

THE ASAS[®] SYSTEM ADDS STRONG AUTHENTICATION TO ORACLE IDM



ASAS SYSTEM KEY FEATURES

- Secure remote, local, and Web access to IDM
- OTP, Challenge/response and PKI authentication
- Easy to install and administer
- Easily fits into current environments
- Driverless token for Authentication
- Secure, encrypted token storage leaves no footprint.
- SDK enables the creation of plug-ins for any RADIUS-compliant system
- Tokens can be used for authentication and AES-encrypted storage of mobile data.
- Tokens are password-protected and will self-erase after a predetermined number of failed log in attempts.

The ASAS[®] System makes the highest standards in e-security available to Oracle Identity Management. The ASAS System provides two-factor remote and local authentication for Oracle Identity Management, enabling secure, fast, and easy access and enhancing efficiency, productivity, and peace of mind.

Necessity

Organizations of all sizes are increasingly recognizing the need to enhance their network and data security through the use of two-factor authentication, specifically, One-time Password (OTP) authentication. This is especially true of companies that have governmental regulations they must adhere to, such as Sarbanes-Oxley, HIPAA etc. They want tools that enable strict and trustworthy measures that ensure network integrity, enhance regulatory compliance, and keep remote data safe.

More and more, organizations are:

- Implementing trustworthy authentication measures with customers and partners, as well as employees.
- Enabling users to securely access data, communications, and work wherever they are without leaving a footprint on the remote machine, thus enhancing secure mobility and productivity.

Confronting Security

Daily, IT has to confront how to ensure local and remote access to authorized users and security from unauthorized use of networked assets, insecure password storage, theft of data and hardware. At the same time, they must ensure that data taken on the road remains secure, even if it is lost or stolen. The ASAS System is designed to help organizations to do just that: secure their networks and data.

The ASAS System and Oracle

The Authenex Strong Authentication System (ASAS[®]) is a complete, network and remote data security system that provides flexible One-time Password, Challenge/Response, and PKI authentication to networked assets. Based on an authentication server and database and a chip-based token called the A-Key[®] token, the ASAS system provides the most secure, easy to use, simple to administer and cost-effective two-factor authentication solution available today. The ASAS System is also easy to install and administer, which frees senior IT staff to do senior IT tasks. And there are no hidden costs, no renewal fees.

A-Key tokens serve as strong authentication devices that support multiple authentication protocols (OTP, PKI, or Challenge/Response authentication). They are used on the client side for authentication and secure data storage.

THE ORACLE AND AUTHENEX PRODUCT FAMILIES

ORACLE IDENTITY MANAGEMENT

Serving as the security backbone for Oracle Fusion Middleware, Oracle Identity Management enables organizations to decrease security threats across diverse IT environments while helping address compliance needs. The family of best-in-class products includes Oracle Access Manager, Oracle Identity Manager, Oracle Identity Federation, Oracle Virtual Directory, Oracle Directory Services and Oracle Web Services Manager. To learn more, visit <http://www.oracle.com/identity>.

AUTHENEX PRODUCTS

The ASAS® System provides fixed password and One-time Password (OTP) authentication for LAN, remote VPN and web-based access.

The v4 A-Key® token provides on-board memory up to 2 GB that is protected by password, real-time encryption, and brute force penetration prevention.

ACert™ software enables the secure generation and storage of digital signatures and certificates for use in PKI implementations. ACert software is an optional component to the A-Key token.

My A-Key™ software enables secure storage of user profiles, which can be used with applications, such as Single-Sign On. My A-Key software is an optional component to the A-Key token.

HDLock™ software encrypts files and folders on a hard disk with 128-bit AES (Advanced Encryption Standard) encryption, and enables users to launch, edit, save and delete in a secure environment.

They contain up to two (2) gigabytes of password-protected, AES-encrypted storage for user data (such as certificates, documents, single-sign on credentials, etc.). A-Key token storage is also protected against brute force penetration: the hardware will self-erase if someone tries and fails to log on a predefined number of times. In case of loss or theft, organizations can know their vital information will not fall into the wrong hands.

Key Features

- **Multiple Authentication Protocols.** The ASAS System brings cost-effective One-time Password, Challenge/Response, and PKI authentication to Oracle Identity Management.
- **Flexible Implementation.** The ASAS System easily works with any RADIUS-compliant component.
- **Easy to Install.** The ASAS System is as easy to install as a word processor: insert the CD and follow the instructions.
- **Easy to Use.** Administration is easy: minimal knowledge is necessary to perform most administrative tasks.
- **Versatile Token.** A-Key tokens can be used for authentication and secure storage of mobile data.
- **Password-Protection.** A-Key tokens enable user and/or admin accounts, which ensures that only authorized users get authorized access to the token.
- **Brute Force Protection.** A-Key tokens are made to self-erase after a predetermined number of failed login attempts.

Authenex and Oracle

The ASAS System in conjunction with Oracle Identity Management provides the most cost-effective, complete two-factor authentication solution. Easy to install and use, the system is usually up and running in about half an hour. Since it is a system of hardware and software components, the ASAS System not only provides IDM users with the most secure authentication available, but it also secures data they take on the road.

To learn more about how Authenex can add the highest standard in e-security to your Oracle installation, please contact Mike Kent at mkent@authenex.com, or call +1 510.324.0230, extension 129.

Disclaimer

When Oracle conducts partner integration and testing, we verify only that the software integration functions according to the partner's proposed integration plan, and that it makes appropriate use of Oracle components and integration technologies in the environment specified in the published Integration Datasheet. Customers are solely responsible for the selection of all third-party software, including any integration software, used in conjunction with Oracle Identity Management and for the results of such use.