Secure your business

The world’s leading software company specializing in Internet Security
We authenticate the World

VASCO® is a leading supplier of strong authentication and e-signature solutions and services specializing in Internet security. Every day, VASCO helps customers around the globe to deploy strong authentication solutions. We have customers in over 100 countries that use VASCO products to secure many different applications and online transactions.

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.
A secure working environment

It is evident that corporate assets have to be protected against malicious attacks from cybercriminals. If this information should ever fall into the wrong hands, consequences may be severe and could even result in a lawsuit or damaged corporate reputation.

For application providers it is also of paramount importance to implement adequate security measures to secure their customers data and identity. In case of data or identity theft, customers could lose confidence in the online service which ultimately may lead to revenue loss.

Traditional static passwords are commonly used to protect content and credentials. However, they don’t offer sufficient protection against malicious attacks and fraudsters as they can be easily obtained. Organizations must seek a fine balance between security, cost and user-friendliness when implementing adequate security solutions. VASCO Data Security, world leader in authentication solutions and services, helps organizations worldwide to seek the best security solution to suit their needs.

The security challenge solved

VASCO provides companies of all sizes with the utmost 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), e-signatures and digital signatures and thus eliminating risks of unauthorized access to your network, applications and data.

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 SMEs with tailored solutions. 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.

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

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

Embedded and OEM Solutions
Embedded security to authenticate the world’s online community
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 and 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. The key is to implement an adequate security solution without compromising on user-friendliness and efficiency.

With a single DIGIPASS authenticator, you can protect access to all your resources and applications. Employees can remotely log on to the corporate network, and at the same time, use DIGIPASS for Windows Logon, Outlook Web Access, or Citrix. Whether you want to secure access to your CRM, ERP, payroll, or SaaS application: your employees will be able to securely log on to all business applications with only one DIGIPASS.

Desktop security

The reasons for strong authentication are clear, but companies sometimes happen to lack the possibility to deploy hardware or mobile authentication devices.

DIGIPASS for Windows is designed to secure networks and applications when these difficulties show up. DIGIPASS for Windows offers companies of all sizes a cost-effective way of protecting their Windows PCs connected to the corporate network against unauthorized access.

DIGIPASS for Windows is very straightforward in use. The application resides on the end-user’s desktop, and a one-time password (OTP) will be generated after PIN-code insertion. Once your OTP has been generated, you can click ‘next’ and can immediately access the application. DIGIPASS for Windows also calculates e-signatures using transaction data.

It is the ideal solution for companies that consider the transparent deployment to the end-user as the major hurdle for rolling out two-factor authentication.
Journalists and home workers at De Persgroep have secure remote access to SLI/VPN Platform

De Persgroep is a leading publisher on both the Belgian and Dutch market. Its journalists and employees need the possibility to remotely log on to the corporate network 24/7. The company looked for a solution that had a low cost per user without impacting the security level. Moreover, it had to be integrated into the existing LDAP Active Directory environment.

De Persgroep found the ideal solution in the combination of DIGIPASS GO 6 and IDENTIKEY Authentication Server, with a competitive price-quality ratio to secure remote access to its SLI/VPN platform in a uniform way. IDENTIKEY Authentication Server could easily be integrated into the existing network environment. DIGIPASS GO 6 was praised because of its user-friendliness, robustness and compactness, which are great advantages regarding the extreme circumstances journalists sometimes work in.

Sony Entertainment Television implements DIGIPASS into its SLI/VPN solution to secure remote access

Sony Pictures Television International (SPTI) backs Multi Screen Media Private Limited (MSM), which is among the region’s leading television channel operators in India. The company deployed an in-house SLI/VPN solution allowing IT staff and travelling employees to remotely access corporate resources and applications. The company wanted to add an extra security layer, compliant with its SLI/VPN solution by implementing some form of authentication. Moreover, the authentication process needed to be straightforward ensuring high user-acceptance.

To ensure access for authorized staff only, Sony Entertainment Television implemented VASCO’s two-factor authentication technology, bypassing the weaknesses of traditional static passwords. VASCO’s DIGIPASS technology combined with the VACMAN software suite, allowed MSM to secure its SLI/VPN solution in a very cost-effective manner. The authentication solution was seamlessly integrated into the existing back-end infrastructure using RADIUS protocol. Employees can now securely access the corporate network and its applications anywhere, anytime using DIGIPASS GO 6.

AMSANT secures e-health records in remote Australia with DIGIPASS

The Aboriginal Medical Service Alliance Northern Territory (AMSANT) is the peak body for Aboriginal community controlled health services in the Northern Territory in Australia. The organization provides advocacy and support services to its 26 independent members who provide primary health care services to Aboriginal people. To assist its members, AMSANT developed a shared IT infrastructure, enabling health care providers in very remote areas to access their applications and sensitive medical records anywhere, anytime. An easy to manage security solution to secure these applications and the patients’ health records was needed.

Each health worker is now provided with a portable, personalized authentication device, namely DIGIPASS 860, as the key to access patient data and relevant programs. This hybrid security device supports both PKI and one-time password generation in one single product. Once the password has been validated, health care professionals can access patients’ medical records online. Moreover, the USB-stick on DIGIPASS 860 gives them added flexibility, as they can log on and use their DIGIPASS to move from one consulting room to another, without losing their computing session.
Security as a 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 through the internet, networks and mobile devices.

Most online applications are by default protected 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. By extension, also the customers are protected. 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.

License protection

A common problem facing online application vendors and service providers is the sharing of user accounts, which can result in revenue losses and potential security threats. DIGIPASS License Protection is engineered to help online application providers address these problems in two ways. On the one hand, it secures the end-user and his credentials. On the other hand, it ensures that only properly authenticated users can gain access to online accounts. Hence authentication is not only a guard against end-user security breaches; it is also an invaluable tool in the protection and retention of revenue.

Document security

When conducted through unsecured electronic channels, the transaction of financial information and the endorsement of legally binding documents can result in considerable financial loss and diminished customer confidence. VASCO’s e-signature solutions help eliminate these security threats, providing electronic confirmation of authenticity and integrity for documents and financial transactions across all industries. If documents should be altered in transit, the e-signature will be rendered invalid.

Digital signatures go one step further and provide non-repudiation besides integrity and authenticity. Digital signatures or a Public Key Infrastructure (PKI) allows enterprises to sign transactions and documents with the approval of certificates and keys.

VASCO’s PKI-offering consists of DIGIPASS CertiID and DIGIPASS Key Devices. This first one is a client-based software suite and provides an answer to the growing need for digital signature solutions for high risk transactions and document signing. The latter include a range of DIGIPASS Key devices, that consist of smart card based solutions and USB devices.
HARIBO Italia secures confidential information of its CRM program with DIGIPASS and IDENTIKEY Authentication Server

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.

DIGIPASS GO 3 guarantees secure access to purchasing and invoicing application

Vocational Education Committees (VECs) are statutory local education bodies in the Republic of Ireland. They provide integrated education services enabling young people and adults to fulfill their potential in a positive learning environment. It prepares students for careers related to a specific trade or vocation outside the academic sphere, such as childcare, furniture design or tourism. To facilitate their purchasing/invoicing process, the VECs turned to Document Centric Solutions to implement a web-based solution.

Document Centric Solutions, specialized in electronic document management solutions, presented an online purchasing/invoicing application. In order to secure remote access, VASCO’s DIGIPASS GO 3 in combination with VACMAN Server was deployed.

Confidentiality of electronic medical files in Promedico ASP guaranteed by DIGIPASS

Promedico ICT Ltd. is a leading company offering ICT-solutions for healthcare. It introduced Promedico ASP, an online software application enabling general practitioners and other healthcare professionals to access, share and exchange their patients’ medical records. Security and confidentiality remain big issues when it comes to sharing patients’ medical records.

Access to the patients’ medical files in Promedico is secured by VASCO’s DIGIPASS 300 in combination with VACMAN Controller. DIGIPASS 300 has an e-signature functionality, allowing general practitioners to sign their messages and update their patients’ records in a secure way.
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 decreased costs but also 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 corner stone 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.
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.
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, to best fit their needs. All DIGIPASS devices are fully customizable with your company’s logo and corporate colors.

To view the complete DIGIPASS family, please visit [www.vasco.com/DIGIPASS](http://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>

### PIN-pad devices

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

<table>
<thead>
<tr>
<th>Key features</th>
<th>DIGIPASS 260</th>
<th>DIGIPASS 270</th>
<th>DIGIPASS 301cv</th>
<th>DIGIPASS 736</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>
</tr>
<tr>
<td>• PIN protection and PIN unlocking</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>
</tr>
<tr>
<td>• Time/event and challenge/ response based</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Long lifetime battery</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Card Readers

A wide range of connected, unconnected and connectable card readers.

**Key features**

<table>
<thead>
<tr>
<th></th>
<th>DIGIPASS 835</th>
<th>DIGIPASS 836</th>
<th>DIGIPASS 865</th>
<th>DIGIPASS 905</th>
</tr>
</thead>
<tbody>
<tr>
<td>No need to install drivers in unconnected mode</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>
</tr>
<tr>
<td>Straightforward deployment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ease of use</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>
</tr>
<tr>
<td>No personalization required</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.

**Key features**

<table>
<thead>
<tr>
<th></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.
IDENTIKEY Authentication Server

IDENTIKEY Authentication Server is VASCO’s off-the-shelf centralized authentication server. It is the perfect choice to secure remote access to corporate resources and various types of (web-based) applications, from remote access and SSL/VPN to SaaS. IDENTIKEY Authentication Server verifies the authentication requests from individuals trying to access applications and centrally administers user authentication policies. Authentication and transaction validation functions can be integrated into existing web-based applications, using a built-in SOAP API. One DIGIPASS device can therefore be used to secure several applications.

IDENTIKEY Federation Server

IDENTIKEY Federation Server is a server appliance providing you with the most powerful identity and access management platform. It is used to validate user credentials across multiple applications and disparate networks. The solution validates users and creates an identity ticket enabling web single sign-on for different applications across organizational boundaries. As validated credentials can be reused, once a user’s identity is confirmed, access to authorized services and applications is granted.

IDENTIKEY Appliance

IDENTIKEY Appliance is designed as a convenience layer around VASCO’s IDENTIKEY Authentication Server, giving organizations the option of running their authentication server separate from all other systems and applications. Some organizations prefer this setup for security reasons or for the sake of minimizing implementation resources. Other companies choose this option to avoid sharing resources among crucial applications, opting instead for several dedicated appliances. IDENTIKEY Appliance is a plug-and-play solution that can easily be installed, all without impacting the performance of existing systems and applications.

VACMAN Controller

VACMAN Controller is a state-of-the-art API-based authentication platform that serves as a back-end for DIGIPASS strong authentication. It automatically processes login requests to ensure only properly authenticated users obtain access to protected online applications. A unique design, unlimited scalability and versatile flexibility, make VACMAN Controller a perfect fit for large deployments in a variety of customer interfacing applications.

DIGIPASS CertiID

DIGIPASS CertiID is a client-based software suite that combines PKI and OTP technology. The software suite was designed for users unfamiliar with PKI technology. DIGIPASS CertiID is installed on the PC of the end-user and is used in conjunction with a DIGIPASS KEY solution - the authentication device.

PKI technology can be used to digitally sign transactions. When an end-user initially requests a certificate, a private key is stored on the (integrated) smart card of the authentication device. This private key can never be exported, leveraging security. To activate the device, the user must enter his PIN code.
DIGIPASS Pack for Remote Authentication

VASCO’s DIGIPASS Pack for Remote Authentication is an out-of-the-box solution, specifically designed for small and medium size businesses. The box contains all necessary hardware and software to provide a high level of security to organizations with limited resources and budgets. Based on proven one-time password technology, DIGIPASS ensures that only authorized users gain access to your corporate resources and applications. DIGIPASS Pack for Remote Authentication is available in packs for 5, 10, 25 or 50 users; allowing swift expansion when the need arises.

The Standard Edition

This includes RADIUS functionality for a single licensed server. This pack targets SMBs that want to protect their remote access infrastructure at the lowest total cost of ownership. This offering is available with DIGIPASS GO 6 one-button authenticators or DIGIPASS for Mobile.

The Gold Edition

The Gold Edition offers web filters to secure Outlook Web Access and Citrix Web Interface in addition to RADIUS support. DIGIPASS Pack Gold Edition includes licenses for a primary and back-up server. It is an ideal solution for SMBs that want to secure additional in-house applications and/or additional user groups on top of their remote access infrastructure.

The Platinum Edition

The Platinum Edition addresses security needs of companies wanting to protect both external and internal access to the corporate network. It also contains DIGIPASS authentication for Windows Logon allowing your users to log-on to Windows desktop and the network with a DIGIPASS generated dynamic password. DIGIPASS Pack Platinum Edition includes licenses for a primary and back-up server.
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

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](http://www.vasco.com/support)
DIGIPASS Ready Partner program

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 or develop new ones based on the combined product offering.

Enterprises can benefit from easier and less costly integrations or leverage their authentication investments. By using the authentication infrastructure and DIGIPASS for multiple applications (remote access, application security, disc encryption, ...), higher return-on-investment is obtained.

Together with our solution partners, we offer solid and proven solutions, resulting in a wide array of benefits.

- Expand market reach
  The joint solution will be announced to all of our account and channel managers via regional or global sales meetings, conference calls, webex sessions, e-mails and on our corporate website. This will enable all of our sales and pre-sales people to pitch the joint solution to their customers and prospects.

- Improve visibility
  DIGIPASS Ready partners will be invited to participate as exhibitors or sponsors of VASCO events, seminars, summits and trade shows. These events will increase visibility of products and solutions and will allow you to network with (channel) partners, VASCO employees, customers and prospects. A range of collateral will be created, thereby promoting and enforcing the strength of our joint offer.

- Create new solutions
  You will be invited to join VASCO for sneak previews of new product announcements and attend VASCO technical workshops.

- Extend your product value and interoperability
  Use the DIGIPASS Ready and VASCO logo as a differentiator to assure your customers and prospects that your products and solutions are interoperable with VASCO’s product and solution suite.

- Support from dedicated technical contact
  Through a dedicated contact with presales and technical knowledge for the solution, we are able to position the joint solution in a most advantageous manner for both prospects and sales.

DIGIPASS Plug-ins

VASCO also offers a full range of integrated solutions for Novell NIMAS, Lotus Domino, AEP (Netilla), Imprivata, Juniper (FUNK), etc. DIGIPASS Plug-ins ensure the native integration of two-factor authentication into partner solutions. As a result, the native features of the existing system or application (scalability, load-balancing, delegated administration) are maintained without having to add additional server hardware.

For a full overview of the DIGIPASS Plug-ins: www.vasco.com/solutionpartners
# 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.

---

**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.

---

**Sales offices**

<table>
<thead>
<tr>
<th>Region</th>
<th>Country</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia-Pacific</td>
<td>Singapore</td>
<td>+65 6123 09 06</td>
<td><a href="mailto:info-asia@vasco.com">info-asia@vasco.com</a></td>
</tr>
<tr>
<td>Australia</td>
<td>Sydney</td>
<td>+61 2 8061 3700</td>
<td><a href="mailto:info-australia@vasco.com">info-australia@vasco.com</a></td>
</tr>
<tr>
<td>Latin America</td>
<td>Brazil</td>
<td>+5511 3443 7541</td>
<td><a href="mailto:E5-brazil@vasco.com">E5-brazil@vasco.com</a></td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>Japan</td>
<td>+61 3 5532 7862</td>
<td><a href="mailto:info-japan@vasco.com">info-japan@vasco.com</a></td>
</tr>
<tr>
<td>Europe, Middle</td>
<td>Africa, Wemmel</td>
<td>+32.2.609.97.00</td>
<td><a href="mailto:info-europe@vasco.com">info-europe@vasco.com</a></td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>India</td>
<td>+91 22 4090 7112-14</td>
<td><a href="mailto:info-india@vasco.com">info-india@vasco.com</a></td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>Japan</td>
<td>+65 6323 09 06</td>
<td><a href="mailto:info-asia@vasco.com">info-asia@vasco.com</a></td>
</tr>
<tr>
<td>Europe, Middle</td>
<td>Africa, Austria</td>
<td>+43 1 9043132-0</td>
<td><a href="mailto:info-europe@vasco.com">info-europe@vasco.com</a></td>
</tr>
<tr>
<td>USA</td>
<td>Boston</td>
<td>+1 508 366 3400</td>
<td><a href="mailto:info-usa@vasco.com">info-usa@vasco.com</a></td>
</tr>
<tr>
<td>USA</td>
<td>California</td>
<td>+1 650 378 1202</td>
<td><a href="mailto:info-usa@vasco.com">info-usa@vasco.com</a></td>
</tr>
</tbody>
</table>

---

**Contact Information**

- **INTERNATIONAL HQ** - Switzerland
  - Phone: +41 41 555 35 00
  - Email: info-europe@vasco.com

- **CORPORATE HQ** - Chicago
  - Phone: +1 630 932 8844
  - Email: info-usa@vasco.com

---

Copyright © 2012 VASCO Data Security, Inc. VASCO Data Security International GmbH. All rights reserved. DIGIPASS®, CertiID™, VACMAN®, IDENTIKEY®, aXsGUARD®, Digipass®, the CertiID™ logo 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, mark, 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.