



ASAS™

Authenex Strong Authentication System

Two-Factor Authentication for VPN and Web Access

Features and Benefits

"60% of intrusions are the result of password-only authentication"
-- Federal Bureau of Investigations

Access Points Protected - Access is only granted when a specific and unique A-Key is used along with an individual's password.

Simple to Deploy, Easy to Administer - Implementation is typically finished in one or two hours. Administrative, managerial and computational overhead are greatly reduced. The challenge/response process is encryption based - eliminating re-synchronization issues that plague other solutions.

Easy Integration for Added Layer of Security - ASAS integrates with your existing security infrastructure. The A-Guard™ authentication server uses RADIUS and TCP/IP protocols, is VPN and firewall interoperable, and supports ODBC to use SQL databases.

Secure Design - The patent-pending chip aboard the A-Key is hacker proof and will fail if removed from the board.

Non-Duplicable - An assigned Electronic Serial Number and a randomly (or administratively) generated 4096-bit shared secret ensure that each key is unique.

Safe and Easy to Use - The user's password is never transmitted over the network or recorded in a central depository. The transition for users is simple - as it is just like using an ATM card at your local bank.

Affordable and Scalable - ASAS is based on a simple and efficient production model; it not only costs less than the industry norm, but scales easily for mass distribution.

ASAS™ marks a new advance in strong (two-factor) authentication for remote VPN and web access. Our unique, patent pending technology utilizes two-factors: something you have, and something you know, as the basis for an extremely secure solution for authentication and encryption applications. Our chip and software are integrally engineered to create a platform of security applications.

100% Two-Factor Authenticated = 100% Safe

Two-factor authentication systems are to network security what a lock and key are to the front door of your home, and yet the majority of small and mid-size networks have been unable to either afford or effectively administer the two-factor solutions available to date. The costs of mass deployment often prevent large enterprises from full implementation - leaving holes in their perimeter. ASAS now ensures that all networks can afford to fully deploy and administer two-factor authentication, leaving just one question: which networks can afford not to?

Strong, safe, easy and affordable

The A-Key™ USB token is central to our platform of security applications. The chip-based A-Key conducts challenge-response sequences directly with our A-Guard™ authentication server using AES (Advance Encryption Standard). The simplicity and production efficiencies inherent in this new approach eliminate the expense and administrative issues associated with traditional solutions.

The "Last Mile" in Authentication

ASAS extends the authentication point from the IP address to an end-user's specified A-Key USB token.

Interoperability With Other Authenex Products

ASAS is fully compatible with other Authenex products, including:

AOne™ - An integrated product from Microsoft and Authenex, featuring Authenex ASAS, ASAC™ and Microsoft® Internet Security and Acceleration Server 2000 (ISA). AOne offers a suite of two-factor network security applications, plus two-factor access control of in-bound and out-bound web pages and files.

Secure Privacy 2.0™ - Allows mobile professionals and consumers to encrypt files, securely exchange files with other Secure Privacy users, delete files securely, and manage passwords.

EDSKI™ (Exchange Dynamic Symmetric Key Infrastructure) - Provides a full spectrum of encryption services for file encryption and secure email as well as delivering the benefits of Public Key Infrastructure (PKI) at a fraction of the cost.

PKI-Ready - The A-Key carries a 15KiloByte (KB) password-activated memory area that can be used for securely storing private keys and certificates

A-Guard Server Requirements

- Microsoft® Windows 2000 Server with Service Pack 2.0 or above.

A-Guard Server Hardware Requirements

- 1 - Available USB port (version 1.1 and 2.0 supported).
- Memory - 256 MB RAM
- Free Hard Disk Space - 20 MB

ISA Server Requirements

- Microsoft® Windows 2000 Server with Service Pack 2.0 or above running Microsoft® Internet Security and Acceleration Server software
- 1 - Available USB port (version 1.1 and 2.0 supported).

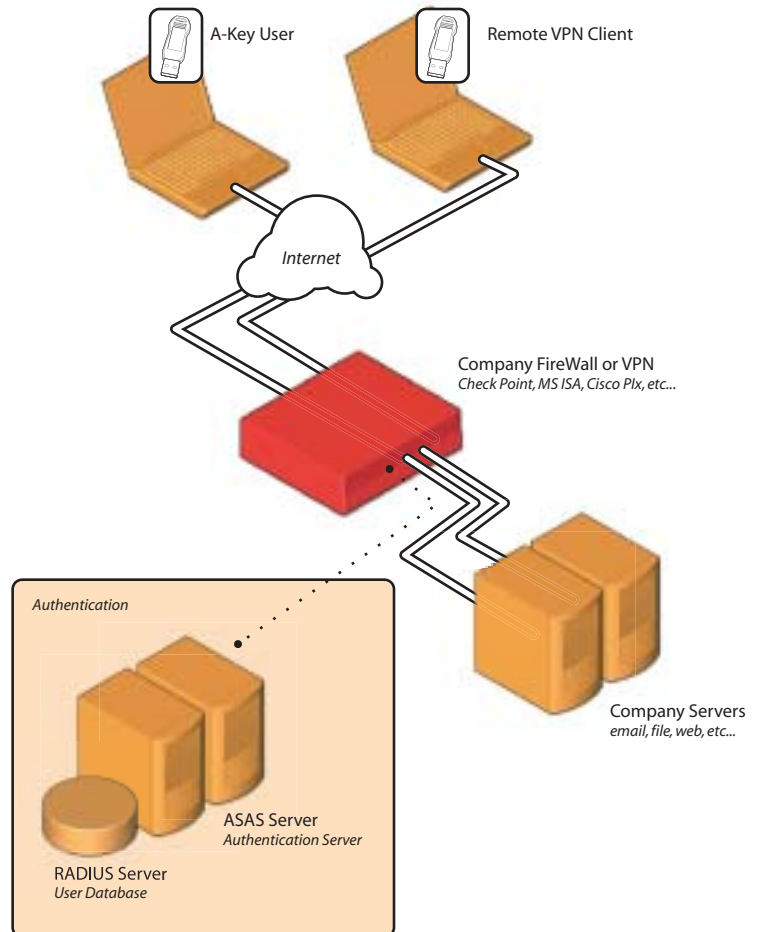
Client Software Requirements

- Windows 98, Windows Me, Windows 2000, or Windows XP.

For a complete list of VPN clients supported, please visit the Authenex website: www.authenex.com

Client Hardware Requirements

- Windows client with one available USB port (version 1.1 and 2.0 supported).



Authenex, Incorporated: www.authenex.com

Corporate Headquarters
333 Hegenberger Road, Suite 555
Oakland, CA 94621 USA

tel. +1 877 AUTHENEX
tel. +1 510 568 6558
fax. +1 510 568 7228

Copyright ©2000-2002 Authenex, Inc. All Rights Reserved. Authenex, A-Key, ASAS, AOne, A-Guard, ASAC, EDSKI and Secure Privacy 2.0 are either registered trademarks or trademarks of Authenex, Inc. All other trademarks, tradenames, service marks, service names, and images mentioned and/or used herein belong to their respective owners.