

The Authenex Overview

Authenex has developed the most affordable, secure and easy-to-use platform for strong two-factor applications – making it possible for enterprises and PC-users to afford and deploy the highest standards in e-security. The Authenex suite of applications includes Strong Authentication, Web Access Control, End Point (File and Hard Drive) Encryption, Secure File Exchange, and Secure Storage for Digital Certificates and Signatures. Each leverages the chip-based A-Key® token - providing simplified management and use. One A-Key is all a user needs to carry.

The Authenex A-Key®

The A-Key is a house-key sized token that serves as the platform for the Authenex suite of strong two-factor e-security applications. The unique benefit of the A-Key is its on-board CPU utilizing an embedded CSP and Cryptographic Functions for PKI environments. Plus, the A-Key is able to conduct 128-bit AES for both data encryption and Challenge-Response sequences. The A-Key is a storage class device that provides a “driverless” experience enabling a user to authenticate from any computer without the need to install applications.

Also, the Hybrid Model A-Key is the only device of its kind that offers users the flexibility of authenticating using PKI, Challenge-Response or One-Time Password methods. A distinctive feature of the A-Key is the USB interface, which allows certificates to be used for PKI infrastructures or Challenge-Response sequences to be conducted, while also capable of being a stand-alone One-Time Password device. All of these features are included in a convenient form factor about the size of a car key.

Strong Two-Factor Authentication

The Authenex Strong Authentication System (ASAS®) provides two-factor authentication for remote VPN, LAN, and web-based access. Authenex ASAS ensures that only authorized users are granted access to network resources by employing the Authenex A-Key. The ASAS authentication server uses RADIUS and TCP/IP protocols, is VPN and firewall interoperable, and supports ODBC to use SQL databases - providing networks with an efficient and secure two-factor authentication system that integrates easily with an existing security infrastructure.

ASAS provides authentication via Challenge-Response or One-Time Password. It will also allow authentication with Microsoft Internet Information Services (IIS) and Outlook Web Access (OWA). The Web Management Console (WMC) gives



administrators a handy tool for maintenance and management of accounts and databases. ASAS has failover functionality and works with the leading VPN and Firewall providers, including Check Point, Cisco and Netscreen, plus the ability to work with Citrix Web Interface.

Digital Certificate Storage

Authenex ACert™ allows digital certificates to be stored on the Authenex A-Key for use in PKI implementations. The A-Key contains flash memory that allows the storage of user information such as digital certificates, PKI information and windows credentials - providing a highly mobile two-factor authentication hardware device for PKI applications.

Endpoint Encryption and Secure File Exchange

Authenex HDLock™ protects notebooks and desktop PCs using strong two-factor authentication and AES (Advanced Encryption Standard) to encrypt and protect the contents of the hard drive. The Authenex A-Key® acts as the key to your computer; without it, the hard drive remains encrypted and inaccessible to anyone else. Even if the hard drive is removed from the computer, the data will still be protected.

Endpoint Encryption and Secure File Exchange (Continued)

The encryption and decryption processes occur on the fly and are transparent to users. Upon hibernation or shut down, the computer will become "locked" and can only be accessed again by authenticating with the A-Key.

HDLock also has a unique feature with its Management Server option. The Management Server allows for a simple web method of recovery that can be hosted internally in the event that an A-Key is lost or misplaced. This offers administrators control over account and recovery options. Also included are reporting capabilities to show active and inactive A-Keys.

Authenex ASafe™ lets you use the A-Key to encrypt and securely exchange files through the Internet or any other type of network or media. ASafe uses AES to encrypt files that can be stored locally on a computer and cannot be opened by anyone other than the original A-Key user. With an intuitive right-click method of operating the application, a user can encrypt, decrypt or create a secure file package.

An ASafe package can be created with multiple designated receivers that will be verified by their A-Keys. Only an A-Key user who is designated to receive the package can decrypt the message. There is also a header message option that can be read by recipients before they decrypt the file.

Strategic Technology Partners Include:

- | | |
|----------------|------------------------|
| ■ Check Point® | ■ Netegrity® |
| ■ Citrix® | ■ MetaInfo® |
| ■ Microsoft® | ■ Novell® |
| ■ VeriSign® | ■ Kensington® |
| ■ Toshiba® | ■ Computer Associates® |

© 2005 Authenex, Inc. All rights reserved. Authenex, ACert, A-Key, ASafe, ASAS, HDLock, and associated logos are registered or unregistered trademarks of Authenex, Inc. All other registered or unregistered trademarks are the property of their respective owners.



Corporate Headquarters
1489 Salmon Way
Hayward, CA 94544
tel: +1 510 324 0230
fax: +1 510 324 0251
www.authenex.com