Nowadays, every company depends on the Internet for its day-to-day operations. Security has become a regular concern for IT administrators and banks alike. Whether it is about securing remote access to corporate networks, business and online applications or online financial transactions, companies are facing a never-ending threat from online fraudsters.

More and more enterprises turn to cloud applications IT-departments have genuine concerns about security when implementing cloud solutions: how secure are these hosted applications? After all, your data reside somewhere on a server hosted by the vendor. Which measures does this vendor take to make sure that his infrastructure is sufficiently stable and redundant? How do they secure the access to the infrastructure and data? The questions are numerous.

As the global leader in two-factor authentication solutions, VASCO® Data Security provides mature technology with a minimal impact on a IT architecture. VASCO’s solutions are designed to complement existing security policies. They have been refined by years of experience in the world’s largest deployments in the banking sector.

VASCO DIGIPASS & IDENTIKEY

VASCO DIGIPASS® technology is used by major banks around the globe and can be regarded as the reference for secure user authentication. Insecure static passwords are replaced with a dynamic, time-limited one-time password and e-signature to protect online transactions.

DIGIPASS is an authentication technology available in over fifty different form factors, ranging from one-button to keypad devices to mobile software applications and Windows programs. Each has its unique features and specifications that address different needs in various markets.

With IDENTIKEY® Authentication Server VASCO introduces affordable two-factor authentication enabling enterprises to secure their applications and networks from unauthorized access. DIGIPASS technology offers the same high-level security as deployed in banks and financial institutions worldwide.
IDENTIKEY product family

A COMPLETE OFFERING TO FIT YOUR NEEDS

IDENTIKEY

The IDENTIKEY product family is continuously expanded as new needs arise in different markets. Technology changes, markets mature and users look for newer, enhanced experiences. IDENTIKEY grows and expands to address these changes. Four major server components exist side-by-side and offer a solution for any security installation:

- IDENTIKEY Authentication Server
- IDENTIKEY Federation Server
- IDENTIKEY Appliance
- IDENTIKEY Virtual Appliance

IDENTIKEY Authentication Server

IDENTIKEY Authentication Server is the next-generation centralized authentication server that supports DIGIPASS technology. It verifies authentication requests from individuals trying to access the corporate network or business applications.

Built around VASCO’s core VACMAN authentication platform, IDENTIKEY Authentication Server is flexible yet robust enough to offer the highest level of security in a convenient administrative package.

The solution is ideally suited for large and small enterprise network security implementations, application security and online banking security.

For more details on IDENTIKEY Authentication Server, please see page 3.

IDENTIKEY Federation Server

IDENTIKEY Federation Server is a server software that adds, in combination with IDENTIKEY Authentication server, strong user authentication to the logon procedure for web applications. The identity and access management platform is used to validate user credentials across multiple applications and disparate networks. IDENTIKEY Federation Server is extremely well suited for large corporations, governments, non-profit organizations and educational institutions looking to secure and manage access to different web-based applications and portals.

For more details on IDENTIKEY Federation Server, please see page 13.

IDENTIKEY Appliance

IDENTIKEY Appliance is a stand-alone authentication appliance that secures remote access to corporate networks and web-based applications. IDENTIKEY Appliance is highly suited for all enterprises that are looking to acquire a dedicated appliance for their authentication needs, avoiding the hassles and cost of installing and maintaining a software-based solution.

For more details on IDENTIKEY Appliance, please see page 14.

IDENTIKEY Virtual Appliance

IDENTIKEY Virtual Appliance is a virtualized version of the physical IDENTIKEY Appliance. It is a plug-and-play solution that runs in an existing virtual environment and can be installed very quickly and easily. The solution is completely scalable by license and, as such, suited for enterprises of all sizes.

For more details on IDENTIKEY Virtual Appliance, please see page 15.
Identifkey Authentication Server

Vasco’s Next Generation Authentication Server

Identifkey Authentication Server is Vasco’s centralized authentication server for enterprise security, online application security and Internet banking. Identifkey Authentication Server 3.4 is the simplest and most cost-effective solution to help authenticate remote and local users accessing the corporate network.

The solution offers strong authentication and validation of transaction signatures with support of EMV-CAP to address the need for e-signatures in commercial and banking web-based applications.

Using an individually assigned Digipass authenticator, remote and local users will be able to quickly and easily prove their claimed identity through a dynamically generated one-time password (OTP). In a similar way, electronic signatures can be generated and used for secure validation of financial transactions.

Identifkey Authentication Server is easy to install, configure and manage. It provides a wide range of interfaces that allow easy integration into existing customer remote access infrastructures and web-based applications. The solution runs on Windows and Linux environments, AD integration and LDAP back-ends.

Identifkey Authentication Server is highly scalable and supports a user load from 5 users to very large deployments (over millions of users). It offers the highest security by integrating Vasco’s proven technology, in place at major banks around the world, to every customer who is looking to replace insecure static passwords by two-factor authentication.

Leverage existing infrastructure

Identifkey Authentication Server can be seamlessly integrated into any RADIUS environment. As such, the customer can keep on using his existing infrastructure. No additional cost is incurred as the existing database and servers do not need to be replaced. The data storage can be integrated in Active Directory or in a variety of ODBC compliant databases. Identifkey Authentication Server interfaces with several RADIUS authentication servers and can perform LDAP lookup on AD, ADAM, and eDirectory.

The solution was designed with web functionality in mind. Identifkey Authentication Server can easily be integrated with online applications via SOAP, allowing easy connection modifications to the server without the need for additional services or development resources. It also uses a web-based administration interface and reports user activity in HTML or XML format.

Simple administration

Identifkey Authentication Server offers several features to make the administrator’s job a lot easier and to help save costs. All administration tools are conveniently available in a single interface. This centralized management tool is accessible via any Internet browser from anywhere in the network. This allows remote management and brings new opportunities for providers of outsourced services.

Identifkey Authentication Server has an extensive reporting functionality allowing to create useful summaries on user history, Digipass activities etc.… These reports, together with the security audit function, can provide crucial input for help desk and accounting purposes.

Additionally, the solution provides an interface that allows system monitoring and performance monitoring of its behavior from a remote service via SNMP.
IDENTIKEY Authentication Server

SMOOTH ROLLOUT

IDENTIKEY Authentication Server includes several tools and features which facilitate a smooth rollout, convenient user registration, or migration from existing products. These include a data migration tool, dynamic user registration, password auto learn, bulk management, auto assign, and others.

An intuitive installation wizard guides you through the setup process. The fast and automated deployment gets you started in no time, with limited involvement from the IT department. Users can self-assign their DIGIPASS authenticators, update their passwords and change their PINs, thus lowering the helpdesk interventions and again reducing costs.

Adding more users and/or applications is as simple as purchasing more licenses. Provisioning for software and mobile authentication devices is available right out of the box.

HIGH AVAILABILITY

VASCO offers several countermeasures against failure, like server failover, redundancy, and database replication for continuous support. IDENTIKEY Authentication Server is scalable for large deployments and is performance upgrade ready.

USER-FRIENDLY

IDENTIKEY-based authentication does not change the end user’s experience or IT infrastructure. It offers a simple way to add multi-factor authentication on top of existing applications.

DIGIPASS

When using IDENTIKEY Authentication Server, end users will be equipped with a DIGIPASS client device. VASCO’s DIGIPASS family offers a wide range of end user authentication devices both software (in the browser, on the mobile) and hardware-based, to suit your needs.

All DIGIPASS authenticators are fully customizable with your company’s logo and corporate colors.
IDENTIKEY Authentication Server is a robust and scalable authentication server for enterprises of all sizes including SMEs. It enhances remote access security to corporate networks and to in-house applications. By adding a security layer to the logon procedure over the Internet, IDENTIKEY Authentication Server secures home workers, road warriors, travelling staff, remote offices, and business partners.

IDENTIKEY Authentication Server is installed on a server of choice. An intuitive installation wizard guides the user through the complete setup. Connections to the front-end clients like the firewall or router, and the back-end servers for additional static password validation are established automatically. Administrator intervention is limited to making a few choices for server location and data storage. This makes IDENTIKEY Authentication Server very simple and easy to install and set up.

IDENTIKEY Authentication Server uses current data communication standards and is compatible with a wide range of products from network equipment manufacturers. It can be integrated directly in the existing infrastructure. As companies grow, additional end user devices and applications can be added.

**Qatargas**

Qatargas is a pioneer in the liquefied natural gas industry in Qatar. Qatargas wanted to secure all its business applications thus ensuring data integrity for all business departments and operation services and provide secure remote access for the workforce and contractors. They wanted to implement a Citrix compliant solution to secure the corporate network and the applications providing secure remote access to the executive management, the remote offices and the contractors. VASCO’s DIGIPASS improved the security level of QatarGas’ remote network and business applications through the use of dynamic one-time passwords. DIGIPASS in combination with IDENTIKEY is compliant with Citrix hence providing secure remote access to the Citrix metaframe.
IDENTIKEY for e-Banking

SECURE ONLINE BANKING

IDENTIKEY Authentication Server is a perfect fit for banks wanting to implement a strong authentication solution without dedicating significant budget and resources or looking to avoid large integration projects. It is also suited for banks in need of a dedicated authentication server solution. With IDENTIKEY Authentication Server, financial organizations can offer strong authentication as an additional security layer to their complete range of banking services: retail banking, corporate banking, mobile banking, call center and others.

IDENTIKEY Authentication Server in combination with DIGIPASS technology provides secure access to online banking applications and electronic signature functionality for transaction validation, making it one of the best solutions in the market to counter man-in-the-middle attacks (MITM).

IDENTIKEY Authentication Server can validate one-time passwords for access control and e-signatures for transaction security. With its EMV-CAP and HSM support, banks in emerging markets have a total authentication solution at their disposal, leveraging their prior investments in a payment card infrastructure for authentication purposes. The HSM capability of IDENTIKEY Authentication Server offers optimal security since cryptographic keys cannot be compromised.

IDENTIKEY Authentication Server is tailored towards financial service providers that can offer it as an authentication service to their customers. By using authentication services, banks can push a part of the security tasks to a service partner and focus on their core business. These services are invoiced on a monthly or quarterly basis, thus making them attractive from an accounting point of view (cash handling, budget control, investment management, etc).

As banks and financial institutions need their infrastructure to be PCI-DSS compliant and cannot add any component that would render such setup non-compliant, IDENTIKEY Authentication Server has been checked and tested according to the PCI-DSS compliancy regulations, so that the mandatory compliancy of any organization that integrates IDENTIKEY Authentication Server remains unchanged.

KEY FEATURES

- Helps to combat MITM-attacks
- Can be easily integrated with existing online banking applications
- Adds strong authentication and e-signature functionality for a safe and secure Internet banking experience
- Fast deployment and implementation
- Complete functionality is provided (authentication, administration, reporting, auditing, user management, DIGIPASS management)
- Centralized authentication platform for several service centers (retail banking, corporate banking, mobile banking etc.)
- Versatile auditing and reporting functionality
- Support for EMV-CAP and Hardware Security Module (HSM)
- Enables financial institutions to remain PCI-DSS compliant
- IDENTIKEY Integration Program brings administrators up-to-date in a few days
CLOUD APPLICATIONS

The cloud concept is quite popular thanks to the various benefits they offer: upfront costs are significantly lower, it is faster and cheaper in deployment, it requires no additional server hardware investments, it is extremely scalable and upgradeable, no dedicated staff is required and thus ROI is guaranteed.

However, IT-departments have genuine concerns about security when implementing cloud solutions: how secure are these hosted applications? Do static passwords provide sufficient protection against unauthorized access, data theft through phishing and key logging attempts? Application providers want to protect the data contained within their application from being compromised. 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.

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.

IDENTIKEY Authentication Server allows online application providers to integrate strong authentication and license protection directly into the application. IDENTIKEY Server can be linked to any web-based application via SOAP. As a result, it is the perfect security add-on for any SaaS application. It also uses a web based administration interface and reports user activity in HTML or XML format.

SERVICE PROVIDERS

IDENTIKEY Authentication Server is also tailored towards providers of managed services. IDENTIKEY can be hosted at a service partner who can offer it to his customers as an authentication service. By using authentication services, companies can focus on their core business while outsourcing the security aspect. These services usually come with monthly or quarterly invoicing, which makes it attractive from an accounting point of view.

IDENTIKEY Authentication Server is the perfect engine to drive authentication services:
- It is a complete flexible and scalable server solution
- Authentication requests for web applications can be forwarded through SOAP over SSL to the IDENTIKEY Authentication Server located at the service provider. Authentication requests coming through standard RADIUS equipment or internal websites can be forwarded through a VPN tunnel to the same IDENTIKEY Authentication Server
- Several customers can be hosted and managed by different delegated administrators
- Extensive reporting is available for customer invoicing

KEY FEATURES

- The SOAP interface allows IDENTIKEY Authentication Server to be linked to any web-based application
- IDENTIKEY Authentication Server offers license protection preventing account sharing and revenue loss
- IDENTIKEY Authentication Server enables service partners to offer authentication services to their customers
- IDENTIKEY Authentication Server provides ASPs with an authentication platform to independently manage and administer several customers
- Customer database can be set up in multiple domains with delegated administrators
- Customizable reporting facilitates invoicing
DIGIPASS Authentication for Windows Logon

DIGIPASS Authentication for Windows Logon, an extension to IDENTIKEY Authentication Server, is a cost-effective solution for enterprises wanting to protect their Windows PCs connected to the corporate network against unauthorized access. It allows users to log on to their Windows desktop on the network via a DIGIPASS-generated one-time password (OTP).

DIGIPASS Authentication for Windows Logon is installed as a small software module on the end user’s Windows environment. It can be installed on desktop PCs and laptops that are connected to the corporate network. As soon as ‘DIGIPASS Authentication for Windows Logon’ is set up, it replaces the original login window by a version that will send the login credentials to IDENTIKEY Authentication Server for verification. When the authentication request is positively validated, the original static password is sent back to the desktop and used for domain login.

When laptops are used outside the corporate network, for instance on the road or at home, the login module will work in unconnected mode, allowing the same strong authentication functionality as in connected mode. This prevents unauthorized access even when these laptops are unsupervised or stolen. If the computer works in unconnected mode, the login credentials are validated against a local database of one-time passwords. These OTPs are generated when the PC operates in connected mode, and they are securely encrypted and stored. With thousands of OTPs generated upfront, the user can work in unconnected mode for several weeks.
Virtual DIGIPASS

Virtual DIGIPASS is VASCO’s mobile SMS and e-mail-based authentication solution that is completely integrated into IDENTIKEY Authentication Server. It offers you a user-friendly and cost-efficient solution for strong user authentication and e-signatures.

The end user can request a one-time password to be delivered via SMS, PBX or e-mail before logging on. It adds another security layer to existing logon functions where static passwords are still in use. With Virtual DIGIPASS, your one-time password is sent by SMS to your portable device or by e-mail to your inbox. Delivering the OTP via a channel that is different from the channel in which the information is submitted, mitigates risks and decreases fraud vulnerability, bringing overall security to a higher level.

Virtual DIGIPASS can be used as a primary authenticator. The solution is compatible with regular cell phones, smart phones, tablets, text pagers and wireless PDAs eliminating the roll out of hardware and software-based authentication devices. It can be implemented for different services such as Internet banking, e-commerce, online applications and remote access. In addition, Virtual DIGIPASS can be used as a back-up authenticator in case the primary device is forgotten or unavailable.

FEATURES

- Uses out-of-band authentication (SMS, e-mail) increasing security
- Event-based and time-based one-time passwords are available
- OTP delivery via SMS message to your mobile phone
- OTP delivery via SMTP to your e-mail address
- OTP delivery via VASCO’s SMS service to your mobile phone
- OTP delivery via PBX system to your mobile phone
- Back-up solution for hardware DIGIPASS
- Also supports e-signature for transaction data validation

BENEFITS

- Highly secure out-of-band OTP delivery
- No extra hardware or logistics investment needed
- No additional authentication device needed (in primary mode)
- Wide range of OTP delivery methods (SMS, email, PBX system)
- Easy to distribute, maintain and deploy
- Fast time-to-market
- Low start-up cost
- Always available, business continuity option
PARTNERS AND DEDICATED MODULES

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 bundle or integrate their solutions with VASCO’s strong authentication solutions.

You benefit from easier and less costly integrations. By leveraging your authentication investments for multiple applications a high return-on-investment is ensured.

For a full overview of the VASCO partners, please visit: www.vasco.com/partners/partners/eco/catalog.aspx

Dedicated modules

VASCO has developed some specific dedicated modules to facilitate the integration of IDENTIKEY Authentication Server with partner products. The available plug-ins allow the seamless integration of DIGIPASS strong user authentication into partner products. As a result, customers can enhance the security of their existing remote access infrastructure at low cost. An overview and details on supported platforms can be found on www.vasco.com.

Available dedicated modules include:

**DIGIPASS Authentication for Juniper SBR**

Juniper Networks’ Steel Belted RADIUS server is a widely used AAA RADIUS server for secure network access. It supports the access technologies, user authentication stores and authentication protocols required by most enterprises. VASCO developed IDENTIKEY Authentication Server DIGIPASS Authentication for SBR, a plug-in which can be installed and configured on the SBR server. The module will forward all authentication requests arriving on the SBR to IDENTIKEY for validation.

**DIGIPASS Authentication for CA SiteMinder**

Computer Associates’ SiteMinder is a centralized Internet access management system that provides user authentication and single sign-on, identity federation and authorization services. It allows enterprises and large corporations to manage their remote access compliant to corporate regulations and policies. VASCO developed IDENTIKEY Authentication Server’s DIGIPASS authentication for SiteMinder, a plug-in that can be installed and configured on the SiteMinder server. The module will forward all authentication requests arriving on CA SiteMinder to IDENTIKEY for validation.
DIGIPASS AUTHENTICATION FOR MICROSOFT OUTLOOK WEB ACCESS (OWA)

Outlook Web Access is the web interface for Microsoft Exchange. It allows mobile or remote users to access their corporate e-mail system over the Internet. MS Exchange web logon uses by default the same user-ID and password as the host system. As a result, unauthorized users can gain access to mailboxes and other confidential data using those log-in credentials. DIGIPASS Authentication for OWA replaces the use of the static username and password by one-time password (OTP) technology using DIGIPASS strong authentication.

DIGIPASS Authentication for OWA can easily be installed and smoothly integrated with MS Exchange without special programming. It does not replace or change the underlying functionality of either MS Exchange or OWA. When installed, it will capture the login data and send an authentication request to IDENTIKEY Authentication Server. When validated, the actual user login and password will be injected into Outlook Web Access and MS Exchange for user logon. The DIGIPASS Authentication for Microsoft Outlook Web Access module adds an extra security layer to remotely access confidential information over unsafe networks at a low cost.

DIGIPASS AUTHENTICATION FOR CITRIX WEB INTERFACE (CWI)

VASCO strong user authentication easily integrates with Citrix Web Interface for XenApp and XenDesktop without undermining the existing functionality. At customer login, IDENTIKEY Authentication Server validates the submitted user credentials. Once validated, the user is granted access to all authorized applications.

By integrating directly with the Web Interface for Citrix XenApp, the new authentication process is transparent to the end user and does not require any additional steps or new log-on screens. The end user experience is unaffected, while the organization enjoys increased security provided by two-factor authentication.

In addition to the regular CWI, the DIGIPASS Authentication for Citrix Web Interface also supports connections from Citrix Receiver or PN Agent clients.

DIGIPASS AUTHENTICATION FOR MICROSOFT REMOTE DESKTOP WEB ACCESS (RDWA)

Remote Desktop Web Access (RD Web Access) enables users to access RemoteApp and Desktop Connection through the ‘Start’ menu on a computer that is running Windows 7 or through a web browser. RD Web Access includes Remote Desktop Web Connection, which enables users to connect remotely to the desktop of any computer on which they have Remote Desktop access.

VASCO’s DIGIPASS Authentication for Remote Desktop Access integrates with the Web Access interface that runs on an IIS webserver, and directs all authentication validation requests towards an IDENTIKEY Authentication Server.

As such, enterprises that deploy IDENTIKEY Authentication Server and DIGIPASS Authentication for Remote Desktop Access can be assured that unauthorized access through the Remote Desktop Web Access to corporate resources is impossible.
Extensions, modules and tools

ADDITIONAL TOOLS

Besides the features and functionality of IDENTIKEY Authentication Server, VASCO offers additional tools which facilitate the deployment, migration, management or daily operation of the authentication server as part of the security infrastructure.

LDAP SYNCHRONIZATION TOOL

The LDAP Synchronization Tool allows manually triggered, automated or scheduled synchronization of complete user accounts between the IDENTIKEY data store and a back-end LDAP directory. The LDAP Synchronization Tool reduces the administrative tasks associated with the creation, deletion or updating of users and assigned DIGIPASS for the IT administrator, since these tasks will be executed automatically.

With an IDENTIKEY database which is permanently up-to-date, administration or helpdesk interventions are reduced to the minimum, further improving the return on investment (ROI).

DATA MIGRATION TOOL

IDENTIKEY Authentication Server contains a Data Migration Tool for the migration of database information from other software towards a version that is compatible with IDENTIKEY. This allows customers using older versions of VASCO software or 3rd party plug-ins, to easily transfer their user database including all assigned DIGIPASS devices, personal and historical information towards the IDENTIKEY database.

PASSWORD SYNCHRONIZATION MANAGER

The Password Synchronization Manager will keep the users’ static password in the IDENTIKEY data store synchronized with the Active Directory password. When users need to update their Active Directory password because of expiration or other corporate compliance rules, the new password will be automatically copied to the IDENTIKEY database, where it is used for verification or replay in certain applications. Because the IDENTIKEY database is automatically updated, administration or helpdesk interventions for password recovery are reduced to the minimum, further improving ROI.

IJZA

The youth care institutions in North Brabant (Netherlands) developed a web-based application to register their youth welfare contacts in an efficient way. Because the information contained in the application database is extremely sensitive and confidential, IJZA was on the lookout for a strong authentication solution to securely access the web-based application. Two-factor authentication was a must. Mobility was another main concern as youth welfare services have a lot of ambulatory employees. Remote access was also a prerequisite because the application runs in-house, IJZA wanted a manageable and user-friendly solution. The combination of IDENTIKEY and DIGIPASS met all of IJZA’s requirements. It is a mobile solution allowing remote access. Furthermore IDENTIKEY has a user-friendly web interface allowing system administrators to manage and run the authentication solution effortlessly.
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. Users can securely switch between the different applications and collaborate with colleagues, business partners, suppliers, customers and partners using one single identity.

Besides acting as an identity provider and authentication manager, IDENTIKEY Federation Server also manages the access to the Internet-hosted applications by assuring that the user’s authentication level matches the level that the applications require. It also handles the flow of user attributes that are requested by the application.

IDENTIKEY Federation Server works as an identity provider within the local organization, but can also delegate authentication requests (for unknown users) to other identity providers. In a federated model, IDENTIKEY Federation Server does not only delegate, but also receives authentication requests from other identity providers, when local users want to access applications from other organizations within the same federated infrastructure.

IDENTIKEY Federation Server is extremely well suited for large corporations, governments, non-profit organizations and educational institutions looking to secure and manage access to different web-based applications and portals. With a continuous growing number of web-based applications, each requiring its own logon procedure, IDENTIKEY Federation Server reduces overall complexity and provides customers with an unprecedented user experience while offering secure two-factor based user authentication.
IDENTIKEY Appliance offers strong user authentication for local and remote access to the corporate network or to web-based business applications. The solution is suited for enterprises wanting a dedicated appliance for their authentication needs, without the hassle of installing and maintaining a software installation. IDENTIKEY Appliance is designed for corporations that want to avoid sharing server resources for too many business critical applications. As a result, they opt for a dedicated appliance to manage authentication requests without impacting the existing IT-infrastructure.

IDENTIKEY Appliance offers the full functionality of IDENTIKEY Authentication Server in an integrated, easy to maintain, 19” rack mountable appliance. In combination with any DIGIPASS® authenticator, it replaces the user’s static passwords with one-time passwords (OTPs) to access the corporate network and its business applications from any remote location.

Multiple hardware versions are available for the smallest SME as well as for the largest multi-national depending on the number of users. Each appliance allows replication towards any other appliance, ensuring the highest availability and adjusted performance at each remote site.

Available hardware versions:

- **AG3000 Series** is suited for smaller businesses or small remote sites. It is a silent, low-power consuming 1U 19” rack server, that has all the features and functionalities of IDENTIKEY Authentication Server.

- **AG5000 Series** is a standard 1U 19” rack server, suited as main appliance for all business environments. It can authenticate up to 10,000 users. It is the ideal appliance to secure VPN, web and Windows logon in large enterprises.

- **AG7000 Series** is a complete redundant 2U, 19” rack server. With its dual core processor, 12 GB of RAM and 1TB hard disks in RAID 1, it is the ideal server for business-critical applications or it can function as the reporting and failover system for medium to large enterprises.

The embedded LDAP Synchronization Tool enhances security and minimizes the administrative tasks of user management. Updates on the user management in Microsoft Active Directory, Novell e-Directory or any other LDAP depository are automatically synchronized towards Identifier, minimizing the administrative tasks of user management.

IDENTIKEY Appliance has extensive reporting and auditing functions. The audit console monitors incoming and outgoing RADIUS and web authentication requests. Functionality statistics allow administrators to easily manage the remote access environment, standard and customized XML reports and extensive log searching.

**BENEFITS**

- Easy to install and administer
- Completely managed server
- An intuitive web-based user interface with wizards
- Programmable back-up function
- Automatic updates with a complete fail safe mechanism
- Dedicated task assignment self-registration for end users
- Remote or outsourced administration
- Hardware and software monitoring with SNMP traps
IDENTIKEY Virtual Appliance is VASCO’s hypervized version of the successful IDENTIKEY Appliance series. IDENTIKEY Virtual appliance complements VASCO’s IDENTIKEY Appliance product range offering hypervisor remote access security providing customers with the flexibility to choose the deployment model that best meets their unique security requirements.

The virtual appliance delivers the same unmatched security features and functionality as the current stand-alone hardware IDENTIKEY Appliance. Offering the many benefits of virtualization such as cost savings, rapid deployment and provisioning, simplified policy management and a web-based administrator interface, IDENTIKEY Virtual Appliance is an excellent choice for organizations that have developed a virtualization strategy and are looking to move their security infrastructure to a virtual environment.

IDENTIKEY Virtual Appliance validates DIGIPASS generated one-time passwords and e-signatures to secure remote access to corporate networks and web-based applications, offering high-level security by replacing weak static passwords.

The appliance is supported on the most popular hypervisor products, guaranteeing a widespread acceptance. IDENTIKEY Virtual Appliance comes in 4 models targeted towards different user numbers, with different numbers of supported CPU Cores and assigned memory.

**BENEFITS**

- Easy to install and administer as a virtual application
- Different models target different numbers of users
- Completely managed server
- An intuitive web-based user interface with wizards
- Programmable back-up function
- Automatic updates with a complete fail safe mechanism
- Dedicated task assignment
- Self-registration for end users
- Remote or outsourced administration
- Affordable for small installations, robust for large deployments
DIGIPASS Pack for Remote Authentication

DIGIPASS Pack for Remote Authentication is specifically designed for small and medium-sized businesses’ secure remote access to sensitive information and internal applications. It is designed for organizations with limited IT resources and budgets and carries all functionalities of an ‘à la carte’ authentication solution.

The pack contains DIGIPASS hardware or software authenticators to generate strong one-time passwords (OTP) to replace insecure, static passwords used during logon procedures. IDENTIKEY Authentication Server verifies the authentication request on the back-end and validates it if it matches the OTP generated on the server side.

The packaged solution contains all necessary hardware and software for a simple two-factor authentication rollout, allowing you to have your authentication project up and running in a day. It is highly scalable, allowing you to add more users and applications when required.

DIGIPASS Pack for Remote Authentication does not change the underlying functionalities of your existing IT infrastructure and applications. It is compatible with most firewalls, access servers, and all RADIUS-based VPNs and supported by over 200 leading application providers. DIGIPASS Pack will interface with any RADIUS client without additional programming requirements. The authentication solution resides on your existing server and involves minimal setup and management. There is no client software required and companies can secure access to their VPN and SSL VPN without extensive system modifications.

DIGIPASS Pack for Remote Authentication is ideally suited for:
- Remote access to internal networks via firewall or SSL VPN
- For traveling staff, home workers, remote offices, business partners, consultants, etc.
- Intranets, extranets, and in-house web applications
- expansion is available for browser-based applications, such as Citrix CWI and SharePoint or Webmail access, such as OWA
AFTER SALES OFFERING

VASCO PROFESSIONAL SERVICES

The implementation of two-factor authentication has many facets: VASCO Professional Services have been designed to assist customers in the deployment of their authentication project. By sharing expertise, VASCO helps you to minimize the challenges and maximize the results by providing them peace of mind throughout the deployment of the project.

The roll-out of a two-factor authentication project is not only about IT-security, it involves the input from other departments as well. As a result it requires a structured approach and careful thought about project management, fulfillment, marketing, IT security, deployment, helpdesk support and many others.

VASCO experts will:

- Manage your authentication project
- Help you with technology choices
- Provide advice on marketing strategy
- Integrate the application
- Manage the fulfillment and stock
- Organize helpdesk support

Our experts will use VASCO’s proven 4-step methodology, taking you from a generic security enhancement objective to a tailored deployment fitting your specific security needs.

VASCO has a number of specific IDENTIKEY based professional services, including:

- IDENTIKEY Authentication Server large deployments module
- IDENTIKEY Authentication Server Installation Package
- IDENTIKEY Authentication Server Integration Package
- IDENTIKEY Authentication Server Provisioning Package

VASCO CONSULTING SERVICES

VASCO Consulting Services have been designed to complement our offering of strong authentication solutions with quality services that help customers to make the most of their authentication investments.

Whether you are looking for information about current security challenges and threats in e-banking, e-commerce or network security, whether advice is needed prior to or during the implementation, VASCO can offer its expertise.

By sharing expertise, proven methodology and best practices, VASCO can help its customers in decreasing time to market of their authentication project.

More detailed information on VASCO’s consulting offer is available on: www.vasco.com/consulting
VASCO’s Security Experts Academy & e-Learning platform (SEAL)

New types of online attacks emerge almost every day; therefore it is critical for IT security professionals to stay informed and 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, resellers and anybody who needs our advice.

SEAL is VASCO’s worldwide community of security professionals. The SEAL training offer consists of general IT security topics. VASCO product training will help people who want to have a career in information security. Through our offering of classroom training, e-learning or DVD-based training and forums, VASCO SEAL allows customers and partners 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

More information is available on: www.vasco.com/training

Support

VASCO technical support is available in a number of pre-defined support packages. Our support plans consist of:

- Standard Monday to Friday business hours support
- 24/7 support
- VIP support using SLAs adapted to specific customer needs
- Pay-per-incident
- Remote assistance

More information on the specific support plans is available on: www.vasco.com/support

VASCO Labs

VASCO offers the possibility to try the wide range of security products online:

- IDENTIKEY Authentication Server
- IDENTIKEY Virtual Appliance
- IDENTIKEY Federation Server
- Available online, from your browser
- Login secured by MYDIGIPASS.COM

More information on the specific support plans is available on: http://labs.vasco.com
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 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.