

The A-Key® 3500 Token

The Authenex A-Key® 3500 token is a chip-based authentication token that offers total mobility with maximum flexibility. The A-Key® 3500 token is the core component of our entire suite of two-factor e-security applications, including strong authentication for VPN, LAN or Web; Strong Web Access Control; Secure File Exchange and Secure Digital Certificate Storage. The versatile token can be used to generate a One-Time Password for authentication. This storage class device can also be inserted into the USB port of a computer for PKI or Challenge-Response authentication – all without the need to install drivers, which makes it not only versatile, but totally mobile.

A-Key® 3500 tokens use the same PC functionality as Smart Cards for Windows domain network log on. However, A-Key® 3500 tokens do not require card readers or the added time and effort to deploy them and train users.

A-Key® 3500 tokens users can configure their tokens so that, once inserted, the token automatically launches the configured Web site in the host computer's default Web browser.

Every A-Key® token is unique, with an assigned electronic serial number (ESN) and a randomly (or administratively) generated 4096-bit shared secret. This ensures non-repudiation of each A-Key® token and Challenge/Response sequence. The convenient car key-sized form factor is completely portable for ease of use.



One-Time Password

The event-based One-Time Password function of the A-Key® token presents unique 6-digit numbers that can be used alongside a password for strong two-factor authentication. The random number generation engine is modular for specific algorithms, including the OATH (Open Authentication) algorithm and others.

Challenge-Response

Our unique Challenge/Response technology uses an onboard encryption engine to execute encrypted Challenge/Response with local or server-side software.

PKI

The A-Key® token is equipped with an embedded Crypto Service Provider (CSP) and crypto functions for PKI authentication. It has on-board 1024/2048-bit RSA key generation and signing, along with X.509 Certificates.

Total Mobility

Our USB storage class A-Key® token enables pre-installed clients or applications to go where users go, enabling those users to authenticate without the need of installing software anywhere, in order to login to a network at any time. The secure storage area of the A-Key® token enables the flexibility to use any computer with just one click.

Secure Certificate Storage and Use

With the addition of ACert™ software, the A-Key® 3500 A-Key® token users can take their digital certificates and key pairs anywhere and use them for PKI-related activities, such as Windows Smart Card Logon, digitally signed and encrypted email and PDF documents, single sign-on for Web sites, VPNs, etc.

Secure Web Logon

My A-Key™ software is optional software that enables A-Key® 3500 token users to securely store Web site logon credentials and automatically log in to Web sites without having to touch a keyboard. With keyloggers on an estimated 50% of all computers, My A-Key™ software on the A-Key® 3500 token is not just convenient, it is necessary.

A-Key® 3500 Token Specifications

Standards Compliance:

- Public Key Infrastructure
 - On-board 1024/2048-bit RSA Key Generation, Signing
 - Microsoft CAPI 2.0 Compliant for Certificate Storage
 - PKCS#11
 - PKCS#12
- Symmetric Key Cryptography: AES 128-bit, AES 256-bit, DES, 3DES, DES-X, MD5 and RC2
- Secure Hash Standard: SHA-1 (FIPS 108-1)
- OATH Algorithm
- USB 1.1 Specification

Hardware:

- On-Board Security Processors
- On-The-Fly Encryption
- SHA-1
- Optional Extended On-board Flash Memory to 512K (Standard 128K)
- Connector: USB 1.1
- Memory Size: 512 KB (On-board Flash Memory)
- Casing: ABS Plastic

Supported Software:

- Operating System(s): 2000, 2003, XP
- Remote Access (With Authenex ASAS® Authentication Server):
 - Dial-up to a remote server with Microsoft RRAS and RADIUS
 - VPN with Microsoft, Check Point, Nortel, Cisco Systems, Netscreen, Safenet and others using RADIUS
 - SSL VPN

Authentication Interoperability:

- Windows Smart Card Logon Compatibility
- Network Login for MS Windows XP, 2000
- Secure Web Access (Microsoft Internet Explorer and Netscape Communicator)
- Citrix nFuse
- RADIUS
- Secure File Exchange
- Microsoft ISA Server

PKI Certificate Storage: Compatible with leading Certificate authorities including Baltimore, Entrust, iPlanet, Microsoft, Verisign, and others.

Encryption:

- File Encryption
- One-Time Password Number Generation: OATH 160-bit

Extra Features:

- URL Auto Launch
- A-Key® Management Tool

SDK:

- A-Key® Device API



FOR MORE INFORMATION
www.authenex.com



Authenex®

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

www.authenex.com