Building a secure banking environment

The world’s leading software company specializing in Internet Security
Full option, all-terrain authentication

VASCO’s full option approach ensures that all authentication technologies are hosted on the single and unique VACMAN® platform. Our range of over 50 DIGIPASS® end user authentication devices, whether they are hardware or software-based, all work with the VACMAN platform.

VASCO’s solutions are all-terrain: independent from the customers’ field of activity, VASCO offers solutions that fit their needs. Renowned for its experience in securing online banking applications, VASCO brings banking level security to a wealth of business applications in several vertical markets, including healthcare, e-gaming, automotive, human resources, education, administration, e-government, legal, supply chain, manufacturing and many others.

Strategy

VASCO offers a complete array of authentication solutions and services to the financial services sector. We expand our penetration by bringing these banking level security solutions to other markets such as business enterprises and the B2B, B2E and B2C markets. VASCO continuously enhances and broadens its line of security products and services to meet the changing needs of its existing and potential customers.

Core activities

User authentication
Log-on access process that verifies if the user is in fact who he claims to be. VASCO’s DIGIPASS technology replaces insecure static passwords with strong one-time passwords. These passwords are only valid for a limited period of time and cannot be reused.

Electronic signature
Secures a transaction or message between two known parties. E-signatures offer adequate protection against man-in-the middle attacks and similar fraud schemes. They allow you to verify that information and transactions haven’t been altered in transit.

Digital signature
Secures transactions or messages using PKI technology between two parties who don’t necessarily know each other, whereby the third party guarantees the identity of all parties involved.

PKI allows banks, enterprises and governments to sign transactions and documents using certificates and keys. PKI solutions provide non-repudiation and data integrity.
Secure online banking

A secure online banking experience

Banks worldwide provide online and mobile financial services, offering their customers a more convenient way to conduct their banking affairs while at the same time improving efficiency and saving on operating costs.

The proliferation of mobile devices created many opportunities for the growth of online and mobile banking services. Security concerns remain, however, as banking accounts are frequently targeted by cybercriminals and fraud schemes become more complex. As a result, banks need to implement adequate security measures to protect themselves and their customer base.

Boost customer trust

VASCO helps banks and financial organizations to secure their online and mobile channels. As a world leader in strong authentication, VASCO offers strong two-factor authentication and PKI solutions to meet any financial organization’s needs.

By deploying VASCO’s renowned DIGIPASS technology, banks are able to authenticate their customers and mitigate risks stemming from phishing scams, hacking, Trojans and man-in-the-middle (MITM) attacks. Secure online/mobile services will boost customer trust and will enable banks to build an enduring competitive advantage.

Tailored solutions

VASCO has a vast experience in the deployment of large scale authentication projects with millions of end users but also attends to the needs of smaller and mid-sized banks with tailored solutions to match their specific needs. We offer a wide range of back-end solutions, including a managed outsourced authentication service. Our end user devices range from software and hardware OTP authenticators to e-signature devices for transaction validation and digital signatures using PKI technology.

DIGIPASS®

Authentication devices providing strong user authentication and electronic or digital signatures. Available in software or hardware format or as a smart card reader

VACMAN®

Back-end core authentication platform suited for massive deployments

IDENTIKEY® Authentication Server

Centralized authentication server suited for organizations of all sizes

DIGIPASS® as a Service

Cloud-based authentication in a managed service model

MYDIGIPASS.COM

Cloud-based authentication platform for B2B and B2C
Retail Banking

Retail banking services were once provided in person. Nowadays, account checking, saving plans or bill payments are offered online or through mobile apps. You can pay your bills, make transactions or purchase goods online - without wasting time in queues.

Sadly enough, retail banking accounts are often exploited by fraudsters for financial gain, most commonly by trying to intercept customers’ passwords. Banking customers who have been hacked not only lose their assets, they also lose their trust in online banking channels and the bank’s reputation is damaged.

VASCO’s strong authentication is a key step towards an increased level of security and the reinstatement of customers’ trust in online and mobile banking services. VASCO offers a wide range of solutions for the consumer electronic banking market, including hardware-based authenticators, smart card readers or software and mobile authentication solutions.

Corporate banking

Corporate banking environments were the first to see the benefits of two-factor authentication. For financial institutions conducting transactions over electronic channels, the most prevalent vulnerability is also the most obvious one: the use of static passwords as a form of user authentication. Outdated and weak, static passwords are ineffective against today’s security threats. Corporate e-banking is tempting for fraudsters, not only because the amount of money involved is substantially higher, but also because banking systems are less likely to detect fraud attempts on these accounts.

As a global leader in two-factor authentication for the financial industry, VASCO offers mature technologies designed to strengthen the existing security policies with minimal impact. VASCO presents a variety of strong authentication solutions, such as amongst others PKI authenticators, smart card readers or other hardware-based DIGIPASS devices.
Customer references

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

As a leading bank in United Arab Emirates, NBF has always set great store by security and data protection. The bank decided to implement VASCO’s DIGIPASS technology to protect its internal applications and to make sure its corporate banking users can approve transactions securely. Ease-of-use was very important, just like the trust the solution should radiate. 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.

Sumitomo Mitsui Banking Corporation implements DIGIPASS 275 to secure its retail banking services

Sumitomo Mitsui Banking Corporation (SMBC) is one of the largest banks in the world. More than 22,000 employees guard the bank’s mission: providing valuable services that help its customers to build their own prosperity, to create sustainable value for its shareholders founded on growth in their business, and provide a challenging and professional rewarding working environment for its dedicated employees.

SMBC needed additional security measurements to meet the changing environment and to counter diversified attacks. The company also wanted to strengthen the value of its banking services and to endorse its customers’ confidence. User-friendliness and a high level of security measurements were the main concerns. DIGIPASS 275 was selected for its easy-portability, its fashionable design and the solution’s intuitiveness.

BW-Bank: online banking security for all

BW-Bank is the first bank in Germany to replace TAN-lists with one of the world’s leading security practices: strong authentication. All BW-Bank customers received a BW-Bank TAN generator, a model from the DIGIPASS family. At the bank’s side, the VACMAN Controller software suite has been implemented to verify all authentication requests.

Meanwhile, all online banking customers use DIGIPASS to access their online banking accounts. And with success: since October 2007, BW-Bank has reported just one case of online fraud.
Mobile Banking

In our fast-paced, ever-connected world, mobile technology is an interesting if not essential feature banks can offer. It was introduced to fill customers’ needs, such as saving time, quality of service or the elimination of geographical barriers. Additionally it also benefits banking institutions when it comes to service costs or customer satisfaction. However, like any emerging electronic channel, mobile banking is vulnerable to fraudsters preying on gaps in security. Even though the platform has changed, the challenges faced in m-banking are similar to those in e-banking.

Today, the most common m-banking channels are telephone banking, IVR (Interactive Voice Response), SMS-based solutions, client/server-based applications (downloadable or pre-loaded), WAP and STK (SIM application Toolkit) banking. To reinforce security in mobile banking applications, mobile authentication is essential. Mobile authentication is a simple, low-impact enhancement that strengthens security.

VASCO offers cost-effective and user-friendly solutions to secure all mobile banking channels. VASCO’s DIGIPASS API brings one-time password and e-signature functionality to end users through their mobile devices, without the need for any additional hardware.

Mobile payments

Mobile payments are an emerging and rapidly-growing alternative payment method. Rather than pay by cash, check or credit card, customers can opt to use their mobile phone to buy goods or services. Thanks to their quick transaction speed and convenience, mobile payments are gaining popularity as a method of paying for items such as music, videos, ringtones, online gaming subscriptions, wallpapers, transportation fare (bus, subway or train), parking meters, books, magazines and tickets.

Mobile payments secured by two-factor authentication provide a secure alternative to credit cards. Since the payment is made via a telephone, no credit card information is stored by the merchant, which eliminates the opportunity for hackers or employees to compromise card information. Because one-time passwords are used, the transaction can be verified to have originated from the exact phone registered for a specific user.

VASCO’s DIGIPASS technology seamlessly integrates with existing mobile payments’ applications. Our mobile solutions offer customers and providers an easy, convenient and secure experience for payment alternatives.

Visual transaction signing: ultimate security and convenience for online and mobile banking services

VASCO’s visual transaction signing solutions protect online and mobile banking services against malicious attacks. Visual transaction signing works with a patented technology whereby a CrontoSign image which resembles a matrix of colored dots, is displayed on the bank’s website.

Account holders enter their transaction details on the bank’s website. These details are then encrypted and presented as a graphical cryptogram on the user’s computer or tablet. Users simply “scan” this image with their mobile phone or a hardware DIGIPASS 760 with built-in camera. The image is immediately captured and decrypted and the transaction details are presented on the user’s mobile phone screen of DIGIPASS 760 for verification. A signature is then generated which the user enters on the bank’s website to confirm the transaction.

Visual transaction signing enhances user-convenience by reducing the level of user interaction when signing online transactions. The solution is ideally suited for banks looking to use e-signatures to secure online transactions without compromising on user-friendliness.
HSBC Bank Brazil provides m-banking using VASCO’s DIGIPASS for Mobile.

HSBC 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 using their mobile phone as an authentication device. The technology is non-reliant on third parties, overcoming provider dependency and network limitations.

DIGIPASS for Mobile empowers financial institutions to quickly launch m-banking services. The solution allowed HSBC to increase its financial services outreach substantially by using a multi-channel approach. In its cooperation with HSBC, VASCO has been honored with the “Best Security Solution” award by the renowned Brazilian banking magazine Relatorio Bancario for its HSBC Brazil DIGIPASS for Mobile banking customer case.

Oman Arab Bank offers its corporate and retail customers a variety of online services and is the only bank in the Sultanate to offer instant bill collection services for telecom providers. The bank also offers online governmental services and has established itself as a leading e-banking service provider. In order to protect its customers against online fraud, the bank implemented VASCO’s renowned DIGIPASS technology in combination with the authentication software IDENTIKEY Authentication Server.

IDENTIKEY Authentication Server could be perfectly integrated into the bank’s infrastructure allowing Oman Arab Bank to add strong authentication to its different applications and channels. DIGIPASS GO 6 and DIGIPASS 260 were deployed for its retail and corporate customer base providing customers secure access to their accounts from anywhere at any time. Thanks to the integration of DIGIPASS technology, the bank was the first to offer card-less ATM services in the Middle East.
Leveraging EMV card investment

EMV cards were deployed to increase the security of credit card transactions by using encryption algorithms that provide authentication of the card to the processing terminal and the transaction processing center. EMV cards can be leveraged for the deployment of two-factor authentication without the cost of issuing any additional personalized authenticators.

The Chip Authentication Program (CAP), a MasterCard initiative which received Visa support, offers two-factor authentication as both a smart card and a valid PIN have to be present for a transaction to succeed.

VASCO’s CAP-based solutions are suitable for mass deployment in retail banking. The customers’ regular debit and/or credit card can be used to generate one-time passwords and e-signatures offering strong authentication. Each of these authentication mechanisms can also secure multiple applications, from e-banking to e-commerce. VASCO can also enhance EMV-CAP solutions with unique authenticators (optical readers, one-button devices) or add-on features like VASCO strong authentication. These enhancements make the deployment of EMV card-based strong authentication even more secure and convenient for banks and their customers.

Preventing ATM fraud

When the Automatic Teller Machine (ATM) was brought into use, thieves used to watch over your shoulder to memorize your PIN and try to steal your debit/credit card. Since then, more complex mechanisms such as skimming and ghost ATMs, have been developed.

Strong authentication can be added to prevent ATM fraud. When a customer wants to withdraw money, he authenticates himself using a one-time password in combination with a PIN code. This extra layer of security can be added without too much hassle as existing ATM infrastructures do not have to be adapted. Besides, the conversion to OTP validation can be executed quite rapidly and inexpensively for banks that already use strong authentication for their online channels.

Banks can leverage their investments made in strong authentication in multiple ways. Either they can link multiple applications, such as e-banking channels, phone banking and ATM operations to a single authentication device. Or they can decide to have a dedicated authenticator for ATM security.
BANRISUL adopts VASCO’s authentication solution for e-banking

Banrisul is a multiple service bank controlled by the state of Rio Grande do Sul and is one of the most profitable banks in Brazil. With a history that goes back almost a century, the bank is focusing on maintaining its leadership position in Rio Grande do Sul. Besides its extensive presence throughout the state, Banrisul has an ability to expand the participation in its current client base by increasing the services used by its customers. By providing its customers with an authentication solution, Banrisul offers them the possibility to access the bank’s online services in total security, anywhere at any time.

Banrisul is the first state bank in Brazil to employ the leading DIGIPASS brand on the market to offer its customers maximum security to conduct their banking transactions. The bank wanted to adopt a solution that was simple to use and had the possibility of unifying strong authentication to digital certification subscription and encryption services. This is one of the reasons, Banrisul chose for VASCO’s DIGIPASS 905 solution. DIGIPASS 905 integrates DIGIPASS security with card reader functionality, offering Banrisul’s customers secure access to its home and office Internet banking services using authentication based on digital certificates stored on smart cards.

DnB Nor implemented VASCO’s DIGIPASS to secure the BankID scheme

DnB NOR is Norway’s largest financial services group offering banking services, life & pension insurances, a financial distribution network and acts as Norway’s largest real estate broker. DnB NOR needed to implement a security solution for BankID that would meet all of BankID’s security requirements. BankID delivers a public key infrastructure (PKI) solution enabling members from the Norwegian public to identify themselves and sign digital documents from authorities, companies and other organizations on the Internet. The BankID scheme works with nearly all Norwegian banks and banking groups, amongst others DnB NOR. It is an open national standard for all citizens with an online-bank, for all enterprises and public offices and is based on PKI technology.

To meet BankID’s security requirements, DnB NOR implemented VASCO’s patented DIGIPASS technology with one-time passwords. Previously, the company worked with different types of systems and security devices for their retail customers. Some customers even had several different devices. DnB NOR wanted to implement one single authentication method to simplify handling which would lead to more satisfied customers and would also reduce costs in the long term. A better and clearer logon process would also reduce calls to the bank’s call center. DnB NOR found in VASCO’s DIGIPASS GO 3 the security solution to suit their and their customers’ needs. DIGIPASS GO 3 is a simple and user-friendly authentication device, offering a high security level compliant with BankID’s security standards.
CLIENT SIDE TECHNOLOGY: DIGIPASS FAMILY

VASCO’s DIGIPASS family offers a wide range of end user authentication devices which all make use of VASCO’s VACMAN core technology. Customers can choose from a wide range of authenticators (OTP, challenge/response, e-signature or PKI devices), both software and hardware-based, which best fit their needs. All DIGIPASS devices are fully customizable with your logo and corporate colors.

To view the complete DIGIPASS family, please visit www.vasco.com/digipass

**One-button devices**

The DIGIPASS GO family combines ultra-portability with user convenience. The OTP is generated at the push of the button.

<table>
<thead>
<tr>
<th>Key features</th>
<th>DIGIPASS GO 3</th>
<th>DIGIPASS GO 6</th>
<th>DIGIPASS GO 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Intuitive use</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Ultra-portable</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Time and event-based authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- DES/3DES/AES/OATH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Long lifetime battery</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**E-signature devices**

A range of small and user-friendly PIN-protected authentication devices.

<table>
<thead>
<tr>
<th>Key features</th>
<th>DIGIPASS 275</th>
<th>DIGIPASS 301cv</th>
<th>DIGIPASS 320</th>
<th>DIGIPASS 736</th>
<th>DIGIPASS 760</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Offers response only OTP, e-signature and challenge/response functionality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- PIN protection and PIN unlocking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Simple and intuitive in use</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Time/event and challenge/response based</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Long lifetime battery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Front-end**

**Card Readers**

A wide range of connected, unconnected and connectable card readers

<table>
<thead>
<tr>
<th>Key features</th>
<th>DIGIPASS 810</th>
<th>DIGIPASS 836</th>
<th>DIGIPASS 840 CV</th>
<th>DIGIPASS 905</th>
<th>DIGIPASS 920</th>
</tr>
</thead>
<tbody>
<tr>
<td>• No need to install drivers in unconnected mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Smart card based OTP, e-signature, PKI functionality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Straightforward deployment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Ease of use</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Leverage EMV or PKI cards deployment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• No personalization required</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Software DIGIPASS**

Software-based DIGIPASS solutions leverage mobile phones, tablet PCs or web-browsers for authentication purposes.

<table>
<thead>
<tr>
<th>Key features</th>
<th>Virtual DIGIPASS</th>
<th>DIGIPASS for Mobile</th>
<th>DIGIPASS Nano</th>
</tr>
</thead>
<tbody>
<tr>
<td>• OTP and e-signature capability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• No hardware deployment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Time and event-based authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• PIN-protected</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Transparent, user-friendly and ultra-portable</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PKI-based solutions**

VASCO’s PKI-offering consists of DIGIPASS CertiID™, a client-based software suite, and a range of DIGIPASS PKI devices, the DIGIPASS KEY range. DIGIPASS CertiID provides an answer to the growing need for digital signature solutions for high risk transactions and document signing. The DIGIPASS KEY range consists of smart card based solutions and USB devices.

<table>
<thead>
<tr>
<th>DIGIPASS CertiID</th>
<th>DIGIPASS KEY 101</th>
<th>DIGIPASS KEY 202</th>
<th>DIGIPASS KEY 860</th>
</tr>
</thead>
</table>

Building a secure banking environment
DIGIPASS for Application Perimeter Protection SDK (DIGIPASS for APPS) is a software development kit that provides application developers with a cross-platform programming environment to secure (mobile) applications.

**Strong authentication**

DIGIPASS for APPS offers a comprehensive set of modules giving you all necessary building blocks to secure your application at every level. The solution allows native integration of strong authentication with one-time passwords and e-signatures ensuring a secure login or transaction signing process. The solution supports the patented CrontoSign technology, VASCO’s visual transaction signing solution.

**Secure storage, secure channel, secure environment**

Additionally, DIGIPASS for APPS also offers unique features to secure the environment in which the application resides, such as jailbreak and rootkit detection and geolocation. The software development kit also provides secure storage as well as a secure channel to ensure end-to-end encryption of business critical data whereby relying on mainstream technologies like HTTPS may not be enough. The secure channel offered by DIGIPASS for APPS can virtually encrypt anything, such as texts, photos or QR codes.

**Full lifecycle management**

Furthermore, DIGIPASS for APPS enables application developers to streamline and manage the entire provisioning, deployment and lifecycle process offering several options for end user activation and device binding features that link a user to a specific device. The solution also foresees in the possibility for end users to use multiple devices for one application with a single license.

The solution is available for the most common programming environments, including iOS, BlackBerry, Android, Windows Phone, Java and Windows. DIGIPASS for APPS is fully customizable overcoming GUI issues and requires no cryptographic skills, reducing integration efforts.
IDENTIKEY Authentication Server

IDENTIKEY Authentication Server is VASCO’s off-the-shelf centralized authentication server. The solution offers strong authentication and validation of transaction signatures with support of EMV-CAP to address the need for e-signatures in commercial and banking web-based applications. IDENTIKEY Authentication Server Banking Edition is the complete and robust protection against man-in-the-middle (MITM) attacks.

IDENTIKEY Authentication Server is a perfect fit for banks wanting to implement a strong authentication solution without dedicating significant budget and resources or looking to avoid large integration projects. It is also suited for banks in need of a dedicated authentication server solution. With IDENTIKEY Authentication Server, financial organizations can offer strong authentication as an additional security layer to their complete range of banking services: retail banking, corporate banking, mobile banking, call center and others.

IDENTIKEY Authentication Server has been checked and tested according to the PCI-DSS compliancy regulations, so that the mandatory compliancy of any organization that integrates IDENTIKEY Authentication Server remains unchanged.

VACMAN Controller

VACMAN Controller is a state-of-the-art API-based authentication platform already integrated by a vast number of leading banks and financial institutions worldwide. It combines all authentication applications, including OTP, challenge/response and e-signature on a single platform. As such the solution gives banks the flexibility they desire to address specific user risk profiles.

VACMAN Controller is ideally suited for large deployments such as corporate and retail banking. Its unlimited scalability enables the processing of heavy volumes of authentication requests for millions of end users. The solution can be seamlessly integrated into any existing e-banking application, regardless of operating system or architecture in a time and cost-effective way. This versatility turns the implementation of a two-factor authentication solution into a hassle-free experience with minimal impact to existing infrastructures and operations.
FOCUS ON YOUR CORE BUSINESS.
OUTSOURCE AUTHENTICATION

The triumph of cloud computing

Cloud computing is the upcoming trend and will dominate the IT landscape for years to come. More flexibility, better scalability and lower costs. The arguments for cloud computing are hard to refute.

With VASCO’s cloud authentication platform MYDIGIPASS.COM, application service providers can 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 financial 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. Authentication becomes an operating expense rather than a capital expense, thus lowering the cost of deployment and enhancing the total cost of ownership. VASCO takes care of the entire authentication process for you: from deployment and administration to the authentication of your end users’ devices.

Ultimate user convenience

MYDIGIPASS.COM offers an ultimate user convenience, both to the application developer as the end user. Thanks to an in-the-cloud offering with a step-by-step integration procedure and by embracing the newest technologies, implementing MYDIGIPASS.COM into your mobile or online services offering becomes a breeze.

Equally convenient for end users, MYDIGIPASS.COM offers consumers different means of authenticating themselves on the platform, ranging from mobile applications that can be easily downloaded, to embedded chips on Intel ITP to hardware authenticators.

Native app integration

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. Previously, mobile app users needed to switch between the mobile application and a separate authentication app, in order to securely log on to the mobile app of their choice. This involved a cumbersome copy-paste process whereby users needed to open the MYDIGIPASS.COM authentication app, generate a strong password and consequently copy-paste this password into the mobile app to which they wanted to log on securely.

The native authentication integration solution now allows users to securely log on from a mobile app by simply clicking the ‘MYDIGIPASS.COM Secure Connect’ button. Users 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.
Up-to-date with latest security trends

New types of online attacks emerge almost every day. It is therefore critical for IT security professionals to stay informed and remain up-to-date on the latest trends. As a leading Internet security company VASCO considers it its duty to actively share information on current and emerging IT security trends and online fraud schemes with its customers, partners, distributors and resellers and anybody who needs our advice.

VASCO’s Security Experts Academy & e-Learning platform (SEAL)

SEAL is VASCO’s worldwide community of security professionals. The SEAL training offer consisting of general IT security topics and VASCO product trainings will help people looking to build a career in information security. Through our offering of classroom training, e-learning or DVD-based training and forums, VASCO SEAL allows you to:

- Become a VASCO Certified Engineer
- Stay up-to-date on the latest security trends
- Develop new skills in IT security
- Get access to a community with an extensive IT security knowledge base
- Exchange information with peers

If you are looking to extend your knowledge in the IT security field, you are welcome to join VASCO SEAL to become a security professional. SEAL courses are appropriate for sales professionals, product managers, support engineers, field engineers and security consultants.

SEAL offering

VASCO’s SEAL comprises the following:

- E-learning: more than 120 hours of web-based or DVD-based IT security training
- Classroom training by VASCO security experts
- VASCO Certification: SEAL training offers IT security professionals the opportunity to become VASCO Certified Engineers
- VASCO Authorized Training Centers: training by VASCO partners
- Junior Programs: trainee and scholarship programs for graduates

More information is available on: www.vasco.com/training
Building a secure banking environment

Fulfillment services

VASCO has built a wealth of experience and know-how about successful mass deployment of authentication projects. VASCO puts this expertise at its customers’ disposal allowing you to diversify your services from your competitors’, to focus on your core business and to lighten the supply chain burden.

- **Branding and customization:**
  Every DIGIPASS can be branded reflecting corporate colors and logos in order to enhance brand recognition for end-users

- **Customized packaging:**
  VASCO offers a wide range of packaging services, ranging from non-personalized individual or bulk packaging to fully customized and branded packaging

- **Refurbishment:**
  Tailor-made service offering to prolong DIGIPASS life-cycle and reduce the economical and ecological footprint of authentication investments

- **Distribution and storage:**
  VASCO can offer supply chain services, delivering orders anywhere in the world, to a central location, branch offices or to end users. We can also store customers’ stock in secure and adapted warehouses

Provisioning services

- **Hardware provisioning:**
  Security parameters can be personalized according to the requirements of corporate security departments. Secrets are stored in DIGIPASS hardware through an approved and audited process. Advanced encryption methods are used to communicate initial PINs and to unlock codes by corporate security departments.

- **Software provisioning:**
  For the provisioning of secrets on mobile phones or third party platforms VASCO offers an application provisioning service which takes deployment and management issues of software-based authentication out of your hands, allowing you to focus on your core business.
Security is a facilitator, not an obstacle

It is critical to businesses around the globe that their business applications are up-and-running at all times and securely accessible. To ensure authentication is not considered a burden but a facilitator, VASCO offers a wide range of support packages and technical support services for environments of all sizes and all types. We can simplify your life with rapid-response coverage around the world and flexible service plans to suit your needs and budget.

For all types of customers VASCO has a tailored answer ranging from basic support to dedicated SLA, ensuring rapid intervention around the globe.

Personalize your support experience with a variety of service options from VASCO. Discover which VASCO Technical Support Plan best fits your needs.

- Standard Support
- 24/7 support
- VIP support
- Pay-Per-Incident
- Remote Assistance Package
- Emergency Support

More detailed information on our support offering is available on: www.vasco.com/support
Professional Services

VASCO’s Professional Services have been designed to assist customers, resellers, partners and integrators in the deployment of their strong authentications projects. By sharing our expertise we help our customers to minimize the challenges and maximize the results of the authentication within time and budget. VASCO’s Professional Services bring many years of experience in the deployment of two-factor authentication projects to the table.

Our offering

Every authentication project is unique. Different customers have different needs. Whichever the driver to implement a strong authentication project, VASCO has the qualified engineers and project managers to turn the customer’s authentication project into a success.

Our Professional Services team will use the proven VASCO methodology in each authentication project. This methodology helps in:

- Defining the scope of the project
- Designing the appropriate solution
- Implementing the products and solutions
- Building applications meeting the customers need
- Supporting the customers partner of in-house team throughout the project
- Certifying the customers application according to the market standards
- Reviewing existing implementations and make recommendations for optimization

Benefits

- An experienced team
  Our experienced and certified engineers ensure seamless integration of authentication into existing applications or infrastructure, using the proven VASCO methodology

- Total cost of ownership
  Realization of projects on time and within budget

- Proven methodology
  Short term deployments, support throughout the project and enhanced security for remote access, LAN, online applications, e-banking and m-banking environments
Together with VASCO, we looked at different ways to use our DIGIPASS devices with VACMAN Controller. Their advice not only led to significant and important enhancements, but also to an overall improvement of our security features. VASCO brought a lot of value and expertise to our project and for this we consider them as a valuable business partner.

Daniel Ratinckx, Head of Delen-Online at Bank Delen
About VASCO

VASCO is a leading supplier of strong authentication and e-signature solutions and services specializing in Internet security applications and transactions. VASCO has positioned itself as global software company for Internet security and designs, develops, markets and supports DIGIPASS®, CertiID™, VACMAN®, IDENTIKEY® and aXsGUARD® authentication products. VASCO’s prime markets are the financial sector, enterprise security, e-commerce and e-government.

WWW.VASCO.COM

INTERNATIONAL HQ - Switzerland
phone: +41 43 555 35 00
email: info-europe@vasco.com

CORPORATE HQ - Chicago
phone: +1 630 932 8844
email: info-usa@vasco.com

Sales offices

Asia - Pacific - Singapore
phone: +65 6123 09 06
email: info-asia@vasco.com

Asia - Pacific - Japan
phone: +81 3 5532 7862
email: info-japan@vasco.com

Europe, Middle East, Africa - Wemmel
phone: +32.2.609.97.00
email: info-europe@vasco.com

USA - Boston
phone: +1 508 366 3400
email: info-usa@vasco.com

USA - California
phone: +1 650 378 1202
email: info-usa@vasco.com

Asia - Pacific - India
phone: +91 22 4090 7112-14
email: info-india@vasco.com

Europe, Middle East, Africa - Austria
phone: +43 1 9043132-0
email: info-europe@vasco.com

Australia - Sydney
phone: +61 2 8061 3700
email: info-australia@vasco.com

Latin America - Brazil
phone: +5511 3443 7541
email: E5-brazil@vasco.com

Asia - Pacific - Japan
phone: +32.2.609.97.00
email: info-europe@vasco.com

USA - California
phone: +1 650 378 1202
email: info-usa@vasco.com

Copyright © 2014 VASCO Data Security, Inc. VASCO Data Security International GmbH. All rights reserved. DIGIPASS®, CertiID™, VACMAN®, IDENTIKEY®, aXsGUARD®, and the VASCO® logo are registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH in the U.S. and other countries. VASCO Data Security, Inc. and/or VASCO Data Security International GmbH own or are licensed under all title, right and interest in VASCO Products, updates and upgrades thereof, including copyrights, patent rights, trade secret rights, mask work rights, database rights and all other intellectual and industrial property rights in the U.S. and other countries. Other names may be trademarks of their respective owners.