

## The Authenex A-Key<sup>®</sup> Token

The Simple, Mobile and Secure Token with Up to 1 Gigabyte 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<sup>®</sup> token. The v4 A-Key<sup>®</sup> token is a password-protected USB token that offers up to 1 GB of encrypted storage for files and applications. It leaves no footprint wherever it is used. The A-Key<sup>®</sup> token is also tamper-proof and provides protection against brute force penetration.



### Benefits:

#### Secure and Immediate Deployment

Applications can be stored and launched from the A-Key<sup>®</sup> token. This significantly reduces deployment costs, while integrating security features into a single, easy-to-manage platform.

#### Total Mobility

Because our storage-class A-Key<sup>®</sup> token is driverless, no installation on your PC is necessary. You have complete freedom to use any available computer. With our embedded applications, the v4 A-Key<sup>®</sup> 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<sup>®</sup> token is equipped with on-board user memory that ranges from 128MB up to 1GB 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<sup>®</sup> token is safe from loss or theft. For added security, the A-Key<sup>®</sup> token is programmed to self-erase after a configurable number of failed login attempts.

#### Simplified Management

The v4 A-Key<sup>®</sup> token contains a simplified management interface that enables two levels of password protection. It also enables A-Key<sup>®</sup> token users to disable password protection, define and change A-Key<sup>®</sup> Token passwords, edit A-Key<sup>®</sup> token lock and self erase settings, unlock an A-Key<sup>®</sup> Token, and erase an A-Key<sup>®</sup> Token.

#### Assists in Compliance Security

The A-Key<sup>®</sup> token helps facilitate regulatory compliance when used with the Citrix<sup>®</sup> 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 1GB
- Real Time Encryption
- Self Erase Mechanism
- PIN Protection
- PIN Management
- User and Administrator Modes

■ **Symmetric Key Cryptography**

- AES 128-bit, 192-bit and 256-bit
- Secure Hashing Algorithms
- SHA-1

■ **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
- -0° to 50° C
- Storage Temperature
- -10° to 70° C

■ **Physical Characteristics**

- Casing
- ABS plastic, tamper evident

■ **Operating Systems:**

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



**Authenex**<sup>®</sup>

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

[www.authenex.com](http://www.authenex.com)