Secure your business

VASCO
THE AUTHENTICATION COMPANY

The world's leading software company specializing in **Internet Security**

A secure and flexible work environment

Today's workforce needs to use their PC to read e-mail, use software and documents, access files on the corporate network, work with applications and access websites anywhere and anytime. IT administrators need to make sure that the corporate resources are accessed in a secure way, whether the employee is in-house, working from home or on the road.

The security challenge solved

In many cases, the security challenge can be solved by implementing strong authentication. Strong authentication ensures that only authorized users access corporate network resources, business applications and corporate data, thus protecting the corporate assets from data theft.

VASCO has established a strong reputation in delivering e-signature solutions for e-banking. VASCO uses its experience in e-banking to bring banking level security to the enterprise security market.

Replace static password by one-time passwords

Static passwords are the weakest link in network security: they can be re-used, guessed, passed on and easily cracked by hackers. For many companies, static passwords are still the only authentication mechanism in place to protect their corporate assets.
With VASCO DIGIPASS, static passwords are replaced by one-time passwords (OTP). An OTP is generated by a hardware or software DIGIPASS. It is only valid for a limited period of time. The password is unique and cannot be reused.
By adding DIGIPASS authentication to the network infrastructure, you eliminate unauthorized access to your network, applications and business-critical data.

Digitally sign confidential documents or transactions

More and more transactions take place online, whether it is money changing hands, contracts being signed or confidential documents being exchanged. To ensure that these transactions are not being altered in transit, companies start to rely on encryption technology to sign documents or transactions. With VASCO's PKI-based DIGIPASS solutions you encrypt files and digitally sign e-mails, documents and transactions.

Secure the access to PCs and laptops

Employees are becoming increasingly mobile, as are results laptops have become an integral part of the standard equipment for road warriors and travelling staff. Laptops are stored in car trunks and overhead compartments in airplanes, as a result they can easily left behind or stolen. Strong authentication offers additional security for laptops through booth encryption and strong authentication for Windows logon.

Adding VASCO's DIGIPASS Authentication for Windows Logon to your infrastructure, or DIGIPASS CertiID, VASCO's PKI-based offering, for booth encryption, you will prevent unauthorized access to laptops and documents when laptops are lost or stolen, hence improving the access to your business critical information.

DIGIPASS™

Secure access to all your business applications with one DIGIPASS

With a single DIGIPASS and IDENTIKEY's server software all corporate applications can be protected. Employees can remotely log on to the corporate network and at the same time use DIGIPASS for Windows Logon, Outlook Web Access and Citrix. Whether you want to secure your CRM, ERP, payroll application, SaaS-application or all of them: your employees will be able to securely log on to all business applications with only one DIGIPASS.

Authentication in the cloud

Cloud-based applications are becoming increasingly popular. Cloud-based tools offer a wealth of advantages in terms of management, maintenance and upgrading. However they also worry IT administrators in terms of security: how are these applications secured, who can access the information stored in them? Application Service Providers (ASPs) have become aware of the security paradigm and are increasingly looking at two-factor authentication to secure their content, their user's content or simply to enhance the trust in online applications.

Next to traditional authentication solutions VASCO offers DIGIPASS as a Service, our cloud based authentication offering. With DIGIPASS as a Service we are meeting the growing need for strong authentication of ASPs with a hosted offering.

VACMAN

VACMAN, VASCO's core authentication platform, is already integrated by a vast number of leading enterprises worldwide. It combines all authentication applications, including OTP, challenge-response and e-signature on a single platform. VACMAN Controller is used for the authentication of millions of end-users. It can be seamlessly integrated into existing e-commerce and business applications in a time-saving and cost-effective way. Furthermore, VACMAN Controller is highly scalable: additional users or applications can easily be added.

IDENTIKEY

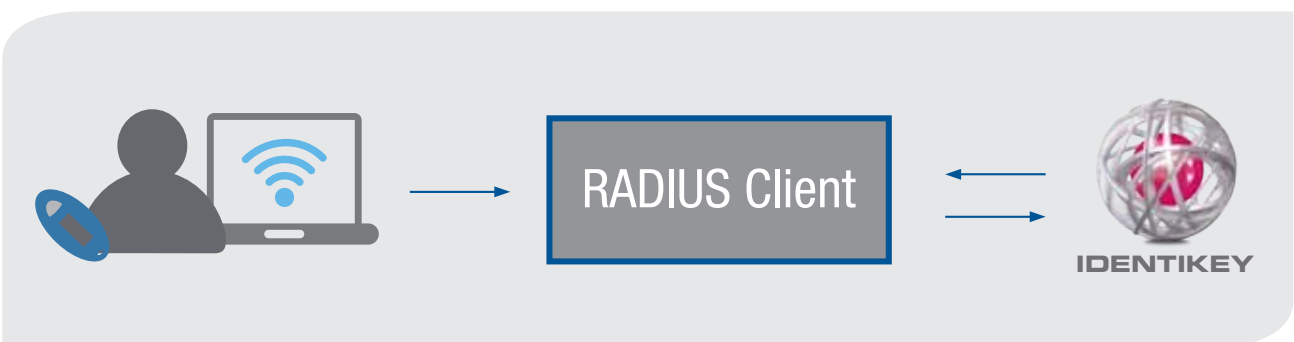
IDENTIKEY is VASCO's comprehensive authentication server for network and application security offering OTP and e-signature capability. IDENTIKEY is based on VASCO's core VACMAN technology and offers an authentication solution for several markets including Software as a Service (SaaS), e-gaming, online gambling, healthcare, automotive, e-banking and VPN access to corporate networks. IDENTIKEY can also be integrated by providers of managed services to offer authentication as a service.

aXsGUARD IDENTIFIER

aXsGUARD Identifier is a stand-alone turnkey authentication appliance for small, medium and large enterprises wanting to improve secure access to corporate networks and applications for remote users or home workers. aXsGUARD Identifier is suited for enterprises which want a dedicated appliance for their authentication needs, without the hassle of installing and maintaining a software installation. The solution has been designed for corporations which want to avoid sharing server resources for too many business critical applications. As a result you opt for a dedicated appliance to manage authentication requests without impacting your existing IT-infrastructure.

aXsGUARD Gatekeeper

aXsGUARD Gatekeeper is VASCO's remote access solution suited for companies looking for a comprehensive security appliance. It has everything a company needs to provide its employees with secure access to the corporate network (VPN, SSL-VPN, application firewall). The built-in two-factor authentication functionality makes this appliance the most secure and complete remote access solution. The easy to configure firewall with IPS keeps hackers out of the corporate network. Optional content scanning (anti-virus, anti-spam, …) provides a total security solution for network connectivity.



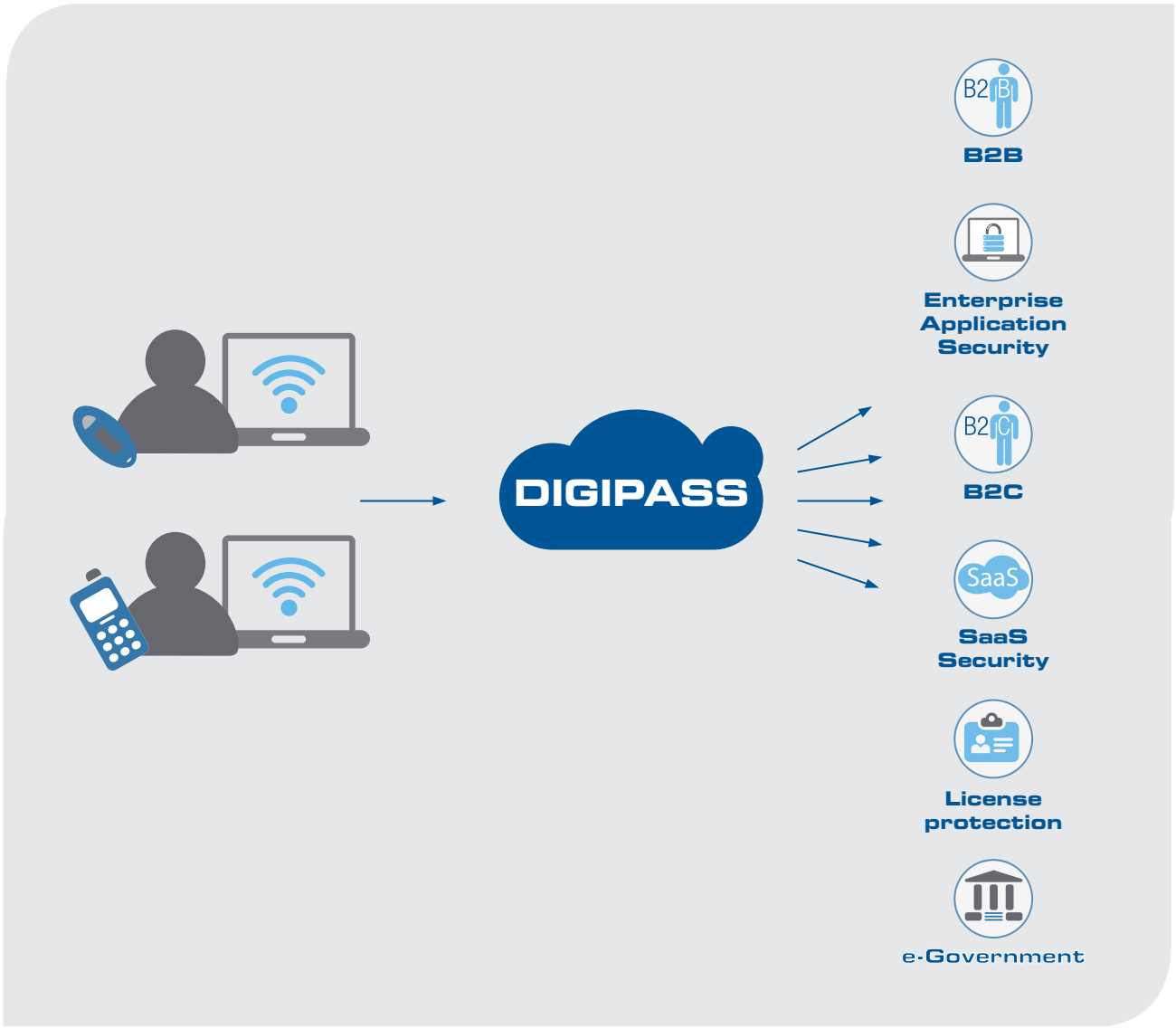
Standard Radius Setup With Authentication Server

DIGIPASS as a Service

DIGIPASS as a Service is VASCO's cloud based authentication service. The offer has been designed for ASPs which want to enhance the security of their web based applications. These ASPs typically want to protect their content, the content of their users, improve the trust in online channels or improve the security of self-service systems which reduce back office costs.

For ASPs traditional authentication does not always offer the adequate solution. Traditional authentication is often considered too costly due to low usage of the application or low transaction value or because the ASP does not have the resources to manager it. DIGIPASS as a Service is the answer to these concerns.

With DIGIPASS as a Service VASCO manages the entire authentication process for its customers. The end-user will use a hardware or software DIGIPASS to generate a an OTP to log on to the web based application or an e-signature to sign an online transaction. The ASP integrates an API which will forward the end-user's authentication requests to the DIGIPASS as a Service platform. The ASP focuses on its core activities while VASCO manages the authentication process. Authentication is either invoiced on a per application, per user, per month fee or as a monthly usage fee.



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: available with the customer's logo and corporate colors.

One button devices

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

Key features

- Ultra-portable
- User-friendly
- Time and event based authentication
- DES/3DES/AES/OATH
- Long life battery

PIN-pad devices

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

Key features

- PIN protection and PIN unlocking
- Simple and intuitive in use
- Time/Event and Challenge-response based
- Offers response only OTP, e-signature and challenge-response functionality
- Long life battery

Card Readers

A wide range of connected and unconnected card readers commonly used for e-commerce and e-ID applications

Key features

- No need to install drivers
- Smart card based OTP, e-signature, PKI functionality
- Straightforward deployment
- Ease-of-use

Software DIGIPASS

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

Key features

- No hardware deployment
- Time and event based authentication
- OTP and e-signature capability
- PIN-protected
- Transparent, user-friendly and ultra-portable

PKI-based solutions

VASCO's PKI-offering consists of DIGIPASS CertilD - a client-based software suite - and a range of DIGIPASS PKI devices, the DIGIPASS Key range. VASCO's PKI-based offering is suited for deployments in:

- **Enterprises:** where digital signature of e-mail, documents or contracts is required. But also for secure access to PCs, laptops and documents including Windows logon, secure VPN access, booth encryption and the secure exchange of documents via USB encryption partition.

- **Government:** where digital signature is required to prove citizens legal identity, or for digital signature of transaction such as tax payment, or secure access to e-government services.

- **Banks:** especially for corporate banking where customers execute high volume transactions with high risk.

DIGIPASS CertilD is VASCO's PKI based client software suite. The DIGIPASS Key range consists of smart card readers and USB devices.

DIGIPASS Pack for Remote Authentication

The DIGIPASS Pack for Remote Authentication is an off-the-shelf authentication solution for SMEs providing them with a high level of security to sensitive information and internal applications from a remote location without compromising security or user convenience. It has been designed for organizations with limited IT resources and budgets and it has all functionalities of an 'à la carte' authentication solution.

DIGIPASS Pack for Remote Authentication is simple to install, easy to manage, allowing you to have an authentication solution up and running within a day. Employees can remotely log-on to the corporate network and applications by using their DIGIPASS. On the server side, DIGIPASS Pack for Remote Authentication uses IDENTIKEY Server. It verifies the authentication requests and centrally administers user authentication policies. On the client side customers can choose between DIGIPASS Go 6, a one-button authentication device which generates an OTP, or DIGIPASS for Mobile, which leverages the mobile phone for authentication purposes.

DIGIPASS Pack for Remote Authentication is available in packs for 5, 10, 25 and 50 users.

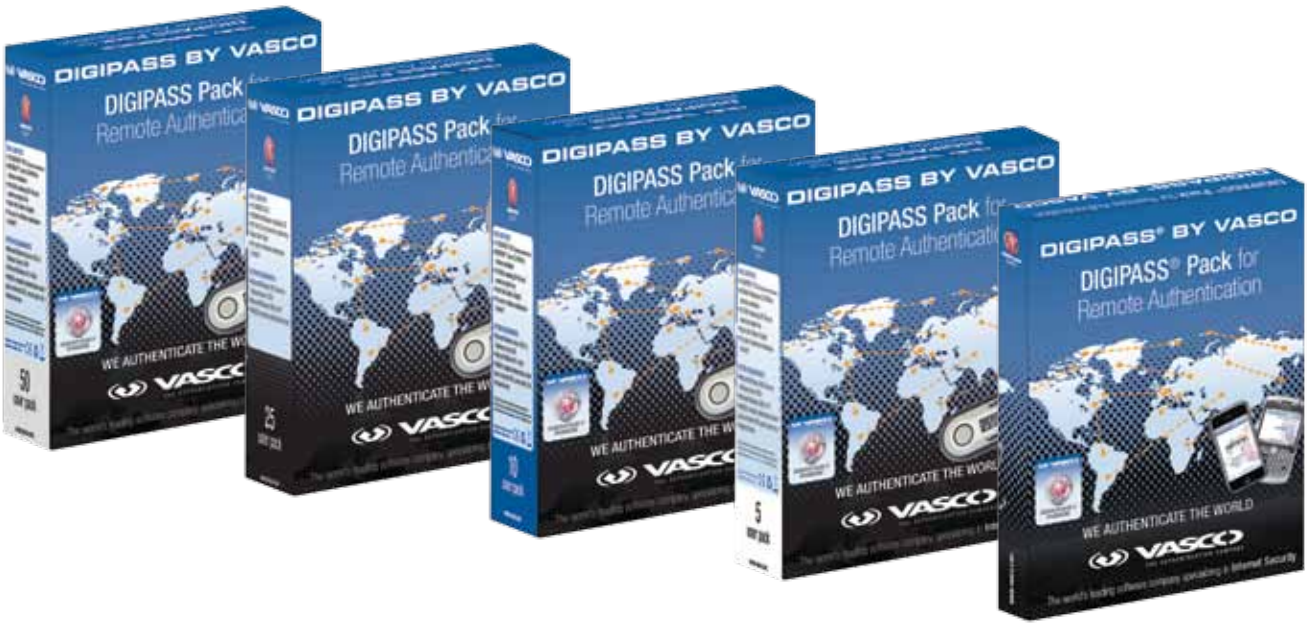
Online installation demo available on:
www.vasco.com/dppack_tutorial

More information available on: www.digipasspack.com

Support

Technical support of VASCO's solutions is provided through the reseller or system integrator. Direct technical support provided by VASCO is available through specific support plans (standard, 24/7, VIP, pay-per-incident, remote assistance) upon request.

More information about our support offering is available on:
www.vasco.com/support



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 solutions or develop new solutions based on the combined product offering.

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

DIGIPASS Plug-ins

VASCO also offers a full range of integrated solutions for Novell NMAS, Lotus Domino, AEP (Netilla), Imprivata, Juniper (FUNK), … 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 VASCO partners:
www.vasco.com/solutions/partners

CITRIX®

"As Citrix continues to grow, strategic partnerships will play an increasingly important role. The company is constantly seeking new partners to contribute to core products and add value for customers. We believe in the solutions VASCO offers and there is a great fit between our products, which is why we teamed up with VASCO."

Mark B. Templeton, President and CEO of Citrix

Technology Partners	Authentication Type						Integration Type						DIGIPASS				Documents	
	Remote	Web	Application	LAN	Management software & tools & tools	Preboot & Encryption	DIGIPASS Pack	IDENTIKEY	AXSGUARD IDENTIFIER	VACMAN	DIGIPASS Plug-In	DIGIPASS CertID	DIGIPASS for Mobile	DIGIPASS GO series	DIGIPASS PIN Pad Devices	DIGIPASS KEY devices	Integration Guide	Compatibility Guide
Adobe			√							√			√	√	√	√		
AEP Networks	√	√	√							√			√	√	√	√	√	√
Alcatel-lucent	√	√	√				√	√	√			√	√	√	√	√		
Apple				√								√	√	√	√	√		
ArrayNetworks	√	√					√	√	√			√	√	√	√	√		
Astaro	√	√					√	√	√			√	√	√	√	√		
Avaya	√	√					√	√	√				√	√	√	√		
Aventail	√	√					√	√	√			√	√	√	√	√		
Barracuda	√	√					√	√	√			√	√	√	√	√		
Belkin	√	√					√	√	√			√	√	√	√	√		
Bluecoat	√	√					√	√	√			√	√	√	√	√	√	√
Borderware	√	√					√	√	√			√	√	√	√	√		
CA			√							√			√	√	√	√		√
Celestix	√	√					√	√	√			√	√	√	√	√		
Check Point	√	√				√	√	√	√			√	√	√	√	√	√	√
Cisco Systems	√	√					√	√	√			√	√	√	√	√	√	√
Citrix	√	√	√				√	√	√			√	√	√	√	√	√	√

Partners

Technology Partners	Authentication Type						Integration Type						DIGIPASS				Documents	
	Remote	Web	Application	LAN	Management software & tools	Preboot & Encryption	DIGIPASS Pack	IDENTIKEY	AXSGUARD IDENTIFIER	VACMAN	DIGIPASS Plug-In	DIGIPASS CertiID	DIGIPASS for Mobile	DIGIPASS GO series	DIGIPASS PIN Pad Devices	DIGIPASS KEY devices	Integration Guide	Compatibility Guide
Cyber-Ark	√						√	√	√			√	√	√	√	√		
Cyberguard	√	√					√	√	√			√	√	√	√	√		
Docomo (Nomadix)	√	√					√	√	√			√	√	√	√	√		√
Evidian	√	√	√				√	√	√	√		√	√	√	√	√		√
F5	√	√					√	√	√			√	√	√	√	√	√	√
Fortinet	√	√					√	√	√			√	√	√	√	√	√	√
IBM - Domino/lotus		√	√								√	√	√	√	√	√	√	√
Imprivata	√	√	√	√			√	√	√	√		√	√	√	√	√	√	√
Juniper Networks	√	√					√	√	√			√	√	√	√	√	√	√
LetterGen					√							√				√		
Linksys	√	√					√	√	√			√	√	√	√	√		
Mandrake				√								√	√	√	√	√		
McAfee				√								√	√	√	√	√		
Microsoft	√	√	√	√		√	√	√	√			√	√	√	√	√	√	√
NEC	√	√					√	√	√			√	√	√	√	√	√	
NetAsq	√	√					√	√	√			√	√	√	√	√	√	√
Netegrity	√	√	√				√	√	√	√		√		√	√	√		√
Netgear	√	√					√	√	√			√	√	√	√	√		
NetGuard	√	√					√	√	√			√	√	√	√	√		
Nokia	√	√					√	√	√			√	√	√	√	√		
Nortel	√	√					√	√	√			√	√	√	√	√		
Novell	√	√	√	√			√	√	√		√	√	√	√	√	√	√	
O2	√	√					√	√	√			√	√	√	√	√	√	√
OpenTrust					√											√		
Oracle	√	√	√				√	√	√	√		√	√	√	√	√		√
OSC (Radiator)	√	√					√	√	√	√		√	√	√	√	√	√	√
Palo Alto Networks	√	√					√	√	√			√	√	√	√	√		
Quest (PassGO)			√				√	√	√	√		√	√	√	√	√	√	√
Redhat				√			√	√	√			√	√	√	√	√		
SecurIT		√	√					√	√	√			√	√	√	√		√
Siebel			√				√	√	√			√	√	√	√	√		
Sonicwall	√	√					√	√	√			√	√	√	√	√	√	√
StoneSoft	√	√					√	√	√			√	√	√	√	√		√
Symantec			√									√						
Ubuntu				√			√	√	√			√	√	√	√	√		
WatchGuard	√	√					√	√	√			√	√	√	√	√	√	√
Zyxel	√	√					√	√	√			√	√	√	√	√		

قطر للغاز
QATARGAS

Qatargas was founded in 1984 and has since then progressively established itself as a leading player in the liquid natural gas industry. Qatargas wanted to secure all its business applications thus ensuring data integrity for all business departments and operational services and provide secure remote access for the workforce and contractors. Qatargas wanted to implement a Citrix compliant solution securing the company's network and applications enabling remote access for executive management, remote offices and contractors. DIGIPASS has leveraged the security of Qatargas' remote network and business applications through the use of dynamic one-time passwords. DIGIPASS in combination with IDENTIKEY is fully compliant with Citix' solutions hence providing secure remote access to the Citrix metaframe.

Qatargas: secure corporate network access

Galápagos

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 data critical to its business, the company wanted to implement a comprehensive security solution for its network, VPN, website and e-mail traffic.
The security solution needed to be implemented into Galapagos' existing IT infrastructure. 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.

Galapagos secures business assets, network and VPN with aXsGUARD Gatekeeper

DORSET County Council

Dorset is a county in South West England on the English Channel coast. The county council was in need of a multiple authentication solution that could secure remotes network access for all employees as well as ensure the confidentiality of data stored on laptops. Dorset County Council implemented a user friendly, cost efficient and easy to deploy authentication solution which is compatible with the council's existing back-end infrastructure. VASCO's DIGIPASS GO3 provides Dorset County Council's ambulant workforce with a secure remote access solution. By deploying DIGIPASS 860 with PKI-functionality, laptop users are able to access the council's network remotely by generating dynamic passwords without compromising business-critical data stored on the laptop's drive thanks to hard-disk encryption. Both DIGIPASS solutions are fully compatible with the council's existing back-end infrastructure, allowing them to deploy two-factor authentication at the lowest total cost of ownership.

Dorset County Council: PKI encryption and dynamic passwords secure the network and confidential information

Penn State was founded in 1855 as an agricultural college. Today Penn State is one of four 'state-related' universities with 19 colleges and 23 locations. More than 80,000 students are currently enrolled in a wide variety of academic programs. Penn State wanted to implement two-factor authentication to secure its online administrative business processes at a reasonable cost. The authentication device had to be fully compliant with the university's existing infrastructure without needing to deploy additional hardware. DIGIPASS was an affordable solution that could be fully integrated within the third party's authentication package. The average battery lifetime of five years and beyond offers a high return on investment.

Penn State: secure online access to administration services

The Protestant Church in the Netherlands is with its 2.1 million members the largest Protestant denomination in the Netherlands. Today, church members use an online registration system. Because this system contains confidential information about church members, security is essential. The Protestant Church wanted to implement a strong authentication solution to secure the member registration application of the Protestant Church and make it remotely accessible. The solution had to be easy to implement, user-friendly and cost-effective. The Protestant Church implemented a personalized DIGIPASS GO 6 device in combination with the authentication software VACMAN Controller to secure its LRP application.

Protestant Church: secure access to online member registration

Picanol Group is an international, customer-oriented group that specializes in the development, production and sale of weaving machines and other high technology products, systems and services. Picanol Group wanted to implement a complete solution for its vendors, consultants and external collaborators to secure internal and external access to its various business applications. The group was looking for a solution that could be implemented in phases and would be easy to expand. The solution must eventually be used not only to secure remote access to applications, but also to secure the group's internal confidential information without having to make additional investments in a later phase. The company deployed IDENTIKEY Gold Edition together with DIGIPASS Go 6, Virtual DIGIPASS and DIGIPASS for Mobile. This combination allows the group to secure access to its business applications for its different target groups. IDENTIKEY works seamlessly with the various DIGIPASS solutions and requires no additional hardware investment. Moreover, the number of users over time is easy to extend thanks to the flexible licensing system.

Picanol Group: secure access to the company's network

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 serving customers in more than 100 countries, including several international financial institutions. VASCO's prime markets are the financial sector, enterprise security, e-commerce and e-government.

www.vasco.com

INTERNATIONAL HQ
CHICAGO
phone: +1.630.932.8844
email: info_usa@vasco.com

OPERATIONAL HQ
BRUSSELS
phone: +32.2.609.97.00
email: info_europe@vasco.com

FINANCIAL HQ
ZURICH
phone: +41.43.555.3500
email: info_europe@vasco.com

YOUR LOCAL OFFICE

BOSTON
phone: +1.508.366.3400
email: info_usa@vasco.com

SYDNEY
phone: +61.2.8061.3700
email: info_australia@vasco.com

SINGAPORE
phone: +65.6323.0906
email: info_asia@vasco.com

BR201009 - v2