



Identikey Server 3.0

DIGIPASS authentication and transaction validation server

Identikey Server 3.0 is a software suite for organizations of all sizes that need to authenticate remote users for access to enterprise networks and its applications. This state-of-the art VASCO product is used to verify authentication requests and to centrally administer user authentication policies. Identikey Server 3.0 and VASCO's DIGIPASS authenticators provide affordable strong authentication and secure access to web applications and virtual private networks. Identikey Server 3.0 is built around VASCO's solid and proven VACMAN core authentication technology and can be flexibly tuned towards the customer's needs for integration in existing business applications. The web-based administration interface of Identikey Server 3.0 offers far-reaching opportunities (such as remote management) and opens new markets for suppliers of Managed Security Services as well as Application Service Providers.

Remote access is one of the most valuable - and most vulnerable - features in a corporate network. Today you simply cannot afford to leave your systems and valuable corporate data unprotected. Identikey Server 3.0 is the simple and cost-effective solution to help you authenticate remote users requesting access to your network.

Using an individually assigned DIGIPASS authenticator, your remote users will be able to prove their claimed identity quickly and easily 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.

Addressing the need for e-signatures in commercial and banking web-based applications, such as online shops, B2B portals and online retail banking, Identikey Server 3.0 offers authentication and validation of transaction signatures.

VASCO offers a wide range of DIGIPASS authenticators that can store several dedicated OTP generation and e-signature applications.

With the increasing number of mobile employees and home-based staff, the need for web-based corporate applications and web-based file access has surged.

Network administrators face new challenges to fulfil growing requests for flexible yet secure access to applications like Outlook Web Access or Citrix Web Interface need to be protected with strong authentication. Identikey Server 3.0 provides an answer to these demands by providing secure authentication for many web-based applications.

Large corporations and demanding customers who offer web-based business solutions can benefit from Identikey's SOAP-based API's for seamless integration of the authentication software into their applications.

Advanced Product Trainings and consultancy services are part of VASCO's offerings to complete any Identikey Server 3.0 integration.

Integration into a customer's web-based application is available through the use of SOAP API's for Authentication, Signature Validation, Administration, Provisioning and Reporting.

FUNCTIONS

- Verification of authentication requests (DIGIPASS One Time Password, DIGIPASS Signature)
- Central administration of users, DIGIPASS authenticators and authentication policies
- Software DIGIPASS provisioning (DIGIPASS for Web, DIGIPASS for Mobile Phone)

FEATURES

- Strong DIGIPASS based two-factor authentication
- e-Signature
- Policy based authentication
- Web-based administration GUI
- Delegated administration
- Bulk management and auto management
- Flexible DIGIPASS assign procedures
- Dynamic user registration
- Password auto learning
- DIGIPASS authenticator auto assign
- Virtual DIGIPASS (SMS-based) support
- Support of radius and webserver based clients
- ODBC database support
- Support of multiple backend authentication environments
- XML-based reporting
- Comprehensive audit system
- Reporting in XML/HTML format

BENEFITS

- Strong authentication without the hassles
- Designed to fit the needs of any size organization
- 'Out-of-the-box' solution, yet flexible towards integration
- Easy to integrate, administer and audit
- No software installation on client PCs
- Seamless solution; easy to use
- Extremely low 'total cost of ownership'
- High Availability: Server Replication and Load Balancing



STRONG, TWO FACTOR AUTHENTICATION

The combination of Identikey Server 3.0 and DIGIPASS authenticators provides a much more reliable form of user authentication than reusable static passwords and can be easily implemented. It's a turnkey solution that can be up and running in a very short time.

TRANSACTION VALIDATION

Based on transaction validation techniques that are in place at numerous banks and financial institutions around the world, Identikey Server 3.0 offers an electronic signature system. VASCO provides an SDK that allows smooth integration of this signature validation functionality into existing web-based applications.

This brings the same level of security and confidentiality of online banking to other markets that require transaction validation.

WEB-BASED USER INTERFACE

All administration functions are conveniently available through a web-based user interface, allowing remote administration and creating new opportunities for managed security services providers.

WIDE RANGE OF SUPPORTED DATABASES

Identikey Server 3.0 supports ODBC compliant databases, such as Oracle 10g (32-bit) and 11g (64-bit), Microsoft SQL server 2005, IBM DB2 8.1 (32-bit) and 9.1 (64-bit), Sybase Adaptive Server Anywhere 10.0 and PostgreSQL 8.2.5.

Identikey Server 3.0 comes standard with PostgreSQL (32-bit).

AUDITING AND REPORTING

The audit console monitors incoming and outgoing radius and web traffic (and several other events) on the Identikey Server 3.0. Informational statistics gathered by the audit console provide critical details necessary to effectively manage your remote access environment. Extensive XML or HTML-formatted reporting is provided for helpdesk troubleshooting, system and security auditing and accounting.

INTEROPERABILITY

Hardware or software conflicts are no concern, Identikey Server 3.0 uses a non-intrusive method of enabling DIGIPASS authentication. Simply position Identikey Server 3.0 between the Network Access Server and your existing RADIUS server; the performance will be unaffected.

MULTI-PLATFORM

Offering a broad choice of supported platforms, Identikey Server 3.0 can be conveniently used on most common Server Operating Systems in Enterprises, such as MS Windows and Linux, both in 32 and 64 bit.

About VASCO

VASCO designs, develops, markets and supports patented DIGIPASS®, DIGIPASS PLUS®, VACMAN®, IDENTIKEY® and aXs GUARD® authentication products for the financial world, remote access, e-business and e-commerce. With tens of millions of products sold, VASCO has established itself as the world leader in Strong User Authentication for e-Banking and Enterprise Security for blue-chip corporations and governments worldwide.

www.vasco.com

BRUSSELS (Europe)

phone: +32.2.609.97.00
email: info-europe@vasco.com

BOSTON (North America)

phone: +1.508.366.3400
email: info-usa@vasco.com

SYDNEY (Pacific)

phone: +61.2.8061.3700
email: info-australia@vasco.com

SINGAPORE (Asia)

phone: +65.6323.0906
email: info-asia@vasco.com

TECHNICAL SPECIFICATIONS

Operating System (Windows version)	<ul style="list-style-type: none"> Windows Server 2003 (32 & 64 bit) with SP1 and above, or R2
Operating System (Linux version)	<ul style="list-style-type: none"> Novell SUSE Linux Enterprise Server 10 Ubuntu 6.06 Server Edition Red Hat Enterprise Linux version 5 32 and 64 bit versions
Processor	Pentium 500 MHz or faster The following conditions may increase the load of the CPU: <ul style="list-style-type: none"> High number of authentication / accounting / signature validation / provisioning / reporting requests RADIUS requests proxied to RADIUS server One or more audit consoles active One or more administrative sessions active ODBC auditing enabled
Memory	Minimum RAM capacity of 512 MB The following conditions may increase memory size requirements: <ul style="list-style-type: none"> User cache enabled with a large number of users to be cached Extensive reporting
Disk Space	Minimum disk space of 200 MB. Recommended at least 500 MB free space. The following conditions may increase disk space requirements: <ul style="list-style-type: none"> Large number of user and token records High number of reports Audit log files that are not archived Server tracing option enabled
Winsock	Version 2.0 or above

COMPLIANCE TO STANDARDS

RADIUS	RFC 2865 and 2866
Authentication	<ul style="list-style-type: none"> DIGIPASS OTP (Challenge / Response, Response Only) DIGIPASS Signature (transaction validation) OATH

www.identikey.com