

Saint-Gobain Isover G + H AG has chosen VASCO's Digipass GOI for secure remote access

Case Study

Secure Remote Access to a corporation's network by customers, road warriors and home workers often constitutes a problem. On the one hand, the remote access procedure must guarantee maximum security, as company-critical data are accessed. In addition, remote access must be user friendly and easy to implement. The cost factor plays an important role too. Strong authentication via VASCO's Digipass Tokens is the best solution for companies searching to secure their remote access applications in a swift, cost-efficient and flexible way.



Digipass GOI

S Saint-Gobain Isover G + H AG is an international manufacturer of insulation materials with its head office in Ludwigshafen (Germany). The company currently employs 1350 people and has several branches in Germany and the neighbouring European countries.

The way it works

End-users get access to the company's network via the Citrix ICA client that exists as a "snap in" for Internet Explorer and thus does not make any larger interventions in the system.

Via the ICA client, the notebook or PC connects to a terminal service in Isover's head office (128 bit encrypted), where it receives a Novell login window, which asks not only for the normal network password, but also for a one-time password, generated by VASCO's Digipass.

The ICA client gives access to the local hard disk in the ICA tunnel thus created so that synchronisation with the local Outlook is possible as well as an exchange of database information with the CRM system (delta files database).

History
In 1999 Saint-Gobain Isover first implemented a remote access application based on VPN, to allow its field representatives, home office users and branches to access the company data. This solution was expensive, because it couldn't be administrated centrally. For example, the PCs and laptops had to be sent to the company's head office to install the VPN client. And if there were defective functions, the machines had to be sent from all over Europe to the head office, which in addition to the logistical expense also reduced the productivity of the employees affected. Access via VPN furthermore required intensive training of the employees and carriers and offers numerous possibilities for incorrect use.

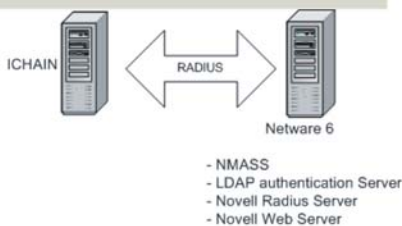
Evaluation Phase
Mid 2002, Saint-Gobain Isover started investigating the implementation of a new Corporate Network Access solution. The main requirements were user friendliness, cost effectiveness and central access administration, with no additional software to be downloaded onto the end-user's

PC or laptop. In addition, the susceptibility to errors had to be greatly reduced. Based on these requirements, the company opted for token-based strong authentication.

In the first evaluation phase, Saint-Gobain Isover requested information about token-based solutions for remote access from various manufacturers and distributors. "We very soon chose VASCO's Digipass, because its software is natively integrated in Novell's Modular Authentication Service (NMAS), that is running on our NDS directory service," explains Andreas Eckert, responsible for the network administration and system programming at Saint-Gobain Isover G+H. "We were able to make massive cost savings, since now we only have to pay for the tokens."

Successful Test and Implementation
When the first evaluation phase was concluded, Saint-Gobain Isover G + H contacted VASCO and ordered Digipass Go 1 strong authentication tokens via a local Vasco reseller.

ICHAIN- NMAS communications



Successful Test and Implementation

When the first evaluation phase was concluded, Saint-Gobain Isover G + H contacted VASCO and ordered Digipass Go 1 strong authentication tokens via a local Vasco reseller. Digipass Go 1 generates dynamic passwords every 36 seconds. Due to its small size, Digipass GO1 is particularly suitable for mobile use. The token can easily be used as a key ring. VACMAN Controller, VASCO's server software is natively integrated in Novell's NMAS and was simply installed on the server side.

Andreas Eckert explains: "We were competently advised by VASCO's staff. They advised and assisted us regarding the choice of tokens and the implementation and execution of the tests." As a result of the close cooperation with Vasco, the technicians of Saint-Gobain Isover G + H were able to install the test environment in less than a week. Within the framework of the test phase, that covered a period of several months, a positive development in comparison with access via VPN could be achieved. It became clear

that the new solution was less susceptible to operating and equipment errors. The management and maintenance costs for the remote access, but also the logistical problems when sending defective devices could be reduced massively. This resulted in an important reduction in operating costs.

Conclusion

Based on the positive results of the test phase, Saint-Gobain Isover G + H ordered several hundreds of Digipass Go 1 tokens. Currently, all the field representatives and home office workers as well as the transport carriers can at any time and from any Internet connected computer get secure access to Saint-Gobain Isover's networks.

"With VASCO's Digipass we were quickly and simply able to achieve our objectives in a swift and simple way. The solution only has to be installed on the server side; a client set-up is no longer necessary on PC's and laptops. Digipass is extremely easy to use. The password is generated dynamically when the Digipass token is

opened.” Andreas Eckert concludes “And of course the security of the company data is guaranteed, as strong authentication is always based on two factors that are independent of each other. In addition to the dynamic password from the Digipass token, the users also need a user name. The user will be granted access to the network if both the user name and the password fit.

Jan Valcke, President & COO at Vasco Data Security explains:

“Due to the integration of our Digipass series in Novell NMAS, we can offer companies Digipass strong authentication at a favourable price. The product is installed

in a very short time. Customers do not require an additional authentication server and technical support doesn't have to be burdened with the cumbersome task of static password management. Digipass was integrated into Novell NMAS with the aim of keeping the Total Cost of Ownership down. We succeeded in that task”



Jan Valcke - President & COO
VASCO Data Security

For regional offices or to learn more about us, visit our web site at www.vasco.com



EMEA

VASCO Data Security nv/sa
Koningin Astridlaan 164
B-1780 Wommel, Belgium
phone: +32.2.456.98.10
fax: +32.2.456.98.20
e-mail: info_europe@vasco.com

APAC

VASCO Data Security Asia-Pacific Pte Ltd.
#14-01 Prudential Tower, 30 Cecil Street
049712 Singapore
phone: +65.6.232.2727
fax: +65.6.232.2888
email: info_asia@vasco.com

AUSTRALIA

Level 11, Tower B, Zenith Centre
821 Pacific Highway, Chatswood
NSW 2067 AUSTRALIA
phone: +61.2.8448.2068
fax: +61.2.8448.2010
email: info_australia@vasco.com

AMERICA

VASCO Data Security, Inc.
1901 South Meyers Road, Suite 210
Oakbrook Terrace, Illinois 60181, USA
phone: +1.630.932.8844
fax: +1.630.932.8852
e-mail: info_usa@vasco.com

All trademarks or trade names are the property of their respective owners. VASCO reserves the right to make changes to specifications at any time and without notice. The information furnished by VASCO in this document is believed to be accurate and reliable. However, VASCO may not be held liable for its use, nor for any infringement of patents or other rights of third parties resulting from its use.