IDENTIKEY Authentication Server 3.15

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 IAS3.15 release. For further information, please refer to the identikey.com website.

ONLINE BANKING APPLICATIONS

IDENTIKEY Authentication Server 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 CRONTO® 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 is designed according to PCI-DSS regulations and can immediately be integrated into existing banking infrastructures.

Administrative actions that require a higher security level can be managed by the Maker/Checker principle.

REMOTE AND LOCAL ACCESS TO EMPLOYEE APPLICATIONS

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

An intuitive SelfManagement Website allows endusers to manage (part of) their Hardware and Software DIGIPASS without Helpdesk intervention, thus freeing up admin resources.

Windows Desktop login with 2FA is achieved by a dedicated Credential Provider that allows login with OTP or Push Notification on PC's, laptops and Windows servers, both in online and offline mode.

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 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)
- CRONTO 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 ADFS3.0/4.0 and SBR
- Support of 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
- Enduser Self-Management Website
- 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 (W7, W8.1, W10)
- 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 staff
- 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
- Support of Push Notification for e-Signature, WebApplication Login and Remote Access login
- 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)
- Helps customers to be GDPR compliant

VASCO
TRUST FOR THE DIGITAL WORLD

IDENTIKEY

STRONG, TWO FACTOR AUTHENTICATION

The combination of IDENTIKEY Authentication Server and DIGIPASS provides strong user authentication that offers a higher security compared to reusable static passwords. IDENTIKEY Authentication Server 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 Cronto 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 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 ADFS3.0/4.0.

WIDE RANGE OF SUPPORTED DATABASES

IDENTIKEY Authentication Server 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. 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 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.

SUPPORTED ENVIRONMENTS

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

Operating System (Windows version)	• Windows Server 2008 R2 with SP1 (64-bit) • Windows Server 2012 (64-bit), 2012 R2 (64-bit) • Windows Server 2012 Essentials (64-bit), 2012 R2 Essentials (64-bit) • Windows Server 2016
Operating System (Windows desktop)	• Windows10 (Including Builds 1511, 1607, 1703, 1709) • Windows Server 2016
Operating System (Linux version)	• SUSE Linux Enterprise Server 11, 12 (64 bit) • Ubuntu Server 14.04 LTS, 16.04 LTS (64-bit) • RedHat Enterprise Linux version 6.7, 7.x (64-bit) • CentOS 6.x, 7.x (64-bit)
Virtual Images	• VMWare ESXi Server version 5.5, 6.0, 6.5 • Citrix XenServer 6.2, 6.5SP1, 7.0 • Microsoft Hyper-V (WS2008 R2, WS2012, WS2012 R2)
Supported Webservers	• Apache Tomcat version 8.5 • IBM WebSphere Application Server 8.5.5 • Should include Java: JRE8, JSP2, JS2.4
Supported Webbrowsers	• Chrome 51, Firefox ESR45, Internet Explorer 11, Microsoft Edge 25
Data store (DBMS)	• Oracle 12c (64-bit, Linux, Windows) • Microsoft SQL Server 2008 R2SP3, 2012SP2, 2016 including Always On (Windows) • MariaDB 10.2.13 (Linux, Windows)
Data store (Active Directory)	• Windows Server 2008R2SP1 AD • Windows Server 2012 AD, 2012 R2 AD, 2016 AD
LDAP Back End Authentication	• Windows Server 2008R2SP1 AD • Windows Server 2012 AD, 2012 R2 AD, 2016 AD • NetIQ eDirectory 8.8 SP8 • IBM Security Directory Server 6.3
HSM	• SafeNet ProtectServer Gold, Orange, Express • SafeNet ProtectServer External 2, Internal-Express 2 • Thales nShield Connect, Solo (on selected platforms)

COMPLIANCE TO STANDARDS

RADIUS	RFC 2865 and RFC 2866
Wireless	EAP, PEAP
Authentication	• DIGIPASS OTP (Challenge / Response, Response Only) • DIGIPASS Signature (transaction validation) • OATH (event based – time based) • EMV-CAP

About VASCO

VASCO designs, develops, markets and supports patented DIGIPASS®, DIGIPASS PLUS®, VACMAN®, IDENTIKEY® and 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

DS-201804-v4