Make it Mobile

How to succesfully implement a secure mobile strategy

www.vasco.com

Make it Mobile

The mobile revolution is inexorable. Mobile devices such as smart phones, netbooks and tablets proliferate in today's personal and professional environment. In order to adapt to the fast paced virtualization and mobilization trend, organizations worldwide will have to make their applications, data and corporate information accessible from any portable device for customers, suppliers and employees.

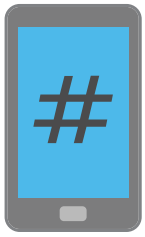
Do benefits outweigh concerns?

The accessibility of mobile applications and mobile working yields many benefits: it can be time-saving, cost reducing and the added bonus of flexibility can enhance overall productivity and customer loyalty. While embracing the flexibility of mobile working, it is essential not to be heedless of the dangers that may come with it. Concerns about data integrity, the privacy and accessibility of sensitive data, and data protection requirements are the most significant obstacles for financial and business organizations to embrace the mobility trend.

Potential threats for mobile applications such as m-banking and m-commerce or even remote access to a corporate network, are similar to those of traditional applications, only the platform and technology have changed. As the business world will continue to change under the influence of continuous technological developments, working practices will change as well. And with the increasing trend of BYOD (Bring Your Own Device) on the work floor, security remains all-important.

Mobile Facts

there will be **1,9 billion** mobile phones worldwide by 2013



	69,7 %	Android
	20,9 %	Apple
	3,5 %	BlackBerry
	3 %	Windows
	2,9 %	Other

Market share based on Q4 2012

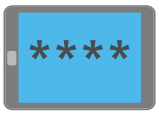
How to succesfully implement a secure mobile strategy

Security is as strong as the weakest link

Protecting access to online applications such as m-commerce or m-banking services or access to corporate networks might be a good solution. However, any security system is only as effective as its weakest link.

Source: Gartner

350 million
employees will use it for work



50% do not password protect their device

51% have financial apps on their phones

35% have shopping apps

60% disire secure mobile authentication

VASCO helps you to succesfully implement a **secure** mobile strategy

Consumers and employees often use the same passwords for a multitude of professional and personal applications. By reusing the same password over and over again, they put every application containing confidential information – although unwillingly and perhaps unknowingly – at risk. Furthermore, mobile devices are often not password-enabled and lack the ability to authenticate users and control access to data stored on the devices.

Added security layer with two-factor authentication

Deploying an adequate security environment for every mobile device used by customers, consumers or employees is a daunting task. Furthermore, end users don't want to be burdened with laborious procedures in order to retrieve information or complete an online transaction.

Two-factor authentication offers an answer to these challenges. It provides a higher level of security than traditional passwords and ensures that only authorized people gain access to sensitive information. The mobile device is then uses as a second factor and can be used as an authentication device to generate a strong one-time password. These passwords, with a limited validity, can be generated on the device itself or can be sent via text message to the user's mobile phone.

Several mobile authentication solutions to suit your needs

VASCO has several solutions in its product portfolio that were developed with the mobile user in mind. DIGIPASS is VASCO's renowned technology that replaces weak static passwords with dynamic passwords that have a limited validity. Fraudsters can thus not reuse an end users password at a later time. Additionally, VASCO's mobile solutions also provide e-signature capability to sign online transactions in all security. This e-signature will be calculated using transaction data, time and the secret stored on the mobile device. If intercepted or altered, the electronic signature will expire and the transaction will not be completed.

VASCO's authentication solutions can be integrated into any existing infrastructure offering multi-platform support. You can also deploy multiple devices to secure your application enabling you to differentiate according to your authentication needs.

Key benefits of mobile authentication

- Enhanced security
- Increased flexibility
- Excellent user convenience
- Intuitive use
- Easy upgradeable
- Limited impact on end-user's experience
- Competitor differentiation thanks to authentication
- Increased customer trust
- No need to deploy hard- or software devices
- Low TCO

How to secure your assets?

Two-factor authentication ensures that only authorized people get access to your sensitive information, your corporate network or your online application.

VASCO's mobile solutions and services:

- DIGIPASS for Mobile
- Virtual DIGIPASS
- DIGIPASS Nano
- DIGIPASS powered by Intel ITP
- DIGIPASS SDK

Mobile security for everyone

VASCO's mobile software solutions are suited for any organization that wants to provide secure remote access to its corporate network or applications. Regardless of size, VASCO offers solutions that fit your needs.

Whether it is to secure your mobile banking, your e-commerce or your gaming applications or your confidential business data, all software solutions can be deployed to fit your needs. We have proven expertise and experience with approximately 10,000 customers worldwide, including almost 1,700 financial institutions.

VASCO's mobile authentication solutions

Software Authentication

DIGIPASS for Mobile

DIGIPASS for Mobile is an application that generates one-time passwords and e-signatures on the mobile device of your choice. The time-based one-time password (OTP) is a dynamic authentication code and the most effective defense against complex cyber attacks.

Users will experience the freedom to conduct their business securely from a mobile device while traveling throughout the world. To enhance user convenience DIGIPASS for Mobile supports QR-codes. Users simply capture the QR code, enter their PIN code and are instantly logged on to the application. Document or transaction signing is equally simple.

The DIGIPASS for Mobile application itself is bound to device-dependent components and linked to the user with a PIN code. Therefore the applications cannot be duplicated on another phone or mobile device.

DIGIPASS for Mobile offers enhanced provisioning services including HSM server side implementation. Customers willing to outsource provisioning can make use VASCO's DIGIPASS as a Service provisioning service.

For more information, visit www.vasco.com/DIGIPASSforMobile

SMS Authentication

Virtual DIGIPASS

Virtual DIGIPASS offers a user-friendly and cost efficient solution for strong user authentication and e-signatures. Virtual DIGIPASS allows dynamic passwords to be sent to a user's mobile phone via SMS.

The solution can be used as a primary or back-up authentication method in case an authentication device is lost or has been forgotten. This guarantees a continuity of service without requiring helpdesk support.

Based on two-factor authentication - something you know and something you "already" have - Virtual DIGIPASS adds another layer of security to log-in functions where static passwords are still in use.

For more information, visit
www.vasco.com/VirtualDIGIPASS

SIM Authentication

DIGIPASS Nano

DIGIPASS Nano enhances the security of online service channels through the use of e-signatures and end- user authentication.

DIGIPASS Nano has a unique form factor and opens new perspectives in using mobile devices as an authentication means. The solution consists of a thin film that is placed on top of any SIM-card enabling the phone to generate one-time passwords and e-signatures. The solution is supported by every compatible mobile phone fitted with a SIM Card.

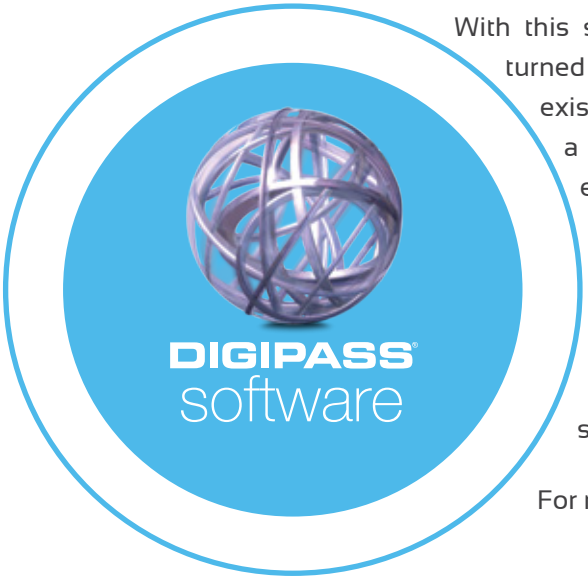
Mobile users will be able to perform secure transactions, access business-critical data or transfer money anywhere at any given time.

For more information, visit www.vasco.com/DIGIPASSNano

Native integration

DIGIPASS SDK

DIGIPASS SDK allows you to natively integrate DIGIPASS technology into your applications. The solution adds strong authentication directly to the application without external software interacting with the company's system. One-time password and e-signature capability become thus an integral part of the online application.



With this solution virtually any device with processing power can be turned into a DIGIPASS authentication device. It leverages the use of existing applications and devices such as third party applications, a browser, desktop or server for two-factor authentication and e-signatures.

DIGIPASS SDK allows the integration of strong authentication into any regular software environment. It can also rely on any external Secure Executive Environment. As a result, DIGIPASS SDK has the best of two worlds: ease of integration, worldwide support and extended security to hardware processing.

For more information, visit www.vasco.com/DIGIPASSsdk

VASCO's mobile authentication solutions

Embedded Authentication

DIGIPASS Powered by Intel

Intel® Identity Protection Technology (Intel® IPT) is a two-factor authentication capability built into select* 2nd Generation Intel® Core™ processor based PCs helping to prevent unauthorized access to important personal accounts.

Intel IPT is a powerful, additional layer of security that links a PC to the online account or financial asset of user's choice, decreasing the ability of thieves to access account information from non-associated computers. Intel IPT helps keep your accounts secure, even if the first layer of authentication is breached.

VASCO is utilizing the embedded security feature of Intel IPT from the world leader in computing innovation. This solution leverages the industry's best security on nearly every laptop and desktop in the world – without the need to provision any software or hardware to the end-user. An activation process is very simple and can be configured according on a web site or application provider specifications.

For more information, visit www.vasco.com/DIGIPASSIntel

MYDIGIPASS.COM™

Don't forget to discover VASCO's latest secure mobile application

DOWNLOAD NOW

iPhone & other

VASCO BUSINESS CASE

Qatargas secures corporate network access by implementing DIGIPASS and IDENTIKEY into its Citrix metaframe

Challenge

Implement a Citrix compliant solution that secures the company's network and applications enabling remote access for executive management, remote offices and contractors.

Objective

The company deployed IDENTIKEY Gold Edition together with DIGIPASS GO 6, Virtual DIGIPASS and DIGIPASS for Mobile. This combination allows the group to secure access to its business applications for its different target groups. IDENTIKEY works seamlessly with the various DIGIPASS solutions and requires no additional hardware investment. Moreover, the number of users over time is easy to extend thanks to the flexible licensing system.

Solution

DIGIPASS has leveraged the security level of Qatargas' remote network and business applications through the use of dynamic one-time passwords. DIGIPASS in combination with IDENTIKEY is fully compliant with Citrix' solutions hence providing secure remote access to the Citrix metaframe.

About

Qatargas pioneered the liquefied natural gas industry in Qatar. Today the company is realizing its vision to deliver LNG to customers around the globe from its facilitiesin Qatar. With remote offices and on- and offshore plants in different locations, Qatargas was looking for a secure remote access solution allowing its employees and contractors worldwide to access its corporate network and business applications.

"We prefer to use software authentication devices whenever applicable to avoid the logistic challenges of delivering hardware devices to our overseas offices and plants. The fact that VASCO's solutions are reliable and simple to manage, was a decisive factor in the decision making process."

Mohammed Abu-Nejim
Head of Data Networks at Qatargas

VASCO BUSINESS CASE

Randstad Germany uses VASCO to secure remote access

Objective

Replace the existing authentication solution for secure remote access to the corporate network for approximately 1,000 mobile employees.

Challenge

The migration had to be made quickly and on the fly, without compromising the security of the remote access solution.

Solution

Randstad opted for the combination of VASCO's IDENTIKEY Authentication server and DIGIPASS authenticators. As a back-up for the hardware DIGIPASS, Randstad also deployed Virtual DIGIPASS and DIGIPASS for Mobile.

About

To protect its sensitive data from unauthorized access, the employment agency Randstad Germany has been relying for years on a strong two-factor authentication solution to secure its remote access. When after the spring of 2011 a security issue was detected in the solution of the manufacturer at the time, Randstad decided to switch to VASCO's DIGIPASS authentication solution and IDENTIKEY Authentication Server.

"Availability and safety were our main priorities for our remote access solution. The concerns we had about the security of our previous solution provider prompted us to look around for alternatives... We were really impressed by the possibilities and found it to be more suitable than our former solution."

Stefan Gräf, Team Manager Network & Storage at Randstad Germany.

VASCO BUSINESS CASE

HSBC Bank Brazil provides full integration between its electronic channels with m-banking and VASCO's DIGIPASS for Mobile

Objective

Enhance HSBC Bank Brazil's multi-channel approach by offering secure m-banking services to its retail customer base.

Challenge

To secure HSBC m-banking services, the application must be small and generic, fit for any mobile device. Furthermore, the application needs to be chip, device and telecom provider independent.

Solution

DIGIPASS for Mobile conveniently provides secure m-banking services anywhere, anytime. From now on, HSBC Brazil retail customers are identified through their mobile phone and social security number instead of their account number. This new method whereby the mobile phone is used as an authentication device enables customers to use their mobile phone to access HSBC services through all channels (ATM, Internet Banking, Phone Banking) without needing to remember their account and branch number in addition to user name and password combinations.

About

HSBC Bank Brazil is the first bank in Brazil to offer integrated m-banking services based on VASCO's DIGIPASS for Mobile. HSBC retail customers can withdraw cash from ATMs, make transactions, money transfers and online payments using their mobile phone as an authentication device.

"We chose VASCO because the company is worldwide recognized as a reliable global authentication services provider. Furthermore, DIGIPASS for Mobile is a highly scalable solution with a very cost effective maintenance and roll out. VASCO's mobile authentication solution allows HSBC Brazil to offer its customers highly secure yet convenient and simplified online user experience."

Marcello Veronese
Head of One HSBC distribution

VASCO BUSINESS CASE

Insites implements VASCO's IDENTIKEY and DIGIPASS solutions to guarantee data confidentiality

Objective

Implement a user-friendly remote access solution that is simple to integrate. Insites wanted to grant its employees secure remote access to the network without compromising data confidentiality.

Challenge

The authentication solution needed to be cost-efficient, user-friendly, flexible and compatible with the Citrix XenApp / XenDesktop network.

Solution

Insites deployed VASCO's DIGIPASS GO 3, GO 6 and in a later phase, DIGIPASS for Mobile in combination with IDENTIKEY Server. This user-friendly solution was very simple to implement and ensures secure remote access to the Citrix XenApp / XenDesktop network for Insites' employees.

About

Insites Consulting is a global online market research company, known for its creative research solutions and specialized in communication and storytelling. Headquartered in Belgium, Insites also has offices in the United Kingdom, the Netherlands and Switzerland. Gathering large amounts of confidential data, the company was in need of a security solution enabling secure remote access to its network data through a VPN portal.

"We wanted to implement a solution that not only would secure access to our business-critical data, but that also allowed us to allocate different users to one user account. We have decided to deploy DIGIPASS for Mobile as well to offer our employees an even greater flexibility as everyone possesses a mobile phone and consequently always carries his DIGIPASS with him."

Gunter Van de Velde
IT manager at Insites

VASCO BUSINESS CASE

Picanol Group implements IDENTIKEY Gold Edition in combination with DIGIPASS technology to secure access to the company's network

PICANOL
YOU ARE ALWAYS AHEAD

Objective

The Picanol Group wanted to implement a complete solution for its vendors, consultants and external collaborators to secure internal and external access to its various business applications.

Challenge

The company wanted a solution that could be implemented in phases and would be easy to expand. The solution eventually will be extended to not only secure remote access to applications, but also internal confidential information without the Group needing to make additional investments in a later phase.

Solution

The company deployed IDENTIKEY Gold Edition together with DIGIPASS GO 6, Virtual DIGIPASS and DIGIPASS for Mobile. This combination allows the group to secure access to its business applications for its different target groups. IDENTIKEY works seamlessly with the various DIGIPASS solutions and requires no additional hardware investment. Moreover, the number of users over time is easy to extend thanks to the flexible licensing system.

About

The Picanol Group is an international, customer-oriented group that specializes in the development, production and sales of weaving machines and other high technology products, systems and services.

"We wanted a solution that would be available to suppliers, consultants and people with or without a mobile company phone. Therefore we decided to deploy different types of DIGIPASS devices. This solution gives us the additional flexibility that we need."

Bart Lagast
System Engineer at the Picanol Group

VASCO BUSINESS CASE

Connection to real-time sales information for Lightplus thanks to DIGIPASS for Mobile

Objective

The sales team wanted to get rid of all the phone calls they had to make to gain safe access to the internal ERP-system. When they are at a customer, they needed the real-time information to offer best deals and to inform them correctly.

Challenge

The solution had to be straightforward, without too many devices or different passwords that had to be remembered. Simplicity was the primary driver.

Solution

Lightplus implemented DIGIPASS for Mobile, allowing remote secure access to the ERP system without the need to carry an extra device which can easily be forgotten. In the back-end, the IDENTIKEY Authentication Server was deployed, in a combination with Citrix.

About

For ages, light has been one of the main needs for every creature, states Lightplus. The company is an authoritative Belgian importer and distributor of LED lighting and low-energy light bulbs since 2003. When on the move, the Lightplus sales team has to log on securely to the internal ERP system. However, the initial procedure proved to be time-consuming and inconvenient. To overcome this problem, Lightplus implemented strong authentication with VASCO's DIGIPASS for Mobile and IDENTIKEY Authentication Server.

"Our VPN-connection is now protected by strong authentication. We are happy that the access is now easy and secure. Our sales team agrees that this mobile solution was the best option. The endless phone calls to get access belong to the past. Everything has become very easy. They consider this as necessary, but confident and secure."

Jo Beuls
managing director of Lightplus

VASCO BUSINESS CASE

VASCO's authentication solutions help Global Radio to secure remote access and develop a long term security policy

Solution

VASCO's IDENTIKEY Server Enterprise Edition at the back-end and a combination of DIGIPASS for Mobile, Virtual DIGIPASS and DIGIPASS GO 3 at the end-user side, allowed Global Radio to quickly implement the authentication solutions within the limits of the tight deadline. The scalability and the flexibility of the solution also provide Global Radio with the opportunity to expand strong authentication to other company applications in the future.

About

Global Radio is UK's largest commercial radio company and the home of many leading commercial radio brands. When searching for a strong authentication solution to secure remote access for its website content editors, Global Radio opted for VASCO's DIGIPASS technology and IDENTIKEY Authentication Server at the back-end.

Objective

Global Radio was looking for an effective, cost-effective and user-friendly authentication solution to secure remote access for website content editors working from home. The solution needed not only to meet Global Radio's immediate authentication needs, but also had to be suited for future larger deployments within the company.

Challenge

The company had already made prior investments, and therefore required a flexible approach with a mix of hard- and software authenticators. The solution must fit seamlessly within the existing infrastructure. Moreover, the system had to be up and running within eight weeks.

"DIGIPASS for Mobile is a budget friendly solution: you don't have to worry about the distribution, and the authenticators can be managed centrally by the company. It is also a very-user friendly solution, as the download and employment process are very straightforward."

Ross Draper, IP Infrastructure Manager at Global Radio.

VASCO®

THE AUTHENTICATION COMPANY

Request more information:

info@vasco.com
www.vasco.com/contactus