IDENTIKEY Server
VASCO’s next generation authentication server

DIGIPASS BY VASCO

The world’s leading software company specializing in Internet Security
SECURE YOUR BUSINESS

Nowadays, every company is dependent 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 hosted applications; also known as SaaS or on-demand applications. The application is offered as a service and runs in the user’s Internet browser, usually with minimal platform requirements and low operational costs. When implementing hosted applications, IT administrators genuinely worry about security of business critical data stored in these applications. How are the accounts protected in an Internet-based application? Is the sensitive information safe in the hands of a third party? Are confidential data only accessible by authorized users?

REPLACING STATIC PASSWORD BY ONE-TIME PASSWORDS (OTP)

Whether facing data theft, phishing or man-in-the-middle scams, regular static passwords no longer provide sufficient protection. Static passwords can easily be guessed, copied, exchanged, shared, and misused. Simple passwords are easy to remember but are highly unsecure. Complex passwords are more secure but are often written down, thus compromising the security. Two-factor authentication has proven to be the best countermeasure against hacking and password fraud.

As the global leader in two-factor authentication solutions, VASCO Data Security provides mature technology with a minimal impact on 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

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 passwords and e-signature to protect online transactions. With IDENTIKEY®, VASCO introduces affordable two-factor authentication offering the same high-level security to enterprises as used in the financial world to help protect them against unauthorised network access and protect their applications.
IDENTIKEY Server

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

Built around VASCO’s core VACMAN authentication platform, IDENTIKEY Server is flexible yet robust enough to offer the highest level of security in an administrative friendly package. Developed using industry standards for data communication, it is a good fit for large and small enterprise network security implementations, application security and online banking security.

IDENTIKEY Server works well with most remote access tools such as SSL-VPN, firewalls, intranets, extranets, and a variety of web applications. It can run on Windows and Linux platforms without causing any of the headaches commonly associated with the maintenance of two-factor authentication systems.

IDENTIKEY Server is robust and scalable, and supports a user load from tens to millions. Server failover and database replication are available for larger deployments.

Leverage existing infrastructure

IDENTIKEY Server integrates seamlessly 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. IDENTIKEY interfaces with several RADIUS authentication servers and can perform LDAP lookup on AD, ADAM, and eDirectory.

IDENTIKEY Server was designed with web functionality in mind. IDENTIKEY Server can also 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

IDENTIKEY 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 for remote management and brings new opportunities for providers of outsourced services.

IDENTIKEY Server has an extensive reporting functionality allowing to create useful summaries on user history, DIGIPASS activities,… These reports, together with the security audit function, can provide crucial input for helpdesk and accounting purposes.

Smooth rollout

IDENTIKEY offers an intuitive installation wizard to guide 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.

IDENTIKEY 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.

Adding more users and/or applications is as simple as purchasing more licenses. The built-in automated deployment feature reduces the helpdesk involvement. 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 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 Server, end-users will be equipped with a DIGIPASS client device. VASCO’s DIGIPASS family offers a wide range of end-user authentication devices which all work with IDENTIKEY. Customers can choose from a wide range of authenticators, both software (in the browser, on the mobile) and hardware based, which best fit their needs. All DIGIPASS authenticators are fully customizable with the customer’s logo and corporate colors.

IDENTIKEY

Secures remote access for remote offices and travelling staff
Secures local network login via wireless access point or Windows Desktop
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.
SECURE ONLINE BANKING

IDENTIKEY Server is a perfect fit for banks wanting to implement a strong authentication solution without dedicating significant budget and resources or that want to avoid large integration projects. It is also suited for banks in need of a dedicated authentication server solution. With IDENTIKEY, 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 provides two-factor authentication for customer 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 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 Server offers optimal security since cryptographic keys cannot be compromised.

IDENTIKEY Server is tailored towards financial service providers who 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 the core business. These services are invoiced on a monthly or quarterly basis, thus making them attractive from an accounting standpoint (cash handling, budget control, investment management, etc).

KEY FEATURES

- Helps 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 reporting functionality
- IDENTIKEY Integration Program brings administrators up-to-date in a few days
- Support for EMV-CAP and Hardware Security Module (HSM)
IDENTIKEY in application security

IDENTIKEY FOR SOFTWARE AS A SERVICE

Software deployments are shifting from a traditional approach where programs are installed on individual computers towards a model where software and applications are offered in an "on-demand" model. Software as a Service vendors host the application, customers pay a subscription fee to use it. When using hosted applications, IT administrators are generally concerned about the security: how do you protect the account, is the information safe in the hands of a third party supplier, can only authorized users access my sensitive data,…

By replacing insecure static passwords with one-time passwords, VASCO enhances application security. Sensitive information is only available to authorized users after they have proven their identity. Data theft and account sharing is no longer possible. 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.

OPPORTUNITIES FOR SERVICE PROVIDERS

IDENTIKEY 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 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 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 Server.
- Several customers can be hosted and managed by different delegated administrators
- Extensive reporting is available for customer invoicing

PROTECT YOUR COMPLETE ENTERPRISE WITH IDENTIKEY

Besides protecting your Internet applications, IDENTIKEY Server offers various extensions to secure employee remote access to the corporate network and resources. Home workers, remote branch offices, traveling staff, and road warriors can use the same DIGIPASS technology to safely connect through firewall VPN, SSL-VPN, or any other RADIUS equipment to the corporate LAN to access data, documents, applications. Additionally, company portals, Outlook Web Access e-mail, and Citrix Web Interface applications can be protected with strong user authentication at the same time.

KEY FEATURES

- The SOAP interface allows IDENTIKEY Server to be linked to any web-based application
- IDENTIKEY Server offers media publishers and SaaS providers a way to avoid account sharing thus ensuring revenue streams
- IDENTIKEY Server enables Service Partners to offer authentication services to their customers
- IDENTIKEY Server provides ASPs with an authentication platform to independently manager and administer several customers
- Customer database can be setup in multiple domains with delegated administrators
- Customizable reporting facilitates invoicing
DIGIPASS AUTHENTICATION FOR WINDOWS LOGON

DIGIPASS Authentication for Windows Logon, an extension to IDENTIKEY 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 setup, it replaces the original login window by a version that will send the login credentials to IDENTIKEY 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 log-on 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 is working 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.

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.
PARTNERS AND DEDICATED MODULES

VASCO has developed a DIGIPASS Ready Partner Program to facilitate the compatibility of solutions from other technology vendors with VASCO DIGIPASS. Solution partners are able to bundle their solutions with VASCO strong authentication or to develop new solutions integrating VASCO authentication.

Customers benefit from easier and less costly integrations. They are able to leverage their authentication investments by using the authentication infrastructure and the DIGIPASS they already have for multiple applications ensuring a high return-on-investment for the customer.

For a full overview of the VASCO partners, visit: www.vasco.com/solutions/partners.

Dedicated modules

VASCO has developed some specific dedicated modules to facilitate the integration of IDENTIKEY 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 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 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 log-on 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 VASCO DIGIPASS strong authentication.

DIGIPASS Authentication for OWA can easily be installed and integrates smoothly with 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 Server. When validated, the actual user login and password will be injected into Outlook Web Access and MS Exchange for user log-on. 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 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.

“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.”

Marc B. Templeton, President and CEO of Citrix
Extensions, modules and tools

ADDITIONAL TOOLS

Besides the features and functionality of IDENTIKEY Server, VASCO is offering 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, as 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).

Password Synchronization Manager

The Password Synchronization Manager will keep the user’s 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.

Data Migration Tool

IDENTIKEY Server contains a Data Migration Tool for the migration of database information from other software towards a version which is compatible with IDENTIKEY. This allows for customers using older versions of VASCO software, such as VACMAN Server, VACMAN Middleware or 3rd party plug-ins, to easily transfer their users database including all DIGIPASS, personal and historic information towards the IDENTIKEY database.
DIGIPASS Pack for Remote Authentication

DIGIPASS Pack for Remote Authentication is specifically designed for small and medium size businesses to provide a high level of security to sensitive information and internal applications from a remote location without compromising security or user convenience. It is designed for organizations with limited IT resources and budgets and carries all functionalities of an ‘à la carte’ authentication solution. The packaged solution contains all necessary hardware and software for a simple two-factor authentication rollout, allowing the customer to be up and running in a day. It is highly scalable, allowing you to add more users and applications when required.

End-users simply press the button of their authenticator or activate the authentication application on their mobile phone to generate an OTP. The end-user enters this OTP into the login screen on his computer along with a PIN. IDENTIKEY Server verifies the authentication request on the back-end and validates it if it matches the OTP generated on the server side. A new OTP will be generated at each login.

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 with no 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

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.
Appliances

aXsGUARD Identifier

aXsGUARD Identifier is suited for enterprises that want a dedicated appliance for their authentication needs, without the hassle of installing and maintaining a software installation. aXsGUARD Identifier offers strong user authentication for local and remote access to the corporate network or to web-based business applications. aXsGUARD Identifier offers full IDENTIKEY Server functionality in an integrated, easy to maintain 19” rack mountable appliance.

The solution has been 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. Multiple hardware versions are available for the smallest SME and to 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:

- **AG3442** is suited for smaller businesses or small remote sites. It is a silent, low power consuming 1U 19” rack server, which still has all the features and functionality of IDENTIKEY and Identifier.
- **AG5502** is a standard 1U 19” rack server, suited as main appliances 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.
- **AG7552** 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.

Thanks to LDAP synchronization, the user management only happens in the main LDAP database (Microsoft Active Directory, Novell e-Directory, or any other LDAP) the company is using. This enhances security and minimizes the administrative tasks of user management.

aXsGUARD Identifier 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 manage
- An intuitive web-based user interface with wizards
- Automatic updates with a complete fail safe mechanism
- Dedicated task assignment allowing to delegate tasks (user, DIGIPASS management, reporting)
- Self registration for end-users
- Remote or outsourced administration
- Remote support (according to maintenance contract)
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, we help our customers 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 a result it requires a structured approach and careful thought about project management, fulfillment, marketing, IT security, deployment, helpdesk support and many others.

Our experts will:
- Manage the authentication project,
- Help customers with technology choices
- Provide advice on marketing strategy
- Integrate the application
- Manage the fulfillment and stock
- Organize helpdesk support.

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

VASCO has a number of specific IDENTIKEY based professional services, including:
- IDENTIKEY Server large deployments module
- IDENTIKEY Server Installation Package
- IDENTIKEY Server Integration Package
- IDENTIKEY 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 an implementation 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 our 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 and 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 consists 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
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.

www.vasco.com

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

OPERATIONAL HQ
BRUSSELS
phone: +32.2.608.97.00
demail: info_europe@vasco.com

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

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

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

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

YOUR LOCAL OFFICE