Make it Mobile
How to successfully implement a secure mobile strategy

Request more information:
info@vasco.com
www.vasco.com/contactus
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 mobile 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 **2.1 billion** mobile phones worldwide by 2017

<table>
<thead>
<tr>
<th>Platform</th>
<th>Market Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>79.0%</td>
</tr>
<tr>
<td>Apple</td>
<td>14.2%</td>
</tr>
<tr>
<td>Windows</td>
<td>3.3%</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>2.7%</td>
</tr>
<tr>
<td>Other</td>
<td>0.8%</td>
</tr>
</tbody>
</table>

Market share based on Q2 2013
How to successfully implement a secure mobile strategy

Security is as strong as the weakest link

Protecting access to applications such as m-commerce or m-banking services or access to corporate networks becomes essential. However, any security system is only as effective as its weakest link.

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.

Source: Gartner (August 2013)

by 2017, 50% of employees will use their own device for work

50% do not password protect their device

51% have financial apps on their phones

35% have shopping apps

60% desire secure mobile authentication

VASCO helps you to successfully implement a secure mobile strategy
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 used as a second factor and can be used as an authentication device to generate a strong one-time password. This password, 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 user’s 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 Apps
• DIGIPASS for Mobile
• Virtual DIGIPASS
• DIGIPASS Nano
• DIGIPASS powered by Intel ITP
• MYDIGIPASS.COM

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 1,700 financial institutions.
**Software Authentication**

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.

For more information, visit [www.vasco.com/DIGIPASSforMobile](http://www.vasco.com/DIGIPASSforMobile)

**SDK for 360° security**

DIGIPASS for Application Perimeter Protection SDK (DIGIPASS for APPS) is a software development kit designed to secure (mobile) applications. It offers a comprehensive set of modules giving developers all necessary building blocks to secure their application at every level.

DIGIPASS for APPS enables application developers to streamline and manage the entire provisioning, deployment and lifecycle process offering several options for end user activation. Multiple devices can be used with a single license.

Highlights include:

- Native integration of strong authentication
- Patented CrontoSign technology, supports an extended list of QR codes and barcodes
- Supports geolocalized OTPs and e-signatures
- Jailbreak and rootkit detection
- Device binding
- Secure storage & secure channel
- Out-of-band login support

For more information, visit [www.vasco.com/DIGIPASSforApps](http://www.vasco.com/DIGIPASSforApps)
SIM Authentication

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

SMS Authentication

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 authentication method or as back-up 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
Visual transaction signing

CrontoSign™ is an innovative patented visual transaction signing solution providing a user friendly and effective way to withstand even very sophisticated attacks by Trojan malware, targeting online banking services.

The Cronto mobile application delivers the most optimal combination of usability, security and cost of ownership by allowing users to verify and sign transactions anytime, anywhere.

Account holders simply scan a CrontoSign image on the bank’s website with their mobile phone. Transaction details are immediately displayed on the screen of the user’s mobile device. Users verify these transaction details and sign the transaction with the generated electronic signature displayed on their screen.

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

Embedded Authentication

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 a user’s choice, decreasing the ability of thieves to access account information from non-associated computers. Intel IPT helps to keep your accounts secure, even if the first layer of authentication is breached.

VASCO utilizes 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. The activation process is very simple and can be configured according to different specifications.

For more information, visit www.vasco.com/DIGIPASSIntel
Native integration for mobile apps

MYDIGIPASS.COM is a cloud authentication platform that allows application service providers to easily integrate strong authentication in their online services. MYDIGIPASS.COM terminates all static password vulnerabilities. Online accounts are protected with OTP technology, putting all phishing and pharming schemes to bed.

The fully hosted and managed service allows organizations to focus on their core business instead of dedicating resources and investments in the set-up and roll-out of an on-premise authentication solution.

MYDIGIPASS.COM now offers mobile app developers the possibility to natively integrate authentication into their mobile apps. The solution is very straightforward and convenient for the end user as the authentication process is seamlessly integrated into the mobile app itself. Users click the ‘MYDIGIPASS.COM Secure Connect’ button and are automatically redirected to the MYDIGIPASS.COM mobile application where they enter their PIN code. Once this is validated by the MYDIGIPASS.COM app, the user is automatically redirected to his mobile app. The authentication process is entirely done in the back-end, invisible for the end user.

For more information, visit mydigipass.vasco.com
For our end users, it was of large importance that the system security was trustworthy and user-friendly. Also, they like the fact that they can choose between different kinds of DIGIPASS: a “physical” device, an SMS-code or an application. Logging in securely is a crucial part of our service.”

Maarten de Vries, Managing Director at ApplicationNet
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.

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.

“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.
National Bank of Fujairah relies on VASCO’s DIGIPASS to protect corporate applications and transactions.

Objective

On the one hand, National Bank of Fujairah wanted to protect internal applications, such as OWA, VPN and Sharepoint. On the other hand, the bank was looking for a secure transaction solution.

Challenge

Ease-of-use was very important, just like the trust the solution should radiate. After all, NBF is an innovative bank that cares about its customers.

Solution

DIGIPASS 275 and DIGIPASS for Mobile were selected, in order to give the end user the possibility to choose his preferred authentication tool. Both solutions can generate OTPs and have a challenge/response functionality, so user authentication and electronic signing can be executed by the same device.

About

National Bank of Fujairah (NBF) was incorporated in 1982 and has had a long established reputation in the areas of corporate and commercial banking, trade finance and treasury. As a leading bank in United Arab Emirates, NBF has always set great store by security and data protection. Therefore, the bank has decided to implement VASCO’s DIGIPASS technology to protect its internal applications and to make sure its corporate banking users can approve transactions securely.

For us, it was important to partner with a market leader that could demonstrate expertise in the financial sector. Furthermore, the availability of various models and the possibility to present two different options to our customers were important to us.”

Nasar Siddiqui
Head of Electronic Channels at NBF
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 need 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, 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
Objective

Croatian Telecom intended to offer a Virtual Desktop to its customers with a completely integrated security solution. They had to design a solution that would provide high security at a competitive price per month per user.

Challenge

The main challenge was to implement a secure but cost-effective solution that is user-friendly and would fit into the existing infrastructure.

Solution

Virtual DIGIPASS in combination with IDENTIKEY Authentication Server provided the perfect answer to the demands of Croatian Telecom. The solution offers an easy-to-integrate, highly secure environment and fits into the pricing policy of the company.

About

Croatian Telecom is a member of the T-HT Group and a leading provider of telecommunications services in Croatia. The basic activities comprise provision of telecommunications services, design and construction of telecommunications networks in the territory of the Republic of Croatia. In addition to the provision of fixed telephony services, the group also provides Internet services, including IPTV, data transmission services and GSM and UMTS mobile telephone networks.

VASCO’s solution is highly portable as the mobile phone acts as an authentication device. End users no longer have to worry or think about carrying around an extra device for authentication, and we don’t have to worry about the distribution process of hardware authenticators.”

Goran Car, Director of Professional Services Division from Combis.
Objective
Rotterdam University was looking for a way to grant secure access to sensitive information to its employees. On top of that, the university wanted to grant a few people the ability to add, change or delete important information without impacting the existing software and application functionalities.

Challenge
A solution that can be easily integrated in the central login system; the Novell e-directory with NMAS, that is easy to use. After a one-time login, the employee should have access to the multiple applications and systems.

Solution
The University of Rotterdam employees now use VASCO authentication technology to consult or adapt important information. Employees can choose between a hardware DIGIPASS GO 3 and GO 6 or a software DIGIPASS. The back-end consists of DIGIPASS plugin for NMAS.

About
Employees of Rotterdam University have to log in through the central login system to get access to the different decentralized systems the educational institution works with. In order to guarantee that only employees get access to this important information such as exams and personal details, VASCO’s authentication solution with one-time passwords (OTPs) was implemented.

The app is installed on the employee’s smartphone, so dynamic passwords can be generated on his own device. This is considered a significant advantage. The integration went smoothly, we had good support from VASCO and we went through the entire integration process without a problem.”

Eric Kerkdijk, ICT Supervision & Operations Manager Rotterdam University.
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
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.
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 a highly secure yet convenient and simplified online user experience.”

Marcello Veronese
Head of One HSBC distribution
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 decided to deploy DIGIPASS for Mobile and 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
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 Authentication Server 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 Authentication Server 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
Marcello Veronese, Director of Digital Channels at HSBC, says; “The enhancement of this broader DIGIPASS for Mobile deployment is the result of more than five years of research and development. We wanted to ensure that our customers would profit from an innovative and easy-to-use authentication solution, not only in Brazil, but also worldwide. Thanks to the partnership with VASCO, we created a state-of-the-art solution. It’s a significant advantage for the Brazilian market where cards with static passwords are still widely in use.”

MOBILE CUSTOMER QUOTES

We are thrilled to partner with VASCO,” says Jean-Louis Van Houwe, CEO of Monizze. “We offer our customers elaborate payment solutions without compromising security. VASCO has built a worldwide reputation as a specialist in securing banking applications. By integrating VASCO’s innovative and renowned technology into our web applications, we give our users the fundamental trust to use our online services in a secure manner without being oblivious about user-friendliness.”

Thinfactory was eager to offer its Cloud Plaza users a two-factor authentication solution with banking level security. In VASCO we found a trustworthy partner that could supplement our service offerings with its DIGIPASS as a Service. Its ease of use, scalability and high level of security are only some of the advantages that were decisive for us,” says Johan Verhaeren, Head of Sales and Marketing at Thinfactory.

Marcello Veronese, Director of Digital Channels at HSBC, says; “The enhancement of this broader DIGIPASS for Mobile deployment is the result of more than five years of research and development. We wanted to ensure that our customers would profit from an innovative and easy-to-use authentication solution, not only in Brazil, but also worldwide. Thanks to the partnership with VASCO, we created a state-of-the-art solution. It’s a significant advantage for the Brazilian market where cards with static passwords are still widely in use.”
Mobile devices are omnipresent in today’s enterprise ecosystem,” says Payam Moini Tabatabai, Founder & CEO of MOBYLLA. “However, regulations may differ from country to country. We need solutions that are compliant with national regulations in different countries. Additionally, we wanted to implement a security solution that doesn’t compromise user-friendliness which is essential for any mobile platform. Users will be reluctant to follow complicated processes on any mobile platform. VASCO’s MYDIGIPASS.COM native authentication solution proved to be the ultimate solution. We are able to offer our customers the best authentication solution combining high security and an unmatched user convenience.”

“We make it a priority to continuously improve our service,” states Danilo Cattaneo, InfoCert’s Director General. “By integrating MYDIGIPASS.COM into Legalmail we can offer double added value to our customers, increase access security and provide even greater convenience and satisfaction in the use of our products.”

Thanks to the cooperation with VASCO, we can offer our customers an extra layer of security, so that their personal data is better protected,” says Serge Van de Zande, founder of Ello Mobile. “The implementation of an ‘in the cloud authentication platform’ fits perfectly in our web-based strategy.”

“Trust is a high value in our business club,” says Business Club Bavaria President Kajetan Brandstätter. “On the Internet, it is very easy to misuse trust. All too often, fraudsters steal access codes and then use the stolen identity as their own. The reputation damage for our business club in that case would be tremendous. We are the first business club to offer our members a real workable and safe security concept.”