



IDENTIKEY Authentication Server 3.8

IDENTIKEY Authentication Server is an authentication software suite for organizations of all sizes that want to address their concerns about secure access to internet applications with a state-of-the-art solution for strong user authentication. This datasheet intends to highlight the technical specifications of the IAS3.8 release. For further information, please refer to the identikey.com website.

ONLINE BANKING

IDENTIKEY Authentication Server 3.8 offers strong authentication and validation of transaction signatures to address the need for e-signatures in commercial and banking applications. Closely integration of Mobile DIGIPASS and Crontosign Color QR code allows for the highest user convenience while maintaining the highest security.

A dedicated dashboard allows helpdesk staff – whether internal or outsourced – to help the endusers in the most efficient and time-saving way. Optional support of EMV-CAP and HSM allows OTP and signature validation inside a tamper-proof security module. IDENTIKEY Authentication Server 3.8 is designed according to PCI-DSS regulations and can immediately be integrated into existing banking infrastructures.

REMOTE ACCESS IN ENTERPRISE SECURITY

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

Network administrators face new challenges to fulfill growing requests for flexible yet secure access to file servers, mail servers, intranet, in-house applications and virtual environments as they need to be protected with strong authentication.

IDENTIKEY Authentication Server 3.8 provides the answer to these demands by offering secure authentication for remote access and login to web-based applications.

SOFTWARE AS A SERVICE

A number of industry analysts have highlighted the emerging trend of Software as a Service. Also known as on-demand applications or hosted applications, this new form of software deployment is slowly replacing the more traditional, desktop-based software.

IDENTIKEY Authentication Server 3.8 can be integrated using SOAP into any Internet application to protect the user login with strong authentication.

FEATURES

- DIGIPASS two-factor authentication
- e-Signature for transaction data validation
- Support for EMV-CAP and Hardware Security Module (HSM)
- Crontosign Color QR Code support
- Support of RADIUS and Microsoft IIS web server based clients (Outlook Web Access, Citrix Storefront, Remote Desktop Web Access)
- Support of Office365 via ADFS3.0 and SBR via dedicated modules
- Support for Internet hosted applications via SOAP
- Active Directory integration, ODBC database support
- Support of LDAP back-end authentication environments
- Enhanced features for DIGIPASS- and user management
- Delegated administration, multiple administration interfaces
- Dedicated Helpdesk dashboard
- Virtual DIGIPASS (OTP delivery via SMS or Email) (Out-of-Band)
- Support of wireless protocols & the return of RADIUS attributes

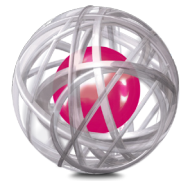
FUNCTIONS

- Verification of authentication requests (OTP, signature)
- Validation of DIGIPASS Authentication for Windows Logon for locally connected users, in online and offline mode
- Web-based administration GUI offers all administration functions in a single browser window.
- Central administration of users and DIGIPASS authenticators
- Dedicated dashboard page targeted at Helpdesk department
- Software DIGIPASS provisioning (DIGIPASS for Mobile/Apps)
- Comprehensive audit system, with storage in a database or text file and an optional live audit viewer.
- Activity reporting with output in XML/HTML format
- Validation of DIGIPASS Authentication for Windows Logon for locally connected users, in online and offline mode
- SNMP Monitoring

BENEFITS

- Easy to implement strong user authentication
- Robust and scalable, easy expandable with users and applications
- VACMAN core technology: proven at major banks worldwide
- Highest user experience by Color QR Code scanning
- Designed to fit the needs of an organization of any size
- 'Out-of-the-box' solution, flexible to allow custom integration
- Easy to install, administer and support
- Easy to integrate in existing infrastructure
- Smooth migration, updates and maintenance
- High availability through server replication and load balancing
- Extremely low TCO 'total cost of ownership'
- Efficient and time-saving tools for Helpdesk staff
- Available as Appliance or Virtual Appliance platforms
- Can be extended with Single Sign On module for Web Applications (IDENTIKEY Federation Server)

For more information, please visit
www.identikey.com



STRONG, TWO FACTOR AUTHENTICATION

The combination of IDENTIKEY Authentication Server 3.8 and DIGIPASS provides strong user authentication that offers a higher security compared to reusable static passwords. IDENTIKEY Authentication Server 3.8 can be easily implemented in any IT environment and provides a turnkey solution that can be operational in a very short time.

TRANSACTION VALIDATION

IDENTIKEY Authentication Server offers highly secure electronic signature validation for banks and financial institutions. Support for EMV-CAP support and Hardware Security Module (HSM) to validate the signature in a secure and tamper-proof environment, are optional. By using the latest Crontosign technology, users can enjoy the best experience for their online banking by simply scanning a Color QR Code in order to log in or confirm a transaction.

INTEROPERABILITY AT THE FRONT-END

IDENTIKEY Authentication Server 3.8 uses a non-intrusive method of enabling DIGIPASS authentication. It can be integrated using RADIUS, with Microsoft IIS-based applications such as Outlook Web Access, Citrix StoreFront or Microsoft RDWeb Access, or with any Internet application using SOAP. Additional modules are available for direct plugin in various 3rd party systems, such as Juniper SBR and Microsoft ADFS3.0.

WIDE RANGE OF SUPPORTED DATABASES

IDENTIKEY Authentication Server 3.8 supports a wide range of ODBC compliant databases for data storage and ships standard with PostgreSQL. The highest convenience and efficiency when adding strong authentication to a group of users, is achieved by using the Active Directory service. The DIGIPASS related data can be stored with the users in the Active Directory.

ADMIN GUI AND HELPDESK DASHBOARD

All administration functions are available through a web-based user interface, allowing remote administration and creating new opportunities for managed security services providers. A dedicated overview of all functions that are required and used on a daily basis by helpdesk staff, allows support of the enduser to be done in a most efficient and timesaving way.

AUDITING AND REPORTING

The audit console monitors incoming and outgoing events on the IDENTIKEY Authentication Server 3.8. Informational statistics gathered by the audit console provides critical details necessary to effectively manage a remote access environment. Extensive XML or HTML-formatted reporting is provided for helpdesk troubleshooting, system- and security auditing and accounting purposes.

FITS IN ANY ENVIRONMENT

IDENTIKEY Authentication Server 3.8 is available in the widest range of supported platforms: Windows Server, Suse-, Ubuntu- and RedHat distributions, VMWare, Hyper-V and Citrix virtual environments as well as dedicated appliance formats.

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

SUPPORTED ENVIRONMENTS

(for more details, please see the IDENTIKEY Installation Guides, System Requirements)

Operating System (Windows version)	<ul style="list-style-type: none"> Windows Server 2008 (64-bit) with SP2, 2008R2 with SP1 (64-bit) Windows Server 2012 (64-bit), 2012R2 (64-bit) SBS2008 SP2+(64-bit), SBS2011(64-bit) Windows Server 2012 Essentials (64-bit), 2012R2 Essentials (64-bit)
Operating System (Linux version)	<ul style="list-style-type: none"> Suse Linux Enterprise server 11SP3 (64-bit) Ubuntu Server 12.04.03 LTS, 14.04.02 LTS (64-bit) Redhat Enterprise Linux version 6.6 (64-bit) CentOS 6.6 (64-bit)
Supported Windows Client	<ul style="list-style-type: none"> Windows 7 (64 bits) Windows 8 (64 bits) Windows 8.1 (64 bits) <p>* Can be used for very small deployments as well as for testing and demonstration purposes</p>
Virtual Images	<ul style="list-style-type: none"> VMWare ESXi Server version 5.5 Citrix XenServer 6.2 Microsoft Hyper-V (WS2008R2, WS2012, WS2012R2)
Supported Webservers	<ul style="list-style-type: none"> Apache Tomcat 8.0.21 IBM WebSphere Applications Server 8.5.5 <ul style="list-style-type: none"> Should include Java: JRE8, JSP2, JS2.4
Supported Webrowsers	<ul style="list-style-type: none"> Chrome 41, Firefox ESR31, Internet Explorer 9, 10, 11
Data store (DBMS)	<ul style="list-style-type: none"> Oracle 11gR2 (64-bit, Linux, Windows) Microsoft SQL Server 2008SP3, 2008R2SP2, 2012SP1, 2014 (Windows) PostgreSQL 9.2.7 (Linux, Windows)
Data store (Active Directory)	<ul style="list-style-type: none"> Windows Server 2008 AD, 2008R2 AD Windows Server 2012 AD, 2012R2 AD
LDAP Back End Authentication	<ul style="list-style-type: none"> Windows Server 2008 AD, 2008R2 AD Windows Server 2012 AD, 2012R2 AD Novell e-Directory 8.8 SP8 IBM TAM Directory Server 6.3
HSM	<ul style="list-style-type: none"> Safenet ProtectServer Gold, Orange, Express Thales nShield Connect, Solo (on selected platforms)

COMPLIANCE TO STANDARDS

RADIUS	RFC 2865 and RFC 2866
Wireless	EAP, PEAP
Authentication	<ul style="list-style-type: none"> DIGIPASS OTP (Challenge / Response, Response Only) DIGIPASS Signature (transaction validation) OATH (event based – time based) EMV-CAP