Secure access to patient data
Secure access to patient data.
References

Health services
P3 AMSANT secures e-health records in remote Australia with DIGIPASS
P4 IJZA secures electronic files in the youth care sector with IDENTIKEY and DIGIPASS

Hospitals
P5 Barmherzige Brüder secure remote access and sensitive data with IDENTIKEY and DIGIPASS technology
P6 Leuven University Hospital protects confidential patient information with VASCO’s DIGIPASS 300

Biotechnology
P7 Galapagos chooses aXsGUARD Gatekeeper to secure its business assets, network and VPN

Healthcare application providers
P8 Confidentiality of electronic medical files in Promedico ASP guaranteed by DIGIPASS

Health insurance
P9 CM Midden Vlaanderens patients’ medical and private data secured
Secure access to patient data

Executive Summary
As healthcare organizations modernize and transfer their services to web-based applications, the information contained within them becomes more vulnerable for unauthorized access. If not properly secured, confidential information such as lab results, patient health data, and billing information can fall into the hands of fraudsters. Therefore, security and confidentiality of patient records must be upheld by securing user access to such critical data.

VASCO’s proven multi-factor authentication technology safeguards user login and ensures that only authenticated users gain access.

Benefits
- Technological convergence and interoperability
- End-user convenience
- Security and confidentiality of patient records
- Regulatory compliance
- Risk mitigation

VASCO’s authentication solutions are suited for:
- Health management organizations and health insurance companies
- Hospitals and healthcare facilities
- Clinical environments and labs
- Medical billing and supporting organizations
- Claims processors
- e-Prescribe applications
- EMR / EHR / HIE systems
- Any web-based medical or healthcare application
- Health information exchange portals
- Medical or healthcare application access via SSL-VPN
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. The organization provides advocacy and support services to its twenty-six independent members who provide primary health care services to Aboriginal people. To assist its members, AMSANT developed a shared IT infrastructure service secured by DIGIPASS technology, enabling health care providers in very remote areas to securely access via the Internet their applications and sensitive medical records anywhere, anytime.

OBJECTIVE
Provide health service providers in the Northern Territory with an easy to manage security solution to secure remote online access over the Internet to applications and patients’ health records.

CHALLENGE
Remoteness and extreme environmental conditions, combined with an unreliable and unstable telecommunications infrastructure constantly challenged the continuity of services. IT capabilities and support in very remote areas were virtually non-existent and low budgets are a major constraint.

SOLUTION
CS2 developed a low cost end-to-end solution integrating VASCO’s DIGIPASS technology to secure remote online access to AMSANT’s e-health system. Redundancy is guaranteed through terrestrial and satellite connections. CS2 integrated NetLeverage’s virtual desktop technology replacing previous desktop infrastructures hence severely reducing local support requirements and costs. All data and applications are centralized, securely stored and managed by ac3’s data center in Sydney.

DIGIPASS 860
Increased identity and data theft, man-in-the-middle attacks and unauthorized access to confidential data demonstrate the growing need for data security solutions. Stringent regulations have been put in place for companies and financial institutions to ensure data security.

DIGIPASS KEY 860 is used in conjunction with DIGIPASS CertiID and can be integrated within any application that supports PKCS#11, MS CAPI standards and CNG.
IJZA secures electronic files in the youth care sector with IDENTIKEY and DIGIPASS

More than 26,000 people are employed in the Dutch youth welfare sector providing specialized help to children and adolescents and their immediate surroundings. Youth caretakers face very divergent situations from education problems, problems with social skills to foster care and crisis aid and relief. IJZA is one of the registration programs allowing youth caretakers to create and follow up electronic files of their youthful clients. To guarantee the confidentiality of the information contained in the database, IJZA took no risks. IJZA opted for VASCO and implemented DIGIPASS together with IDENTIKEY to secure access to its web application.

OBJECTIVE
The youth care institutions in North Brabant developed a web based application to register their youth welfare contacts in a straightforward and efficient way. Because, the information contained in the application’s database is extremely sensitive and confidential, IJZA was on the lookout for a strong authentication solution to secure access to the web based application.

CHALLENGE
Two-factor authentication was required for securing the application. Mobility was a necessity because youth welfare services have a lot of ambulatory employees. Remote access was a second important requirement. Because the application is running in-house, IJZA wanted a manageable and user-friendly solution.

SOLUTION
The combination of VASCO’s authentication server IDENTIKEY and DIGIPASS met all of IJZA’s expectations and requirements. It is a mobile solution allowing remote access. IDENTIKEY has a user-friendly web interface allowing system administrators to manage and run the authentication solution effortlessly.

DIGIPASS GO 3
User acceptance of security tools is a crucial factor in guaranteeing the success of security solution implementations for secure access to remote applications and networks. An alternative to the risk that static PINs and TAN lists (pre-printed lists of TransAction Numbers) pose, DIGIPASS GO 3 is very affordable, ultra-user friendly, and quick and efficient to rollout to users.

IDENTIKEY
IDENTIKEY Server is an off-the-shelf centralized authentication server that supports the deployment, use and administration of DIGIPASS strong user authentication. It offers complete functionality and management features without the need for significant budgetary or personnel investments.
Barmherzige Brüder secure remote access and sensitive data with IDENTIKEY and DIGIPASS technology

The computer center of the Barmherzige Brüder Austria is the central ICT service provider for eight hospitals, three residential and nursing homes, and a spa/health center in Austria. Together with the IT departments at each site, the central data center provides IT services that support hospital management and operation processes for a total of 5,500 end-users. In order to secure its sensitive data and confidential records and to make them remotely available, the Barmherzige Brüder implemented an authentication solution with one-time password technology using VASCO’s DIGIPASS and IDENTIKEY server.

OBJECTIVE
A gradual replacement of the existing one-time password authentication solution to secure remote access. The new solution must support authentication via SMS.

CHALLENGE
When deploying the new solution, the existing authentication devices from the previous system still needed to function until their ‘end of life’. This would require a seamless integration with the existing authentication server.

SOLUTION
The Barmherzige Brüder decided against the upgrade of their existing solution and chose for the combination of VASCO’s IDENTIKEY Server with DIGIPASS. IDENTIKEY authenticates all DIGIPASS users and forwards all other authentication requests to the appropriate server. Gradually, the older devices will be replaced by DIGIPASS.

DIGIPASS GO 6
DIGIPASS GO 6 is a ‘one-button’ authenticator, based on VASCO’s proven DIGIPASS technology. Banks and other organizations can effectively combat internet fraud by replacing static or paper based password systems, using DIGIPASS GO 6.

IDENTIKEY
IDENTIKEY Server is an off-the-shelf centralized authentication server that supports the deployment, use and administration of DIGIPASS strong user authentication. It offers complete functionality and management features without the need for significant budgetary or personnel investments.
Leuven University Hospital protects confidential patient information with VASCO’s DIGIPASS 300

Leading medical technology, high quality innovative medicine, care and trust are part of the Leuven University Hospital’s mission. With its 1,894 beds and more than 8,000 staff members, the UZ Leuven is one of the largest and most renowned health care centres in the Benelux. The UZ is also a leader when it comes to ICT. Doctors who are not part of the hospital’s permanent staff can consult their patient’s UZLeuven file through the Internet, with the patient’s consent. Specialist research, carried out at the UZ, can be interpreted online in a local doctor’s practice and employees can access the UZ network from home.

OBJECTIVE
How can you make the Internet, which is an open system, secure enough? How can you guarantee that only people who are authorised have access to the UZ network, in order to guarantee that only the right people have access to the applications they need to use.

CHALLENGE
UZ staff are not necessarily computer specialists. The LISA-programme was integrated in a browser which means users do not need to download cumbersome programmes. Determining factors for choosing VASCO’s DIGIPASS were security and the user-friendliness of the software.

SOLUTION
The UZ Leuven’s Information Systems service built its own security infrastructure and acquired the DIGIPASS 300 and DIGIPASS Libraries from VASCO in order to guarantee verification.

DIGIPASS 300
A DIGIPASS 300 personal authentication device eliminates the weakest link in any security structure: the use of static passwords. DIGIPASS generates a one-time password that enables you to identify customers and employees who are accessing your computer systems or networks.

E-signatures can also be generated to sign financial transactions. Most importantly, it provides secure access from any location.

This product is in phase out. Please contact your local sales representative for more information.
Galapagos chooses aXsGUARD Gatekeeper to secure its business assets, network & VPN

Galapagos is a European biotechnology company specialized in drug discovery for the treatment of bone and joint diseases. To secure its business critical data the company wanted to implement a comprehensive security solution to secure its network, VPN, website and e-mail traffic. A proven technology and thorough support were two decisive criteria. VASCO’s aXsGUARD Gatekeeper proved to be the ultimate solution. aXsGUARD could be effortlessly integrated into Galapagos’ existing IT infrastructure providing the company with a cost-efficient, low-maintenance and all-encompassing security infrastructure.

OBJECTIVE
Implement an overall security solution to secure Galapagos’ e-mail, website, network and VPN.

CHALLENGE
The security solution must be implemented into Galapagos’ existing IT infrastructure. Stability and support are decisive factors, as Galapagos’ IT resources are limited. Secure remote access to the corporate network is a must.

SOLUTION
aXsGUARD was one of the few solutions that could be perfectly integrated into the company’s exiting infrastructure. Since the implementation of aXsGUARD downtime is non-existent and rendered support is excellent. Galapagos’ employees and external researchers can securely access the company’s corporate network from anywhere in the world.

AXSGUARD GATEKEEPER
A full scale authentication appliance, aXsGUARD Gatekeeper is the most cost-effective authentication appliance on the market, targeted for the SME market. Optional modules allow you to organize your total network connectivity security in a structured and integrated method.

Monitoring, auditing and reporting features provide IT administrators with the necessary tools to check all network activity. aXsGUARD Gatekeeper, VASCO’s remote access solution, addresses the security issues IT administrators face.
More and more general practitioners create electronic medical files about their patients. Exchanging that information with other practitioners and health care providers however, is not as common as it seems. Security and confidentiality remain big issues when it comes to sharing patients’ medical records. Promedico ICT Ltd., a leading company offering ICT-solutions for healthcare, introduced its innovative software product ‘Promedico ASP’ enabling general practitioners to share and exchange medical information in a secure way.

OBJECTIVE
Provide secure access to Promedico’s online application for authorized users only and protect medical records from confidentiality breaches.

CHALLENGE
Access to Promedico ASP must be secured without needing to install additional soft- and hardware in the GP’s practice. Patients’ medical files should be accessible for authorized at any given time and location. Security standards must comply with local legislation.

SOLUTION
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 GPs to sign their messages and update their patients’ records in a secure way.

DIGIPASS 300
A DIGIPASS 300 personal authentication device eliminates the weakest link in any security structure: the use of static passwords. DIGIPASS generates a one-time password that enables you to identify customers and employees who are accessing your computer systems or networks.

E-signatures can also be generated to sign financial transactions. Most importantly, it provides secure access from any location.

This product is in phase out. Please contact your local sales representative for more information.
Patients’ medical and private data secured by DIGIPASS GO 6 and IDENTIKEY

CM Midden-Vlaanderen is a local branch of CM, the largest Belgian health insurance agency, which vouches for more than 500,000 socially insured. In order to facilitate the exchange of patient and insurance information between different hospitals and between the hospitals and CM, the internet application Curenet was developed. As it contains data belonging to the private sphere, access to the application needed to be adequately secured. CM Midden-Vlaanderen relied on DIGIPASS GO 6 in combination with IDENTIKEY Enterprise.

OBJECTIVE
CM Midden-Vlaanderen wanted to secure its Curenet application, containing private and medical information of patients and insured persons from unauthorized access.

CHALLENGE
The solution had to be trustworthy and convenient to use, and should seamlessly integrate into the Curenet application.

SOLUTION
VASCO’s DIGIPASS technology combined with IDENTIKEY Server Enterprise Edition was considered to be the most handy and trustworthy solution, especially because VASCO had already gained a lot of recognition thanks to its proven services in the banking sector.

DIGIPASS GO 6
DIGIPASS GO 6 is a ‘one-button’ authenticator, based on VASCO’s proven DIGIPASS technology. Banks and other organizations can effectively combat internet fraud by replacing static or paper based password systems, using DIGIPASS GO 6.

IDENTIKEY
IDENTIKEY Server is an off-the-shelf centralized authentication server that supports the deployment, use and administration of DIGIPASS strong user authentication. It offers complete functionality and management features without the need for significant budgetary or personnel investments.
VASCO is a world leader in strong authentication and e-signature solutions, specializing in online accounts, identities and transactions. As a global software company, VASCO serves a customer base of approximately 10,000 companies in over 100 countries, including approximately 1,700 international financial institutions. VASCO’s prime markets are the financial sector, enterprise security e-commerce and e-government.

OUR MISSION
To authenticate the world.

OUR VISION
Full-option, all-terrain authentication

Full-Option
All our authentication technologies, solutions, and services are hosted on our single unique platform, VACMAN Controller.

All-terrain
VASCO brings banking security to 50 different vertical applications, such as healthcare, e-gaming, automotive, human resources, education, administration, e-government, legal, manufacturing and many more.

OUR STRATEGY
VASCO is committed to providing financial institutions with an array of authentication solutions and services at the lowest total cost of ownership. In addition to the financial sector, VASCO technologies secure sensitive information and transactions for the enterprise security, e-commerce, and e-government industries, and we are constantly enhancing our current offerings in order to better meet the specific needs of our customers within those markets.

For additional information please contact VASCO:
info@vasco.com
+32 2 609 97 00
www.vasco.com/
healthcare