We authenticate the world
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 our 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.
Products and markets

**VASCO’s product lines**

**VACMAN®**
Back-end core authentication platform suited for massive deployments

**IDENTIKEY® Authentication Server**
Centralized authentication server suited for organizations of all sizes

**IDENTIKEY® Federation Server**
IDENTIKEY access management platform. Validation of user credentials across multiple applications and disparate networks

**IDENTIKEY® Appliance**
Dedicated IDENTIKEY authentication plug-and-play appliance for medium to large enterprises

**aXsGUARD® Gatekeeper**
Stand-alone authentication appliances for remote access and Internet security

**DIGIPASS® as a Service**
Cloud-based authentication in a managed service model

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

**Embedded and OEM Solutions**
Embedded security to authenticate the world’s online community

**Target markets**

**Online banking security**
Account and transaction security for e-banking and m-banking

**Online application security**
Secure log-on to mission-critical applications (portals, SaaS, e-commerce, e-gaming, cloud applications, ...)

**Enterprise security**
- Secure remote access for your customers, partners and (mobile) workforce
- Corporate network security
- Secured web applications

**E-government**
User authentication to secure government applications accelerating delivery of online services
Secure online banking

A secure online banking experience

Banks worldwide are increasingly providing 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. However, online banking has its drawbacks.

Online banking accounts are frequently targeted by cybercriminals and fraud schemes become more complex. Security issues remain a major concern for customers and corporations alike. 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 channels. As 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 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 and end-user devices ranging from software and hardware OTP authenticators to e-signature devices for transaction validation and digital signatures using PKI technology.

VASCO’s authentication solutions that suit your needs

Back-end:

- VACMAN Controller
  VASCO’s core authentication technology suited for large deployments
- IDENTIKEY Authentication Server
  Centralized authentication server for smaller and mid-sized banks looking for short deployment cycles. IDENTIKEY Authentication Server Banking Edition is a complete solution against MITM attacks
- DIGIPASS as a Service
  Cloud-based authentication in a managed service offering

User-end:

- DIGIPASS family
  Range of over 100 different authentication devices including one-button and PIN-pad devices, (EMV CAP) card readers and software-based solutions
- DIGIPASS CertiID™
  VASCO’s client-based PKI solution for strong user authentication and transaction signing
We Authenticate the World

HSBC Bank Brazil provides m-banking using VASCO’s DIGIPASS for Mobile

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 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.

Customer references

Oman Arab Bank provides secure e-banking services with DIGIPASS technology to prevent identity theft

Oman Arab Bank provides secure e-banking services with DIGIPASS technology to prevent identity theft. The bank implemented VASCO’s renowned DIGIPASS technology, including IDENTIKEY Authentication Server and IDENTIKEY Authentication Server, which could be perfectly integrated into the bank’s infrastructure. Oman Arab Bank used these technologies 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.

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.

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.

DIGIPASS 275 was selected in order to give the end user the possibility to choose his preferred authentication tool. DIGIPASS 275 can generate OTPs and has an e-signature functionality, so user authentication and electronic signing can be executed by the same device.

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.

DIGIPASS 275 was selected in order to give the end user the possibility to choose his preferred authentication tool. DIGIPASS 275 can generate OTPs and has an e-signature functionality, so user authentication and electronic signing can be executed by the same device.
Secure remote access

Protecting your corporate resources and confidential data is essential for every organization. Secure remote access to networks and business-critical information has become a necessity for companies worldwide as workforces are more dispersed and become increasingly more mobile.

Accessing corporate resources anywhere at any time poses real challenges for data security, a trend which is only accelerated by the exponential adoption of mobile devices such as smart phones, tablets and palm tops.

Aside from rethinking company security policies and infrastructural changes, one must also keep the end-user in mind. The key is to implement an adequate security solution without compromising on user-friendliness and efficiency.

Dynamic passwords and digital signatures

VASCO Data Security, world leader in authentication solutions and services, provides companies of all sizes with the most advanced solutions to meet their security needs.

With its DIGIPASS technology, VASCO brings banking level security to the enterprise market by replacing weak static passwords by dynamic one-time passwords (OTP), eliminating risks of unauthorized access to your network, application and data.

DIGIPASS can be used to securely log-on to the corporate network as well as for Windows Logon, Outlook Web Access and Citrix among others.

Online transactions or confidential documents can be secured with an electronic or digital signature ensuring that information is not altered in transit.

VASCO’s authentication solutions that suit your needs

For SMEs

- DIGIPASS Pack for Remote Authentication
  An out-of-the-box solution for secure remote access including server software and end-user authenticators

For companies of all sizes

Back-end:

- aXsGUARD Gatekeeper
  A comprehensive UTM solution for secure remote access
- IDENTIKEY Authentication Server
  Centralized authentication server available in four different packages for Enterprise use
- IDENTIKEY Appliance
  A dedicated authentication appliance for medium to large enterprises
- IDENTIKEY Federation Server
  Identity and access management platform to validate user credentials across multiple applications and disparate networks
- DIGIPASS as a Service
  Cloud-based authentication in a managed service offering

User-end:

- DIGIPASS family
  Range of over 100 different authentication devices including one-button and PIN-pad devices, card readers and software-based solutions
- DIGIPASS CertiID™
  VASCO’s client-based PKI solution for file and disk encryption, document, e-mail and transaction signing
Customer references

Stageco builds redundant network for its branch offices with aXsGUARD Gatekeeper

Stageco is an international staging company that builds and designs standardized and custom-made stages and structures for some of the most famous artists. The group has employees in nine offices worldwide that need to keep track of the logistic process for every event. Plagued by unstable VPN-connections and outages, the company decided to build a redundant network by creating e-tunnels with VASCO’s aXsGUARD Gatekeeper.

By installing a second aXsGUARD appliance, Stageco was able to create the so called e-tunnels, ensuring a fast, stable and redundant connection to the network and stock database for its remote offices. The solution also enables single sign-on resulting in a far more efficient and user-friendly way of working.

Galapagos secures business assets, network and VPN with aXsGUARD Gatekeeper

Galapagos is a European-based biotechnology company specialized in the discovery and development of drugs for the treatment of bone and joint diseases. To secure business-critical data, the company wanted to implement a comprehensive security solution for its network, VPN, website and e-mail traffic.

Stability and support were decisive factors, considering Galapagos’ limited IT resources. Secure remote access to the corporate network was also considered a must. aXsGUARD Gatekeeper was one of the few solutions that could be completely integrated into the company’s existing infrastructure. Since the implementation of aXsGUARD Gatekeeper, downtime is non-existent and rendered support is excellent. Galapagos’ employees and external researchers can access the company’s corporate network securely from anywhere in the world.

Global Radio secures remote access and develops a long-term security policy with strong authentication

Global Radio is UK’s largest commercial radio company and the home of many leading commercial radio brands. With more than 50 locations across the country and over 18.5 million listeners on air, Global Radio covers almost every genre and geographical area in the UK. When searching for a strong authentication solution to secure remote access for its website content editors, Global Radio opted for VASCO’s DIGIPASS for Mobile in combination with Virtual DIGIPASS and DIGIPASS GO 3, and IDENTIKEY Authentication Server Enterprise Edition at the back-end. VASCO’s solutions were not only able to tackle occurring security challenges, but also fitted ideally in the company’s long-term security development policy.
Security as competitive advantage

Security is an all important concern for application providers and its users alike; even more so now that applications are frequently more accessible over the internet, networks and mobile devices.

Most online applications are protected by default with a username and static password combination. Static passwords however can easily be intercepted and no longer offer sufficient protection.

Application providers want to protect the data contained within their application from being compromised and by extension their customers. They need to sidestep security issues and take countermeasures against fraud and data theft if they want to build and retain customer trust and avoid credibility and revenue loss.

Integrated security

VASCO’s strong authentication solutions are designed to address security issues associated with online applications and to combat fraud and various attacks without compromising user-friendliness. Solutions include both active and passive authentication and can be delivered via hardware, software and mobile devices. Strong authentication can be deployed for any kind of online application such as e-brokerage, insurances, e-commerce, e-gaming, e-health solutions, CRM, ERP, payroll applications, SaaS applications and many others.

VASCO’s back-end authentication solutions allow online application providers to integrate strong authentication and license protection directly into the application. They provide an ideal solution for any provider that has the business aspiration to acquire and manage millions of users.

VASCO’s authentication solutions that suit your needs

**Back-end:**
- **VACMAN Controller**
  VASCO’s core authentication technology suited for large deployments for a variety of customer facing applications in different verticals - including online gaming, e-commerce, CRM, ERP, web portals...
- **IDENTIKEY Authentication Server**
  Centralized authentication server to enhance the security of your web applications
- **IDENTIKEY Federation Server**
  Identity and access management platform to validate user credentials across multiple applications and disparate networks
- **DIGIPASS as a Service**
  Cloud-based authentication in a managed service offering

**User-end:**
- **DIGIPASS family**
  Range of over 100 different authentication devices including one-button and PIN-pad devices, card readers and software-based solutions
- **DIGIPASS CertiID™**
  VASCO’s client-based PKI solution for file and disk encryption; document, e-mail and transaction signing
We Authenticate the World

Customer references

HARIBO Italia secures confidential information of its CRM program with DIGIPASS and IDENTIKEY

HARIBO Italia, the Italian subsidiary of the multinational company HARIBO, is Italy’s leading supplier of gums and jellies. In order to manage its sales contacts and information, the company’s sales agents use an in the cloud CRM program. User-friendliness was of crucial importance. HARIBO’s sales agents should not perceive the solution as an obstacle. A limited deployment cost and a low impact on the existing IT-infrastructure were additional deciding factors.

HARIBO deployed VASCO’s DIGIPASS technology and IDENTIKEY Authentication Server. The company’s fifty-five sales agents, spread all over the Italian territory, can now use DIGIPASS GO 6 together with the Barracuda SSL-VPN solution, to securely and remotely access the CRM program.

Online game operators trust VASCO’s solutions to secure users’ accounts

To secure end-users’ gaming accounts from being stripped by fraudsters, online game operators implemented a solution which can simultaneously process login requests of more than hundred thousands of players and which is user-friendly at the same time. The solution must also reflect the gaming company’s identity by incorporating logos and images to enhance the brand recognition.

DIGIPASS GO 6 in combination with VACMAN Controller offers strong authentication securing remote access to the game without the need of installing additional software on the PC. DIGIPASS GO 6 is user-friendly, portable and can be used as a marketing tool since its casing is fully customizable and can reflect corporate branding.

Cardinal IP: a SaaS-application to manage Intellectual Property Assets secured by DIGIPASS

Cardinal IP is a global leader in patent research. Confidentiality and security are extremely important when protecting customer’s intellectual property data and research. Cardinal IP needed to implement a cost-effective and scalable technology to secure access to the corporate extranet and its SaaS solution ‘IP Dashboard’ with a security level compliant with the FISMA requirements. The security solution had to be fully integrated into Cardinal IP’s custom-built web-based applications and the corporate extranet and yet had to remain manageable and ensure a high level of user acceptance.

VACMAN and DIGIPASS technology were integrated into Cardinal IP’s web applications and extranet using ASP.NET and SQL Server tool. This ensures that all employees and customers accessing the corporate network and applications are properly authenticated. Because no additional software needs to be installed on the end-users’ computers, VASCO’s authentication solution was cost-effective and readily accepted by Cardinal IP’s employees and customers alike.
As e-gov booms, security is essential

Governments around the world adopt e-government strategies to offer citizens an increased portfolio of public services. The implementation of e-government has significant benefits: procedures are simplified, paperwork is reduced, services are accessible outside business hours; all resulting in a cheaper, more efficient and convenient delivery of information and services.

At the same time, privacy and data concerns have soared. Citizens need to confide in the fact that data and credentials are protected and can be exchanged in a secure environment.

Governments need to ensure that critical data and applications related to national security, public services, taxation and revenue, healthcare etc. are adequately secured. They should be vigilant to take essential security measures to address these challenges. Additionally, government applications and data need to adhere to compliancy rules set in international standards for secure online access to government systems and bodies.

OTP and PKI technology enhance security

VASCO’s two-factor authentication solutions provide end-user authentication to ensure secure remote access, eliminating weaknesses commonly associated with static passwords. Our PKI solutions offer governmental bodies and institutions a secure PKI environment for transaction and online document signing ensuring integrity and non-repudiation of data.

VASCO’s electronic ID card readers allow citizens to access online applications and request online documents at any time. Enterprises can use VASCO’s eID card readers to link applications to a specific ID ensuring authorized access.

DIGIPASS eID card readers are available in connected, connectable and unconnected mode. Unconnected devices read the data contained in the chip of the card and generate OTPs for secure log-on to applications, mail or networks. Connected card readers can be linked to specific applications and allow users to access authentication and signatures certificates stored on the chip.

VASCO’s authentication solutions that suit your needs

**Back-end:**
- **VACMAN Controller**
  VASCO’s core authentication technology suited for deployments with a large number of end-users
- **IDENTIKEY Authentication Server**
  Centralized authentication server that enhances remote access and application security
- **IDENTIKEY Appliance**
  A dedicated authentication appliance
- **aXsGUARD Gatekeeper**
  A comprehensive UTM-solution for secure remote access

**User-end:**
- **DIGIPASS family**
  Range of over 100 different authentication devices including one-button and PIN-pad devices, card readers and software-based solutions
- **DIGIPASS eID card readers**
  Connected, connectable and unconnected electronic identity card readers
- **DIGIPASS CertiID™**
  VASCO’s client-based PKI solution for strong user authentication, file and disk encryption, secure mail exchange and document and transaction signing
VASCO’s DIGIPASS 820 eID reader is easy to put away in a police uniform thanks to its convenient flat design. It can also be used in all weather conditions, as the eID reader is shock proof and is protected against dust and liquids by its rubber key pad. The high ease of use permits the police officers to check a citizen’s address information in seconds.
Authenticate the online community

DIGIPASS embedded and OEM solutions are VASCO’s response to the changing authentication market. It is a proof of VASCO’s commitment to find more convenient, portable and cost-effective ways to secure the online community. VASCO strives to develop authentication solutions that can operate on any platform and are suited to secure any application.

OEM solutions

VASCO develops practical security solutions that balance cost, security and convenience for every customer. VASCO’s DIGIPASS family was designed to run on one single infrastructure and all different form factors are interoperable with each other.

This allows VASCO partners to add strong authentication to their offering without major investments or disruptions to their businesses. As authentication becomes a crucial element in every security infrastructure, VASCO’s product portfolio provides organizations with a unique competitive advantage that could lead to increased market share and revenue. As our solutions are so versatile, they can meet the demands of any customer.

Embedded security solutions

VASCO’s mission with its DIGIPASS Embedded Security Solutions (DESS) is to enable DIGIPASS technology on client devices and applications; whatever these may be. Dormant DIGIPASS are embedded into products of leading vendors, bringing authentication within everyone’s reach.

This process shifts the authentication paradigm: rather than distribute security devices to end-users, VASCO simply provisions that security to a device the end-user already has.

DIGIPASS Embedded Security Solutions challenge the belief that increased user convenience automatically entails on decreased cost but also in diminished security. With an embedded approach, costs are inherently lower. The equation hence changes from having to sacrifice security for the sake of cost or convenience to one where security becomes the cornerstone of any online application.

Opportunities for DIGIPASS embedded security include:

- Computer platforms
- Mobile platforms
- Existing security credentials and smart cards
- USB/SD/MMC/SIM or other memory devices or cards
- Security software

Dormant DIGIPASS are embedded into products of leading vendors, bringing authentication within everyone’s reach.
Cloud-based 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.

VASCO offers DIGIPASS as a Service, a fully outsourced authentication model. It has been designed for application service providers wanting to add strong authentication to protect their content, data and applications.

DIGIPASS as a Service overcomes a number of issues commonly associated with the deployment of a two-factor authentication solution. Native integration of strong authentication might require infrastructural changes. Additionally, deploying two-factor authentication to a large number of end-users might be considered costly and time-consuming. Logistic burdens, portability of authentication devices, multiple authenticators for different applications, the installation of software on the end-user’s PC, associated administration... the hurdles are plentiful.

Authentication from A to Z

DIGIPASS as a Service overcomes these apprehensions; 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.

Furthermore, with VASCO’s DIGIPASS Plus devices, multiple authenticators for different applications belong to the past. DIGIPASS Plus devices possess a second identity enabling end-users to use one DIGIPASS device for several applications. Together with VASCO’s DESS strategy, we bring authentication within everyone’s reach. DIGIPASS as a Service allows organizations and application providers to focus on their core competencies without worrying about security issues.

MYDIGIPASS.COM

MYDIGIPASS.COM is an online platform that allows web application owners to facilitate password management while adding an additional level of security to the access log-on procedure. VASCO allows website owners to freely integrate strong authentication using DIGIPASS one-time passwords on their site for-end users to secure access to their services and content.

Website owners can boost customer trust by providing secure single sign-on for all applications connected to the platform. Additionally, back-office and support costs can be reduced by eliminating costs associated with password management.

End-users in turn can conveniently and securely access their applications through the MYDIGIPASS.COM portal using VASCO’s DIGIPASS technology. To generate a one-time password to log on to the platform, they can use one of the hundred million dormant DIGIPASS in the field or download a mobile client on MYDIGIPASS.COM free of charge.
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. VASCO's mission is to provide IT security professionals with the knowledge necessary to safeguard their clients from cyber threats.

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

SEAL is VASCO's worldwide community of security professionals. The SEAL training offering consists of general IT security topics and VASCO product trainings that 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
Security is a facilitator, not an obstacle

It is critical to organizations 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

Support offering

VASCO has a support offering specified per user type:

- Banking and application security customers can choose from a number of standardized support packages ranging from standard support during business hours, 24/7 support, service level agreement (SLA) based support, pay-per-incident and remote assistance support
- For enterprise security customers, technical support is provided through the reseller or system integrator. Direct technical support provided by VASCO is available upon request
- VASCO distributors, system integrators and certified engineers benefit from a standard technical support during business hours
- For VASCO resellers, technical support is provided through the distributor. Direct technical support provided by VASCO is available upon request

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 solution, VASCO has the qualified engineers and project managers to turn your authentication project into a success.

Our Professional services team will use the proven VASCO methodology:

- Define the scope of the project
- Design the appropriate solution
- Implement the products and solutions
- Build applications to meet the customer’s needs
- Support the customer’s partner or in-house team throughout the project
- Certify the customer’s application according to market standards
- Review 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 the 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
We Authenticate the World
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 Ratincx, Head of Delen-Online at Bank Delen
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 customer’s 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.
Extensive distributor and reseller network

VASCO works closely together with over 400 channel partners and system integrators around the globe. VASCO’s channel partner program provides the channel partners with:

- Commercial and marketing support including: commercial briefings, newsletters, pre-sales support and presentations, lead generation, demonstrations, product specific marketing documentation, joint marketing campaigns, mailings and events and access to the partner extranet

- Technical support and cooperation with VASCO’s Technical Account Managers to help negotiate major contracts

- Training and certification to assist channel partners in full understanding of the product line

- Resources to leverage strategic relationships: benefit from VASCO’s partnership with other technology vendors such as Novell, Citrix, Check Point, Cisco,…

Solution partners

VASCO has developed a DIGIPASS Ready Partner Program to facilitate the compatibility of solutions from other technology vendors with VASCO’s DIGIPASS. Solution partners are able to either bundle their solutions with VASCO’s solutions or develop new solutions based on the combined product offering.

Solution partners benefit from a number of partner advantages including web presence, VASCO training, co-marketing initiatives, sales and technical support and event participation.

Customers benefit from easier and less costly integrations as they are able to leverage their authentication investments. By using the authentication infrastructure and the DIGIPASS they already have for multiple applications (remote access, application security, disc encryption, …) the customer receives a higher return-on-investment.

For a full overview of the VASCO partners: www.vasco.com/solutions/partners
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 a 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
e-mail: info-europe@vasco.com

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

Sales offices

Asia - Pacific - Singapore
phone: +65 6233 09 06
e-mail: info-asia@vasco.com

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

Latin America - Brazil
phone: +55 11 3443 7541
e-mail: E5-brazil@vasco.com

Asia - Pacific - Japan
phone: +61 3 5532 7862
e-mail: info-japan@vasco.com

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

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

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

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

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

Copyright © 2014 VASCO Data Security, Inc. VASCO Data Security International GmbH. All rights reserved. VASCO®, CertiID™, VACMAN®, IDENTIKEY®, aXsGUARD®, DIGIPASS® 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, rights 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.