses the wire, and the OTP expires in 30 seconds.

In this system the static password can still be used for back-end authentication as an extra security check. But when this password changes, the user must re-synchronize his DIGIPASS user account with the new password. Up to now, this has been done manually by the user or the administrator. VASCO's newly released Password Synchronization Manager can be used to perform this task automatically. There is no need for further manual interaction.

VASCO OFFERS STRONG USER AUTHENTICATION SOLUTIONS

As a world leader in strong authentication, Vasco Data Security is offering VACMAN as the de facto server software for protection of office applications for enterprises of all sizes.
VASCO's DIGIPASS technology has proven to be the most secure solution for strong authentication and is available in VACMAN Middleware for Enterprise Security and in IDENTIKEY Server for Application Security.

By replacing static passwords with dynamic OTPs, users can prove they are who they claim to be. VASCO's time-based system can generate dynamic OTPs that change every 32 seconds, and are virtually impossible to hack. This is by far the most secure solution available in the market today.

DIGIPASS INCREASES SECURITY LEVEL

Protection of internet based computer infrastructures has traditionally been accomplished with static passwords. Every user is assigned a password that he needs to present when accessing the corporate network. On regular intervals, the passwords are updated or renewed, to avoid unauthorized usage. All user credentials are stored in a database that is accessible to an authentication system.

Whenever a user wants to remotely connect to the LAN, his login credentials will be compared with the database fields. If the data match, the user is confirmed and granted access to the company resources.

The use of a static password for remote access has been proven to be highly insecure. Hackers, phishing techniques and Man-in-the-Middle attacks have driven enterprises to deploy a stronger means of authentication.

VASCO is offering its DIGIPASS solution as an answer to the growing need for tighter security. Static passwords are replaced by dynamic One Time Passwords that are time-based and change every 32 seconds, making them completely tamperproof. They are generated by a DIGIPASS device and verified by an authentication server, like VACMAN Middleware or IDENTIKEY Server. The user and his OTP are validated by the server, and access is granted. An additional function can forward the original static password from the VASCO software to the back-end authentication system, adding an extra layer of security.

STATIC PASSWORD RENEWALS

By eliminating the step where the user enters his static password, the chance of misuse by others is significantly reduced. When the static password changes, the DIGIPASS user account needs to be updated with the new password. Currently this has to be done manually by the user or the administrator, and results in increased operational costs and inconvenience.

PASSWORD SYNCHRONIZATION MANAGER

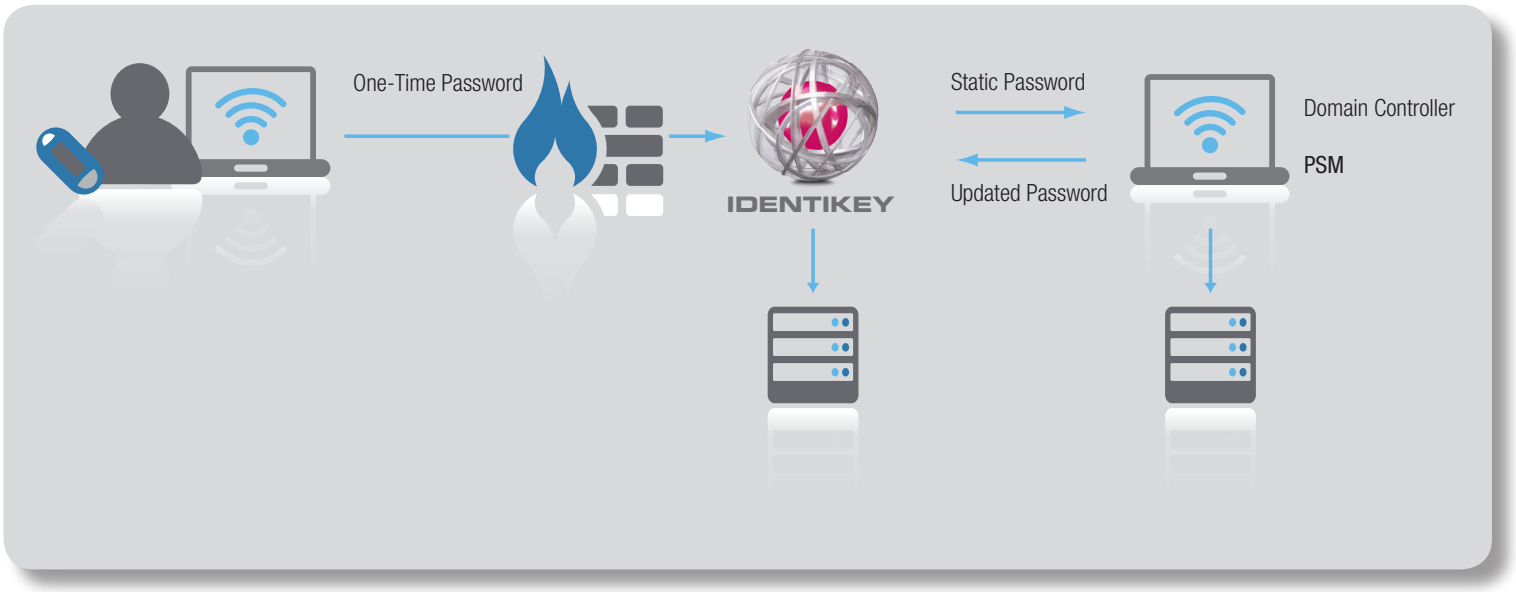
VASCO has created a new tool to automatically synchronize the renewed static password between the user management system and the authentication server. The Password Synchronization Manager (PSM) can be used to perform this task automatically, which eliminates the need for any manual interaction. It is installed on the Domain Controller and sends the updated static password to IDENTIKEY Server or VACMAN Middleware.

KEY FEATURES AND BENEFITS:

- Automatically updates the DIGIPASS user account with a renewed static password
- Avoids the need for administrators to update the password manually
- Greatly reduces the cost of password management
- Brings added value to existing VACMAN Middleware and IDENTIKEY Server installations

SUPPORTED PLATFORMS AND COMPATIBILITY

- Windows Server 2000, Windows Server 2003
- SQL Server 2000, SQL Server 2005
- Compatible with VACMAN Middleware 3.0
- Compatible with IDENTIKEY Server 3.0
- Supports static password updates in ODBC database and Active Directory (VM 3.0)



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