AUTHASAS™
AUTHENTICATION AT YOUR SERVICE

Technical White Paper Authasas Advanced Authentication

June 2009

Authasas
Advanced Authentication

Asterweg 19D12
1031 HL Amsterdam
The Netherlands

www.authasas.com
info@authasas.com

t: +31 (0)26 373 61 70
f: +31 (0)20 524 13 68

AUTHASAS™

AUTHENTICATION AT YOUR SERVICE

ABSTRACT

Authasas Advanced Authentication is a comprehensive software package that seamlessly integrates with Microsoft Windows 2000, XP and 2003 Server™ and supports a multitude of advanced authentication technologies and devices. Authasas provides authentication, authorization, and auditing functionality, as well as centralized administration services.

Authasas is a scalable, customizable, and modular software package that has been fully integrated with Microsoft Windows Active Directory. Authasas is compliant with the open industry standard BioAPI (www.bioapi.org) and allows new authentication hardware to be easily pluggedin at any time without reinstalling the Authasas software.

Authasas is fully client/server enabled and supports standalone installations. It is the most seamless and universal authentication solution currently available on the market, supporting the largest number and the widest variety of existing biometric and nonbiometric authentication devices and technologies.

AUTHASAS™
AUTHENTICATION AT YOUR SERVICE

CONTENTS

Passwords + Humans = Problems

In most businesses, the only security measure protecting sensitive corporate data from unauthorized access is the user password. However, simple passwords are too easily compromised. While stronger password policies are possible, many employees push back as they find it difficult to use longer, more complex passwords that change frequently. Stronger password policies are also likely to create security problems tempting users to record passwords in areas where they can be easily stolen.

Businesses have traditionally been left with two less than ideal options:

- Relax password policies thus accepting the risk of less secure corporate data.
- Implement a stronger password policy thus losing productivity and increasing Help Desk costs.

Companies often invest in the most sophisticated firewall and antivirus tools, but ignore the fact that passwords remain a key element of their threat management strategy and are therefore, the *weakest link* in the security chain of their network security infrastructure. By replacing passwordbased authentication with more secure authentication technology, overall network security is improved. Each technology has its own set of features, but by making thoughtful decisions about the choice and implementation of authentication technology or a combination of technologies for a particular network, network administrators can greatly improve the security of their important data and applications.

Authasas Advanced Authentication provides an off-the-shelf, convenient password replacement solution, supporting multiple biometric and non-biometric authentication technologies, a wide range of hardware devices, centralized account management, powerful administrator tools and broad reporting capabilities. Authasas is the most intuitive and comprehensive authentication management infrastructure available today.

The Authasas SECURITY PLATFORM: An Overview

The Authasas Advanced Authentication security platform encompasses several key concepts and features that are critical to any security software package:

- **Authentication** – Verification of users' claimed identities by using one or more of the following: secrets (what
- you know), tokens (what you have) and biometrics (what you are and what you do).
- **Authorization** – Determination that a user is authorized to carry out a particular action, such as logging on
- to a VPN, running an application, accessing a database, etc.
- **Audit** – Detailed logging of authentication and authorization actions, with the ability to review and analyze
- logs to uncover suspicious activities, failures, etc.
- **Administration** – System administrators can enroll users and define policies that control authentication and authorization for particular users, user groups, or applications.

In addition to these four key components, Authasas is designed to enhance both overall system security and convenience by focusing on:

- **Integrity** – Authentication data (such as user authenticators), device/terminal/workstation communication, as well as policy and system settings are secured and protected from tampering and forgery by other applications, hackers, etc.
- **Confidentiality** – Secret application data as well as authentication and authorization information is encrypted to protect it from access by unauthorized users, hackers, etc.
- **NonRepudiation** – Logging of security events that are supported by biometric authentication prevents users from claiming that an action occurred without their knowledge and acceptance.

Authasas is designed to address both overall system security and user acceptance with the following goals in mind:

- **Convenience** – Security functionality should be easy to use, so that users will not attempt to bypass it.
- **Flexibility** – Different applications call for different security measures, therefore security layers must be flexible in order to provide the right level of protection to the problem being addressed.

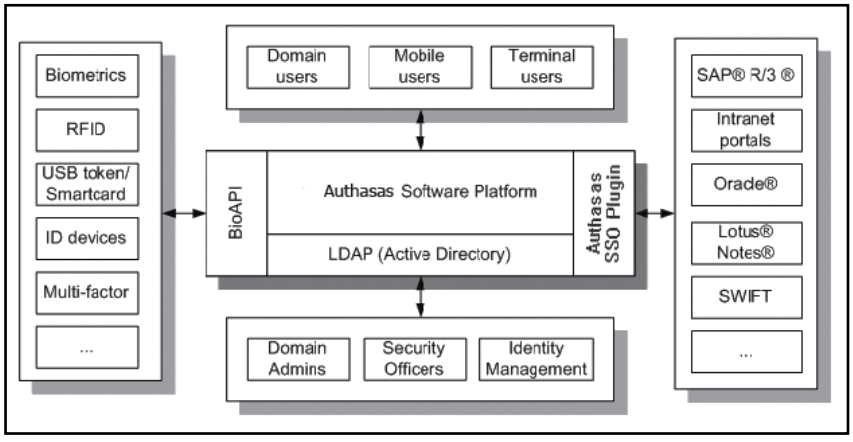
- **Centralization** – Administrators must be able to manage the entire system in a consolidated and integrated manner, from a central or multiple locations.

Authenticator

Throughout the Authasas Advanced Authentication system, we use the term "Authenticator" to mean the authentication data contained in or captured by the biometric or nonbiometric devices (such as fingerprint, facial image, USB token, RFID card, etc).

HighLevel Architecture

Authasas provides a flexible architecture that results in a common software platform thereby enabling scalability, making it easy to add features and support new technologies in the future. In addition to authentication on a PC or network, Authasas provides a universal software interface and Software Development Kit (SDK) that can be used to build scalable and centralized single signon (SSO) solutions to thirdparty applications, such as SSO to SAP® R/3®, Oracle®, Lotus® Notes®, Intranet portals, etc.



Biometric Standards Compliance

Authasas Advanced Authentication was designed from the ground up to support the BioAPI open standard which makes it possible to easily plug in new authentication hardware at any time without reinstalling or restarting the Authasas software. Both biometric and nonbiometric technologies are supported by Authasas through the use of BioAPI and Biometric Service Provider (BSP) modules. A BSP module is vendorsupplied software that provides enrollment and verification services for a particular hardware device.

BSP modules are completely interchangeable or *pluggable*" into the Authasas Advanced Authentication system. Multiple BSP modules can be installed on a server and workstation to reflect the needs of each organization. Such flexibility allows an organization to tailor its use of authentication hardware to best match its workstation environment.

Active Directory Integration and Support

Authasas fully supports and utilizes Microsoft Windows Active Directory (AD). AD technology was introduced with Windows 2000 to replace the traditional Windows NT SAM database. The following is a partial list of major AD advantages and their relevance for Authasas:

- Multimaster domain model
- Load balancing
- Support for complex (ntier) domain configurations and *sites*
- Automatic data replication of both operating system and third-party data
- Robust failover capability
- Extensible schema
- Tightly integrated with the Domain Name System (DNS)
- Global Catalog

Customers gain considerable robustness through AD, and can substantially lower their Total Cost of Ownership (TCO) for Authasas enabled AD domains. Authasas integrates with many of the failover and data replication services that the operating system provides. AD's multimaster domain model allows the domain to function normally in the case where a Domain Controller (DC) becomes unavailable. As long as the domain consists of more than one DC, there is no single designated DC to process information updates. In case of a DC failure, and assuming the worst case scenario, only the last data that was received but not replicated across the domain/forest is lost. As long as the DC becomes available again, the updated data may not even be lost but may just be unavailable until the DC goes live once again. AD's use of DNS and its Global Catalog subsystem greatly supports service discovery and reduces network bandwidth usage.

The information maintained by the operating system is made available in a standardized and straightforward form.

Authasas Advanced Authentication fully leverages these mechanisms to provide data replication, a robust and fast server discovery to its clients on the network.

Authasas AD Data

To support and make full use of AD, Authasas extends the AD schema by extending existing Computer and User classes with new attributes. These attributes contain fingerprint, password, settings and other support information.
Authasas AD data is opaque to AD and other AD enabled applications. The data is digitally signed and encrypted using cryptographic algorithms specified by the customer when they are installing the Authasas Server software and specifying the unique Enterprise Key of the organization.

Extension of the AD Schema is optional. Authasas could instead use existing attributes such as Photo, Audio, etc., which as a rule are not used in the domain of the organization. Using existing attributes is ideal for evaluations and pilots.

Encryption Algorithms

Authasas supports the open Microsoft CryptoAPI interface, which in turn provides a secure interface for the cryptographic functionality that is supplied by the installable Cryptographic Service Provider (CSP) modules.

Authasas allows the customer to choose required cryptographic algorithms and key lengths for all cryptographic operations (keys exchange, digital signature, data encryption and hashing).

Authasas uses the Microsoft Enhanced Cryptographic Service Provider by default, thus providing stronger security by supporting longer key lengths and additional cryptographic algorithms such as RSA, SHA1, RC4.

Authasas Advanced Authentication Workstation

Authasas GINA

The Graphical Identification and Authentication (GINA) DLL is the portion of the Windows 2000/XP/2003 Server™ operating system that challenges a user for his username, domain, and password during the logon process.

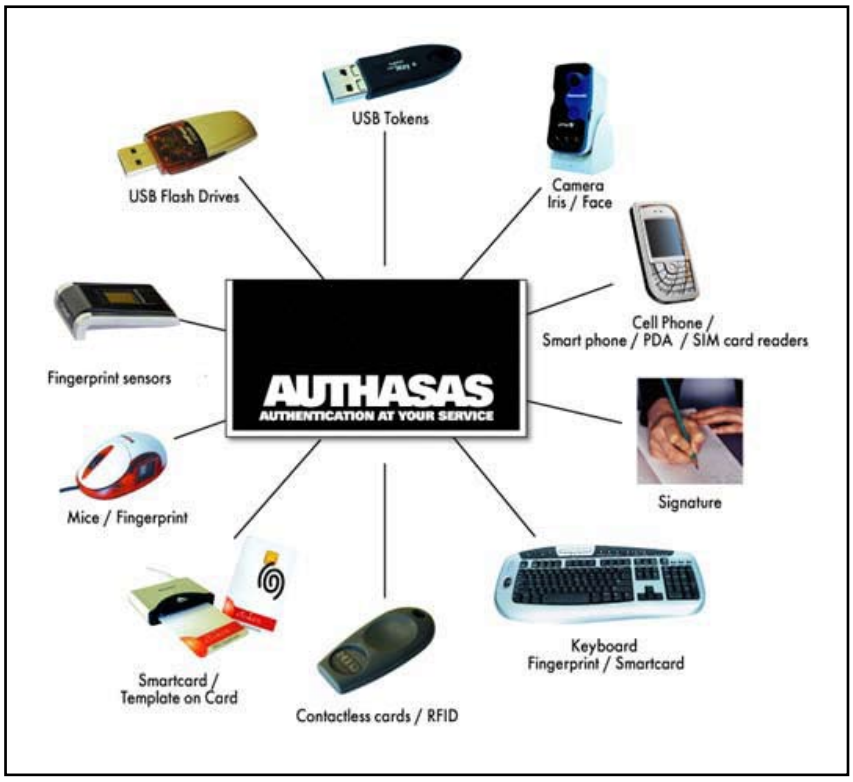
Authasas Advanced Authentication extends the functionality of this DLL to call a selected BSP. The same Microsoft secure key sequence that invokes the standard GINA DLL (Ctrl-Alt-Del) is also used to invoke the Authasas provided GINA DLL. Authasas GINA communicates with the user, hardware device and Authasas Enterprise Edition to perform the authentication procedure.

Authentication Technologies Supported

Authasas GINA is ready-to-support *out of the box*, any of the following authentication technologies:

- Static biometrics (Finger, Face, Iris, etc)
- Dynamic biometrics (Keyboard or Mouse signature, Handwriting, etc)
- RFID cards (HID, Milfare, etc)
- GSM SIM card (Cell phone, Smart phone, etc)
- USB tokens or Smartcards (Aladdin eToken, Rainbow iKey, etc)
- Template on board (Flash drive, contactless card, etc)
- Memoryless card and tokens (Dallas iButton)
- Single- an multifactor authentication
- Any combination of authentication technologies
- Future Technologies

With Authasas, it is possible to use any hardware device or authentication technology. Authasas makes it easy to plug in new hardware at any time without reinstallation of the Authasas software. The diagram below illustrates the wide range of authentication technologies and hardware devices that are supported *out of the box* by Authasas.



Available Authentication Scenarios

The Authasas Advanced Authentication Workstation supports all of the following authentication scenarios:

- Standalone PC
- Networked PC
- Cached logon
- Windows Terminal Server
- Citrix® Metaframe®, N-Fuse® session
- Windows XP Remote Desktop
- Dialup/GPRS/VPN/RADIUS session
- Crossdomain authentication (trusted domains)
- Launching application via *Run As* command

Authentication procedure

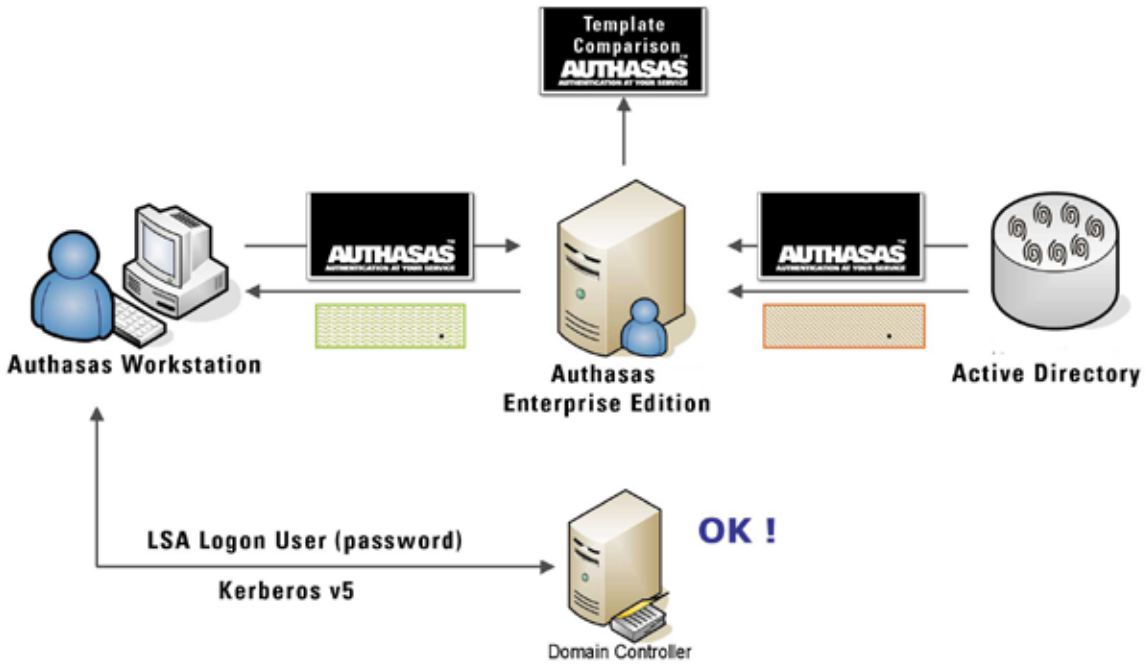
During logon a user need not memorize a series of ever changing passwords. With Authasas the user enters his username followed by his authenticator using biometrics or non-biometrics authentication technology. Depending on which *pluggable* BSP module has been installed and selected, the authenticator presented during logon is compared against the previously enrolled authenticator stored at the authentication Authasas Enterprise Edition and the user is either accepted or rejected.
Users whose biometric identification records are already enrolled in the Authasas Enterprise Edition database (Active Directory), are only required to enter their user name and present their biometric authenticator. Authasas transparently supplies the user's "hidden" and encrypted password to the Windows security system to complete the logon process. This authentication flexibility reduces password maintenance expense by avoiding calls to the help desk for password-related problems, while providing a more secure block against hacking-related problems.

Typical Logon Process

This section describes the typical logon process on the network:

- The user enters Ctrl-Alt-Del sequence, provides user name, domain name and selects the preferred authentication method to be used (biometrics or nonbiometrics authentication hardware installed on the computer)
- Authasas GINA loads the corresponding BSP module and the user is challenged for the authenticator. The authenticator is captured from the user, then encrypted and sent to Authasas Enterprise Edition together with the user and domain names. In the case of a password challenge, Authasas GINA captures the user's password and sends it through the WINLOGON process for normal validation by the Windows security system.
- The Authasas Advanced Authentication Enterprise Edition retrieves the user's enrolled authenticator stored in the Active Directory database and decrypts it. The Authasas Enterprise Edition then decrypts the authenticator presented by the user and loads the corresponding BSP module for comparison. If there is a match, the user's password (which was also retrieved and decrypted from Active Directory) is encrypted and returned to the Authasas GINA.

- Authasas GINA then decrypts the password and passes the user name and password to the WINLOGON-process to complete the normal Windows logon by password. The user is then logged onto his desktop and connected to the domain server.



Automatic Lock PC

Authasas GINA provides a secure screensaver capability for Windows 2000/XP/2003 Server™ that locks the keyboard and hides the desktop when a user leaves his desk. Upon return, the user presents his authenticator to unlock his workstation. The screensaver can be invoked manually through a key sequence or via a configurable timeout value. To use the secure screensaver feature, users must configure their screen savers to be *Password Protected*.

Users can also manually lock a workstation independent of the screensaver timeout function through the standard Windows 2000/XP/2003 Server™ lock function.
In addition, in the case of using smartcard, USB token or flash drive the Windows session will be automatically locked once the device is plugged out. This saves precious time for the user who now does not have to worry about logging out before leaving his desk.

Credential Caching

Credential caching refers to the mechanism that allows a user to be disconnected from the network but still be able to use domain credentials for logon. When credential caching is enabled, Authasas stores a user's authenticators locally. These authenticators are retrieved and verified locally when the user is disconnected during logon.

Authasas's authenticators caching functionality closely resembles Windows built-in functionality for password-based network-detached logon.

Only the network administrator can enable caching for a particular computer (for example a laptop). Authasas minimizes client side security risks by storing authenticators in digitally signed and encrypted form using the operations facilities of the Microsoft Data Protection API and Microsoft CryptoAPI.

Once the administrator disables the caching option for a particular computer all data cached on this PC will be removed regardless of the user wishes.

AUTHASAS™
AUTHENTICATION AT YOUR SERVICE

Authasas Advanced Authentication Enterprise Edition

The Authasas Advanced Authentication Enterprise Edition provides secure matching of authenticators and the storage and retrieval of user credentials for Active Directory. With Authasas Enterprise Edition installed on a domain, administrators can centrally manage user accounts, authentication technologies, policies and rights.
Credentials are centrally stored and provide users access from any workstation within the domain – logging on from any Authasas workstation using advanced technologies or from any workstation using a legacy password.
The Authasas Enterprise Edition can be installed both on the domain controller and member server, fully leveraging existing infrastructure investments thus avoiding the purchase of additional hardware and software servers.

Scalability and Load Balancing

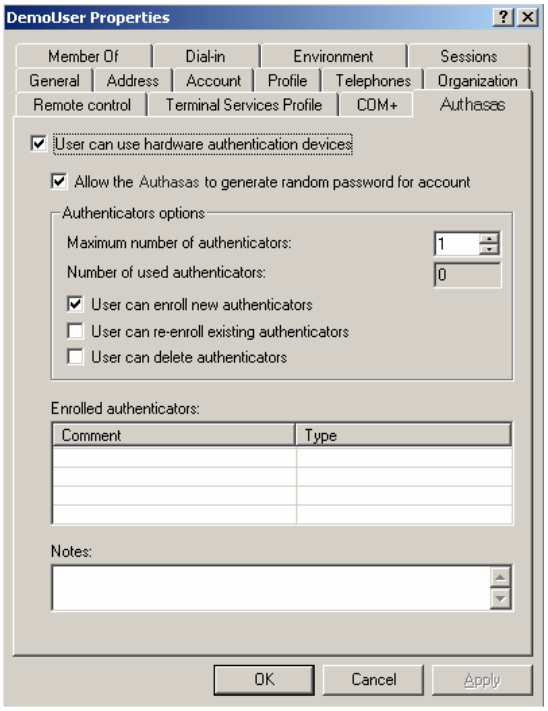
Authasas can be scaled to domains of virtually any size. The presence of several instances of the Authasas Enterprise Edition provides multimaster clustering, automatic load balancing, hotswapping, scalability and faulttolerance.
Authasas provides powerful intelligent server search algorithms enabling client components to find and establish communication with the nearest Authasas Enterprise Edition available. If no Authasas Enterprise Edition was found in the scope of the site, the process of searching for a server continues within the domain of the organization.

Client/Server Communication

There are significant advantages to the Authasas architecture in terms of communication and configuration flexibility.
All sensitive information communicated between clients and servers is digitally signed and encrypted. Authasas uses the builtin Windows environment encryption layer provided by the Windows Remote Procedure Call (RPC). In addition, Authasas performs a two-way client-server validation with the help of the Windows Kerberos protocol prior to user authentication. In this process, the client is first authenticated by the server and then the server is authenticated by the client thus facilitating mutual authentication of both end points and ensuring reliable and secure communication.

Administration Tools

Authasas Advanced Authentication extends the User Manager application provided by Windows: Active Directory Users & Computers (ADUC) snapin. Authasas adds a new property page *Authasas* to the existing user profile dialog. This allows network administrators centralized access to Authasas functionality from anywhere within the Active Directory forest, and through the applications and access points native to Windows.



Authasas New User Enrollment

The process of enrolling new Authasas users is very simple and consists of the following steps:

- Using the standard "New Object – User" wizard, an administrator simply enrolls a new user in a domain as usual. At this point the user is a normal domain user and can logon on to the network using his password. This step is not necessary and can be skipped if the user is already enrolled as a domain user.
- The administrator then opens the "User Properties" dialog box and selects the Authasas tab. By enabling and applying the "User can use hardware authentication devices" option, the administrator indicates that the registered domain user is now a Authasas user. Also, the administrator has the ability to adjust Authasas user settings to comply with the security policies of the organization.

- When the user logs on to the network on the next occasion (using the password, which the user still knows) the Authasas Workstation will welcome the new Authasas user and offer to carry out the authenticator enrollment procedure. After that, the user is allowed to a use a hardware authenticator instead of his password, which will normally be automatically randomly generated once the first authenticator has been enrolled.

Authasas User Viewer

Authasas provides an additional Authasas User Viewer MMC console intended to provide system administrators with the capability of listing all domain users and viewing their Authasas specific properties. The Authasas User Viewer console can also be useful to security officers by enabling them to identify which employees are not Authasas users yet, which are Authasas enabled but have not enrolled their authenticators yet and which are already Authasas users.

All of the data that the Authasas User Viewer console displays can be sorted or exported for analysis in more powerful report writing applications such as Microsoft Excel or Crystal Reports.

Policies

Authasas policies allow the administrator to customize how Authasas operates and interacts. Many policies determine authentication and security requirements. Using Authasas policies, the overall security of the system can be increased or decreased to support various security and user requirements.

Audit

Audit refers to the process of logging and/or recording events. Events in Authasas typically take on the form of a user ("SomeUser") who succeeded or failed to do "something". Authasas audit trails or logs enable administrators to see which system resources were or are being accessed, by whom, and from what workstation.

There are numerous benefits to having audit trails available. Chief among those benefits is the ability of the network/domain administrator to identify problems, possible security breaches, and to view the status of the domain.

In order to support Windows functionality and integration requirements, Authasas leverages the native Windows Event Viewer subsystem to report all events. It extends the standard Event categories to include a Authasas specific node.

Authasas provides a powerful mechanism for multicentralized auditing. By specifying the names of the audit servers, administrators and security departments can access different views of system events and use the native Windows Event Viewer to control the health of the system.

Localization

Authasas Advanced Authentication is available in English, Spanish, German (8-2009), French (8-2009) and Dutch. Language resources support Unicode and are stored in a separate file in XML format.

An Authasas Software Development Kit (SDK) is available for custom integration into customer's environment and applications as well as for extending the current functionality of the Authasas system.

System Requirements

Authasas Advanced Authentication Enterprise Edition:

- Microsoft Windows 2008 Server™
- Microsoft® Windows 2003 Server™ (Standard Server and Enterprise Server only)
- Microsoft Windows Active Directory®
- 30 MB of available hard disk space
- Additional 0,3K-10K hard disk space per user depending on authentication technology and hardware

Authasas Advanced Authentication Workstation Software:

- Microsoft Windows 7 Professional or better
- Microsoft Windows Vista Business or better
- Microsoft Windows 2000, XP, 2003 Server™
- 30 MB of available hard disk space
- Authasas for SAP® R/3® addon:
- SAP® Server 4.0B, 4.6C, 4.7, 6.4 (No server interventions)
- SAPGui® 6.2, 6.4 (Windows only)
- SAP® Enterprise Portal 6.0
- Supported Hardware
- Both biometric and non-biometric technologies

Single Sign-on

The Authasas Advanced Authentication fully supports different Single Sign-on systems:

- Active Identity SecureLogin SSO
- Passlogix v-GO SSO
- Oracle eSSO

Supported Hardware

Both biometric and non-biometric technologies are supported by Authasas through the use of BioAPI 1.1 and 2.0 and vendor-supplied BSP modules:

- Digent FD/FM 1000 fingerprint sensor
- BioLink U-Match fingerprint sensor
- Iridian with Panasonic Iris camera
- OmniKey CardMan 5121/5125 RFID/Smartcard reader (MIFARE/HID)
- Aladdin eToken Pro/SC
- Aktiv USB ruToken
- GSM phone/SIM card (IrDA, Bluetooth)
- Dallas iButton (USB/COM/LPT readers)
- Any USB flash drive
- Any other BioAPI 2.0 or 1.1 compliant hardware

Biometrics sensors supported through Bio-Key BSP;

- Atmel AT77UR200 (500 dpi)
- Authentec AF-S2, AES4000, 1601/1610, AES2501/2510 swipe (250-500 dpi)
- Crossmatch Verifier 300 (500 dpi)
- Digital Persona U.are.U 4000b (508 dpi)
- Biometrika HiScan & FX2000 (500 dpi)
- Fingertech BIOCA-120 (400 dpi)
- Fujitsu MBF200 (500 dpi)
- Futronic FS-80, FS-88, FB-80 & FB-88 (500 dpi)
- GreenBit DactyScan 26 (500 dpi)
- Identix DFR-200, BTO-500, DFR-2100, DFR-2080 (500 dpi)
- Lumidig Venus (500 dpi)
- SecuGen Hamster III, III+, IV (508 dpi)
- Tacoma Technology Inc, STM01A1 (500 dpi)
- Testech BIO-I (500 dpi)
- UPEK TCS1 & TCS2 (Touch Chip) TCS3 (Touch Strip) (508 dpi)
- Validity Sensors Inc, VFS130, VFS201, VFS301 (500 dpi)

Reader Device Manufacturers Supported;

LAPTOPS:

- Hewlett Packard
- Dell
- Toshiba
- Sony
- IBM/Lenovo
- Motion Computing
- MPC

KEYBOARD:

- Cherry
- KSI

FINGERPRINT READERS:

- Atmel
- Authentec
- Biometrika
- Crossmatch

AUTHASAS™
AUTHENTICATION AT YOUR SERVICE

- Digital Persona
- Fingertech
- Futronic
- GreenBit
- Hyundai
- L1 Indentity Solutions
- Lumidigm
- Precise Biometrics
- Secugen
- Silex
- Startek
- Testech
- Tacoma technology Inc.
- Targus
- UPEK
- Zvetco Biometrics