

The Authenex A-Key[®]

The Simple, Mobile and Secure Token with Up to 2 Gigabytes of Encrypted Storage

In today's business world, mobility is a key factor in enabling employees to be more productive and corporations to reach markets in ways they have never been able to before. However, with increased mobility comes greater security risk as sensitive corporate data stored on devices and networks become vulnerable to unauthorized access and theft.

Authenex offers the most cost effective two-factor authentication solution that enhances security and mobility through the Authenex v4 A-Key[®] token. The v4 A-Key[®] token is a password-protected USB token that offers up to 2 GB of encrypted storage for files and applications and also enables secure Challenge/Response and PKI (certificate based) authentication and email security. It leaves no footprint wherever it is used, yet enables secure remote login from anywhere in the world. The A-Key[®] token is also tamper-proof and provides protection against brute force penetration.



Benefits:

Secure and Immediate Deployment

You can use your A-Key[®] token to access essential enterprise applications on an ASAS[®] Server-protected network without installing anything on your machine. Also, customized applications can be stored and launched from the A-Key[®] token. This significantly reduces deployment costs, while integrating security features into a single, easy-to-manage platform.

Strong Two-Factor Authentication

The chip-based A-Key[®] token and the ASAS[®] Server offer greater flexibility than other solutions, by enabling PKI and Challenge/Response authentication from the same token. In addition, the token supports Authenex's robust suite of security applications.

Total Mobility

Because our storage-class A-Key[®] token is driverless, no installation on your PC is necessary. You have complete freedom to use any available computer. Without embedded applications, the v4 A-Key[®] token also enables you to travel and authenticate from any local or remote computer without having to install additional software on the remote machine.

Secure on-Board User Memory

The A-Key[®] token is equipped with on-board user memory that ranges from 128MB up to 2GB and can store documents and/or applications. This memory is protected by a user password and real-time 128-bit AES (Advanced Encryption Standard) encryption.

Self Erase Security at Hardware Level

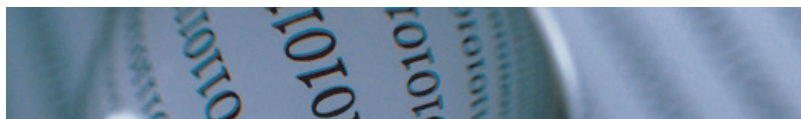
User data inside the A-Key[®] token is safe from loss or theft. For added security, the A-Key[®] token is programmed to self-erase after a configurable number of failed login attempts.

PKI

The v4 A-Key[®] token is equipped with embedded Crypto Service Provider (CSP) for PKI-related operations (such as digital signatures, encryption and authentication) using X.509 digital certificates. The A-Key[®] token has an on-board 1024/2048-bit RSA key generator. The embedded CSP is MS CAPI and PKCS#11 compliant.

Assists in Compliance Security

The A-Key[®] token helps facilitate regulatory compliance when used with the Citrix[®] Presentation Server, in that all applications and data are kept on the server instead of the desktop and protected by two-factor authentication to minimize risk of exposure to theft or loss.



■ Features:

- On Board User memory Area up to 2GB
- Real Time Encryption
- Self Erase Mechanism
- Personal Password Manager (Optional)
- Personal Profile Synchronization (Optional)
- Public Key Infrastructure (PKI) (Optional)
- Challenge-Response (Optional)
- One-Time Password (OTP) (Optional)

■ Standard Compliance:

- Public Key Infrastructure
 - On Board 1024/2048-bit RSA key-pair generation
 - X.509 Digital Certificates
 - MS CAPI compliant
 - PKCS#11
 - PKCS#12

■ Symmetric Key Cryptography

- AES 128-bit, 192-bit and 256-bit
- Secure Hashing Algorithms
 - SHA-1
- OTP Algorithm
 - OATH compliant (160-bit)
- Equivalent to FIPS-140 Level 3 security

■ Hardware:

- On-board Security Processor
 - V4, 100MHZ
 - AES 128-bit, 192-bit and 256-bit
 - SHA-1
- On Board Memory
 - From 128 MB up to 2 GB
- Interface
 - USB 2.0
- Operating Temperature
 - -10° to 60° C
- Storage Temperature
 - -20° to 70° C

■ Display

- 6-Digit Numeric LCD (Optional)
- Battery (available on token with display)
 - 5 year life

■ Physical Characteristics

- Casing
 - Injection molded plastic, tamper evident

■ Operating Systems:

- Windows 2000 Professional and Server
- Windows XP Home and Professional
- Windows 2003 Server

■ LAN and Remote Access (With Authenex ASAS® Authentication Server):

- Dial-up to a remote server with MS RRAS and RADIUS
- VPN with: Check Point™, Cisco Systems®, Microsoft®, Netscreen™, Nortel®, Safenet™ and/or others using RADIUS
- SSL VPN
- Secure Web Access
- Network Login for MS Windows 2000 and 2003 Servers and XP Home and Professional Editions

■ PKI Certificate Storage:

- Compatible with leading Certificate Authorities including: Baltimore™, Entrust®, iPlanet™, Microsoft®, Verisign, and others
- X.509 Certificates

■ Encryption:

- Hard Disk Encryption (optional)
- File Encryption

■ OTP Number Generation:

- OATH 160-bit

■ Personal Password Manager

- Microsoft Internet Explorer

■ Authenex SDK:

- ASAS Authentication API
- ASA Management API
- A-Key® API



Authenex®

Authenex, Inc.
1489 Salmon Way
Hayward, CA 94544, USA
T.+1 877.288.4363

www.authenex.com