Mass-Distribution Two-Factor Authentication System

Cost-Advantage Security for the Enterprise and Critical Data
"Think of what changes when literally everyone in the developed world can have a strong network authenticator the way everyone has an ATM card."
Executive Summary ................................................................. 1

Authenex Offers Many Returns on Your Security Investment ........................................... 3
  Total Cost of Acquisition ............................................................................. 3
  ROI of Security Technologies .................................................................... 5
  Consolidation Savings: Eliminating the Need for Multiple Systems ....................... 6

One Technology Offering Myriad Security Solutions ....................................................... 7
  Two-Factor Authentication Solutions .......................................................... 7
  Encryption Solutions .................................................................................. 10

The Gear: Authenex's System Merges Proven Technologies ............................................ 12
  A-Key: ASIC-Based Two-Factor Token Is Attack-Proof ...................................... 12
  The A-Key: Feat of Semi-Conductor Design, a Coup for the Authentication Arts ...... 13
    A-Guard Authentication Server & Authentication Protocol ............................... 14
    Authenex Authentication Scheme - An Important Crypto Advance ................. 14

User Perspective: Initialization and System Set-up ......................................................... 15

Administrator's Perspective: Resources Maximize Flexibility ....................................... 16

Three Deployment Models for Maximum Flexibility ....................................................... 17
  Enterprise Turn-Key Package .................................................................. 17
  Enterprise Production Package .................................................................. 17

  Authenex EDSKI Subscription Service ....................................................... 17

A World of Ubiquitous Two-Factor? Authenex Says Yes ................................................ 18
One of the most basic and pervasive security vulnerabilities for networked computing environments is the use of logins and passwords, an exposure that always lands at or near the top of most every security expert's list of vulnerabilities. By 2005, business and government spending on VPNs, firewalls and other network access control technologies will top $14.2 billion, according to IDC. However, too many of many of these security systems also rely on passwords, authenticators which can be defeated by sloppy habits (i.e. writing down passwords in the workspace), by social engineering or through scripted, automated attacks that even novices can download and operate.

Authenex rejects the status quo and focuses on the basic question of how to cost effectively deliver strong authentication. The company's two-factor, hardware-based authentication system works with greater ease than even password systems, while employing a hardware token key that cannot be forged. Password systems demand only one factor for authentication - something you know; two-factor systems require a password and the presence of a hardware token - something you know plus something you have. The Authenex two-factor system is more affordable than any two-factor system yet devised, lending itself to practically any application scenario from internal network security to managing E-commerce access. The Authenex system represents a major advance in network security that is reminiscent of the introduction of Automatic Teller Machine (ATM) cards introduced to the banking industry 25 years ago.

The Authenex Strong Authentication System (ASAS™) has been developed to work with the ASIC chip-based A-Key. The A-Key is a hardware device that connects to the Universal Serial Bus (USB) port of any desktop PC, laptop, palmtop, thin client or other terminal devices and works with the A-Guard authentication server to manage access to networks or Web sites. When a user wants to request access, he will insert the key into the USB port and type a PIN (password) into a dialogue box. It works like an ATM card, a scheme so familiar that users intuitively understand it.

The Authenex solution lends itself easily to mass distribution. The A-Key, for example, is inexpensive enough to be given away for free in consumer applications. Many Web commerce models have failed due to profit-killing fraud. Meanwhile, fiduciary and regulatory pressures are quickly mounting, compelling one industry after another to adopt means for authenticating, auditing and securing transactions, communications and customer records.

For the enterprise, the Authenex solutions deliver stronger and more effective authentication for a fraction of the cost of other systems. From the IT manager's point of view, the A-Key operates like a reader-less smart card. The USB-hosted authenticator allows for quick and easy deployment since USB ports are on almost all terminal devices. Using the Advanced Encryption Standard (AES) encryption, the Authenex system enables strong two-factor authentication for local and internet-based applications.
ASAS™ gives network managers, applications designers and marketers freedom in developing authentication and auditing schema. Most importantly, to help keep security budgets under control, the Authenex system offers considerable savings by consolidating authentication regimes into a single low-cost system. ASAS supports remote VPN, Web, LAN, and wireless authentication. Also the A-Key™ strengthens PKI and SSO by securely storing digital certificates and user credentials; thereby providing mobile two-factor authentication.

Authenex's EDSKI™ (Exchange Dynamic Symmetric Key Infrastructure) cryptosystem provides a suite of encryption services that deliver the benefits of Public Key Infrastructure (PKI) without the management headaches and budget-busting costs of PKI. The EDSKI system employs government approved AES to secure transmitted data, sign documents and transactions, as well as to validate file authentication and integrity.

The EDSKI client software (Authenex Secure Privacy) works with the A-Key to provide two-factor encryption and decryption for any local files or folders. This tool allows users to keep confidential files private even in a shared PC environment at the office or home. Additionally, it provides data privacy protection in the all too common situation of lost or stolen notebook computers. The EDSKI server, whether hosted in an enterprise or as a subscription service through Authenex, allow encrypted files to be securely transferred to a specific A-Key holder and only the targeted recipient(s) A-Key can decrypt and view the file. 

Reliable user authentication is the foundation of all information security systems. When an enterprise has strong authentication, it mitigates many significant security exposures. With ASAS and EDSKI, strong authentication and encryption solutions are no longer prohibitively expensive, even for small and medium sized enterprises.
A primary focus of Authenex is to offer technology solutions that provide all the authentication and cryptographic services an enterprise requires - at the lowest possible cost. To do this, the Authenex solutions combine inexpensive hardware tokens with cryptographic systems to authenticate users, encrypt archived files on terminal devices, and apply legally recognized electronic signatures for integrity validation as well as for evidentiary and auditing purposes.

Authenex performed cost-benefit analyses for enterprises implementing the Authenex solutions. There are a number of ways to measure and analyze the value of technology and here, we will examine the Authenex ASAS solution using three different approaches:

- **Total cost** of initial acquisition;
- **ROI** for basic security functions, based on a common scenario;
- **Consolidation savings** from deriving security services from one system.

## Total Cost of Acquisition

Below is an acquisition analysis of the most common authentication technologies and the Authenex system, based on a thousand-seat scenario. Authenex isn't the least expensive solution out of the box - some low-end "software tokens" carry off that prize. It is, however, the lowest-cost hardware-based two-factor system by a wide margin, one that can satisfy the application requirements in commercial and even retail consumer deployment scenarios given its low cost of acquisition.

<table>
<thead>
<tr>
<th>System</th>
<th>Number of Users</th>
<th>Estimated Deployment Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenex</td>
<td>1000</td>
<td>$37,000 - $42,000</td>
</tr>
<tr>
<td>RSA SecureID</td>
<td>1000</td>
<td>$116,776</td>
</tr>
<tr>
<td>Challenge-Response Tokens</td>
<td>1000</td>
<td>$60,000 - $100,000</td>
</tr>
<tr>
<td>Smart Cards</td>
<td>1000</td>
<td>$60,000 - $65,000</td>
</tr>
<tr>
<td>Biometrics</td>
<td>1000</td>
<td>$100,000</td>
</tr>
<tr>
<td>Hardware Tokens</td>
<td>1000</td>
<td>$80,000</td>
</tr>
<tr>
<td>Software Tokens</td>
<td>1000</td>
<td>$60,000</td>
</tr>
<tr>
<td>PKI</td>
<td>1000</td>
<td>$100,000 - $200,000</td>
</tr>
</tbody>
</table>

1. Latest Authenex Price List - includes tokens and A-Guard authentication server
2. GSA pricing schedule from Electronic Systems of Richmond (<www.esr.com>), based on prices for 4-year tokens, 1000-seat ACE Server license and annual maintenance fee for the 'Plus Maintenance' contract
7. Ibid
In this analysis, we've omitted login/password systems because, given the risk exposures associated with such systems, they are actually worse than no protection at all in some ways. Not only do users abuse such systems by leaving passwords pasted to monitors, but they're also open to attacks with downloadable hacking tools. Despite such weaknesses, these systems are still quite expensive. A call to a Help Desk for a password reset can cost an organization US$32.50 to US$57.50, according to Gartner Group, Inc. (Forrester Research also found that password management costs upwards of $200 per year, per user.)

Cost per-token or per-seat is only representative of the cost of adding a new seat to an existing system. Typically, authentication schemes require user tokens, an authentication server as well as authentication and authorization management software. Some of the two-factor systems, considered in the development of the price ranges in the previous chart assume the presence of a working PKI; therefore, other costs may not be included in the this chart.

ROI of Security Technologies

Like all value-divining metrics, there are a number of ways to calculate a return on investment. The most sophisticated models of security ROI account for annual dollar costs of security losses, maintenance costs and statistical measurements of a technology’s effectiveness - numbers unavailable for the surveyed technologies. Another method of modeling ROI is by assuming a baseline of loss-and-recovery burdens and calculating the cost of eliminating the security exposures that precipitate losses with each technology.

\[
\text{Loss-and-Recovery Burden} \div \text{Investment} \times 100 = \text{Security ROI (\%)}
\]

In this simplified formula, the Return on Investment (ROI) is determined by the cost of replacing lost data objects (proprietary images, client lists, patent applications) and the cost of the labor required to restore systems that have been damaged by a security breach. For purposes of comparison, we've assumed a common loss-and-recovery burden of $250,000 - substantial but less than 10% of the average loss reported by respondents to the CSI/FBI Computer Crime Survey in 2001 that reported dollar-denominated damages of: $2,031,337.
By the ROI calculation above, based on the upper limits of each technology's estimated acquisition cost, Authenex is ahead of the competition by a wide margin. It should be noted that rate of return and ROI is a function of the loss-and-recovery burden that an enterprise actually bears. Authenex stands out by making two-factor authentication affordable in a much wider range of application scenarios than was previously thought possible.
Of course, a complete security solution does more than authenticate users to the network, although strong authentication forms a cornerstone for all other security functions. Beyond initial authentication, a comprehensive system must also enable:

- Secure transfer of data, so that critical information will not be compromised.
- Application of legally recognized electronic signatures so that critical documents and transactions can be authenticated and audited.
- Secure archiving of files against theft and the loss of confidentiality.

To acquire these security functions, enterprises need to implement a number of security technologies. Typically, an enterprise would use an internal password system authenticating employees to a network, a two-factor authentication system for remote users, a cryptographic system for securing e-mail and signing documents and a file-security system to encrypt files on laptop computers.

All of these systems have their own associated costs for deployment and maintenance. However, each system alone omits some essential functionality, compelling IT managers to deploy multiple security systems. With the Authenex system, internal and external authentication routines can be controlled by ASAS; the EDSKI cryptosystem can be used to encrypt files for document signing and transactions-signing routines; and, archived files can be secured on laptops with end-point encryption.

Quite simply, Authenex has pulled it all together by developing a comprehensive technology platform providing everything an enterprise needs for managing user authentication and assuring data privacy, data integrity and data authenticity.
Authenex’s ASAS and EDSKI products create authentication and security schemes that were previously closed to most enterprises and many specific applications. ASAS and EDSKI hold out cost-advantaged security in two principal deployment areas - strong authentication and encryption applications to secure documents, records and transactions.

<table>
<thead>
<tr>
<th>Two-Factor Authentication Solutions for Enterprise &amp; E-Commerce</th>
<th>Encryption Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote access / VPN authentication</td>
<td>Secure Privacy (local file encryption)</td>
</tr>
<tr>
<td>E-Commerce site authentication</td>
<td>Record authentication</td>
</tr>
<tr>
<td>Membership and ASP sites</td>
<td>Hard drive lock -- (Encryption of entire HD to prevent access to programs and files)</td>
</tr>
<tr>
<td>LAN authentication</td>
<td>Record authentication</td>
</tr>
<tr>
<td>Wireless</td>
<td>Record integrity validation</td>
</tr>
<tr>
<td>Mobile two-factor authentication for PKI and SSO</td>
<td></td>
</tr>
</tbody>
</table>

Two-Factor Authentication Solutions

ASAS simplifies the toughest authentication functions for internal authentication and management of off-site users connecting to the network. The A-Guard authentication server is designed to interoperate with existing network architecture. It is RADIUS-protocol compliant, able to communicate and work with all the popular firewalls, VPNs, RAS, and NAS. Currently running in a Microsoft Windows 2000 and Linux platforms with a built-in LDAP directory (thereby, enabling it to synchronize with the enterprises’ network directory services whether it is LDAP or Active Directory), it can support LDAP and Active Directory. (For more, see A-Guard Authentication Server & Authentication Protocol on Page 18.)
**Remote Access / VPN Authentication** - Authentication is critical to providing knowledge workers with convenient remote access to corporate data, while providing IT staff with improved security, simpler manageability and easier integration. Authenex's two-factor authentication solution is compatible with the world's most popular Remote Virtual Private Network (VPN) solutions including Check Point, Cisco and Nortel in order to provide these critical capabilities to today's enterprises.

![Diagram of Client, VPN Server, A-Guard, Domain Controller, File Server / Exchange Server, LAN Users]

**Web Authentication** - The Authenex two-factor authentication solution is so much less expensive than competitors that it enables mass deployment to any number of users, like ATM cards. The viability of ASAS to intra-enterprise and B2B e-commerce applications is obvious, as these low-cost authenticators can make deployment of secure Extranets for managing critical businesses processes easy - and inexpensive. Web-based applications are ASAS™-enabled with APIs or servelets. Every user is authenticated with strong two-factor technology and every transaction can be electronically endorsed, in accordance with electronic signature laws, with an AES key unique to the user. Authenex can revolutionize the market for online banking, stock trading, online gaming, and Internet auctions with the first, easy-to-use authentication system that can potentially eliminate the billions of dollars that Internet businesses lose annually to fraud. Strong two-factor authentication stops intruders and electronic signatures, and makes it far harder to refute transactions.

"For the consumer, using an A-Key has high-tech appeal, the token providing a 'secret decoder' that gives the user his membership in the crypto cognoscenti"
For many e-businesses, the costs imposed by fraud make profitable online businesses impossible by devastating already thin margins. The A-Key™ is inexpensive enough to give away to customers for added security in even the lowest-margin enterprises. Login/Password systems do not provide the two-factor authentication strength required to secure electronic transactions.

In addition, for retailers or consumer service providers, the A-Key also provides ideal branding opportunities. Printing the corporate logo on the back of the token makes for functional consumer give-aways that will make a brand impression every time it is used. For the consumer, Web-based services using an A-Key will have a certain high-tech appeal and the token itself becomes a physical credential of the holder’s membership in the cryptography cognoscenti.

For all types of online trading, Authenex’s A-Key can bring strong authentication to the task of managing consumer relationships and business relationships and, most importantly, locking out fraud.

*A Unique Authentication Offering via Microsoft ISA Server* - Working closely with MS ISA server, ASAS goes far beyond simple support for the RAS and VPN functionality with strong authentication. The collaboration of Authenex and Microsoft, has created a very compelling combined product offering. The combination of ISA with ASAS will deliver not just authentication to just a website, but down to every single page served, enabling the most detailed of authentication regimes. Highly confidential material can only be viewed with the activation and presence of an associated and authorized A-Key.
Two-Factor Authentication Solutions (continued)

Event-Based Authentication - ASAS also provides two-factor authentication for tasks such as originating and approving loans, issuing purchase orders, and for accessing sensitive and personal information. In addition, ASAS allows an enterprise to audit access to sensitive information as required by government regulations or industrial conventions. When an application reaches a critical - or regulated - stage, ASAS can be integrated into an application to require specific authorization to review, for instance, a patient record. Event-based authentication capability integrates easily into existing legacy or Web-based applications.

LAN Authentication - The Authenex ASAS can be used to support any LAN configured for LDAP or Active Directory. Current authentication methods such as password protection or newer smart cards are being used to enable authentication within today's enterprises. Authenex' two-factor authentication solution is much more secure than one-factor, password-based systems, dramatically less expensive and easier to deploy than smart cards. What's more important in terms of manageability, the same system can be used for remote access and a host of cryptographic security services once it is established for local authentication services.

PDA Token Extension - By the end of 2002, users will be able to download the shared secret of the A-Key into a PDA in a one-time encrypted form and thereby turn the PDA into a token serving as the second factor of authentication. In doing this, the user can have two-factor authentication for both accessing a wireless network and for protecting the content of the PDA with AES encryption. Meanwhile, the hardware A-Key can still be employed without any change in usage profile or performance.

Enhancing PKI - Public Key Infrastructure (PKI) keeps track of users' keys with "digital certificates," which associate an individual with a unique "public" key. (That key can be used by correspondents to encrypt messages to an individual which can only be read if he possesses the correlating "private" key to decrypt.) PKI is complex and, since the private key is often stored on a workstation, subject to compromise by physical access to the machine or via unauthorized network access. With ASAS, private keys are stored on tokens. This increases security dramatically, and makes PKI a more mobile solution. Digital certificates can also be stored on tokens, in a PIN-secured area, reducing the certificate management burden. Bottom Line: Authenex's system enhances PKI implementations by closing its inherent security vulnerabilities. The A-Key is seamlessly integrated to with Microsoft's CryptoAPI (MS-CAPI) key pair generation.

Encryption Solutions

One by one, industries and government agencies are being confronted with regulations mandating security and auditing systems for processing of electronic records. Critical documents and transactions have to be electronically signed in accordance with laws governing electronic signatures enacted in recent years. Electronic signatures and documents need to be checked for authenticity. Critical internal communications have to be conducted through secure channels. In addition to other major drawbacks, the solutions offered by PKI to satisfy these requirements can entail substantial modifications to business policies and processes. With Authenex's EDSKI system, important files can be secured anywhere the user stores them. In addition, critical transactions, authorizations and documents can be electronically signed, validated and audited according to the most rigorous evidentiary standards, and easily integrated into almost any business process.

End-Point Security - Files in local storage devices have become subject to increasing vulnerability over the past few years. For example, many corporations and even defense agencies have reported increasing volumes of sensitive documents, stored on unsecured laptops, falling into the wrong hands. The loss of such vital information can be extremely damaging, if not catastrophic. The EDSKI and the Secure Privacy suite protect against such security breaches and also provide "Critical transactions, and documents can be signed and audited, according to the most rigorous evidentiary standards. "
data privacy and integrity checking in shared computing environments as well as on laptops and mobile devices. Using a hardware token for both encryption and decryption of local files ensures data security from unauthorized access or theft. In addition, for access assurance, keys can be recovered by IT staff, even if tokens are lost or stolen.

Secure File Transfer - Files secured with EDSKI encryption can be securely transferred to any user - and only the recipient's A-Key can decrypt the file, thus providing electronic signatures, data integrity validation and document confidentiality. Once an AES-encrypted file is sent to an intended recipient, the file can only be decrypted by that specific recipient's unique A-Key. After the server authenticates the recipient's token, the encrypted file can be opened by the recipient. With this scheme, any number of important business processes can be secured and made to comply with evidentiary or privacy requirements that may be mandated for a business transaction or a critical document.
Authenex's ASAS and EDSKI systems use a symmetric key scheme — the 128-bit U.S. government-adopted Advanced Encryption Standard (AES). Authenex authentication and cryptographic suite combine the efficiencies of symmetric key cryptography with the flexibility of public-key cryptographic systems, while sidestepping the management headaches associated with each. By using a puzzle-based challenge/response scheme to authenticate users, the Authenex system further avoids the additional costs and overhead otherwise required for creating secure channels to transmit keys.

Since no keys are transmitted during the authentication process or at any time, the Authenex system avoids one of the most enduring weaknesses and exposures of all cryptographic systems: managing and securing the keys themselves. Equally as important in the management of an information security system, encryption keys in the Authenex system are fully recoverable by IS staff.

**A-Key: ASIC-Based Two-Factor Token Is Attack-Proof**

Authenex has leveraged its expertise in semi-conductors to build a USB-based authenticator token that is attacker-proofed at every level of its physical make-up and in every facet of logic design. But despite the high technology built into the A-Key, from the user perspective, operating an A-Key is as simple as punching in a PIN at an ATM machine. The user will never be called upon to drive the authentication system and, by design, he plays no role in keeping it secure.

When a registered user plugs the A-Key token into the USB port, an on-key program calls up a dialogue box into which the user types his password. Authentication at this stage is done locally and entirely on the A-Key. If the wrong password is entered, a user can only enter it again after a one-second delay. This built in pause mechanism helps to secure lost keys and other key-attack situations by adding years to a full-blown brute force attack (where every possible alpha-numeric string is attempted).

Only when the correct password is entered is the user data released to perform the correct challenge-response puzzle calculation that actually authenticates the user to the A-Guard authentication server. (For more, see: A-Guard Authentication Server & Authentication Protocol, Page 1819.) Users can give away their passwords by taping them to their monitors or writing them on their desks - or they can lose or give away their A-Keys - each without imperiling the authentication system. Only through collusion - giving away the A-Key and providing the PIN to an attacker - can the system be compromised.
The A-Key is a single propriety ASIC chip, sealed in one piece injection-molded enclosure using a USB interface to connect to terminal devices such as PCs. The ASIC contains the key's Electronic Serial Number (ESN); a unique 256-byte ID Pad specifically assigned to the user's ESN that is employed in the challenge/response puzzle test during authentication; and 16 unique AES keys.

After the user has initialized it, the A-Key stores the user generated password or pass phrase (up to 64 ASCII characters) in secured memory for user authentication to the key. The password is never transmitted. It is known only by the User unless the corporate policy dictates that the password be stored in a central file. Further, for customized applications, the A-Key has 15K of password-protected memory for user data such as private keys for PKI implementations.

Using an ASIC eliminates the reprogramming attacks that have been mounted successfully on EPROM-based USB-based tokens. All of the chip's memory resides under the ASIC and that memory space is entirely password-enabled. The ASIC will execute no commands before the correct password has been entered - and the user authenticated.

<table>
<thead>
<tr>
<th>Data</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESN</td>
<td>Token-specific Identifier</td>
</tr>
<tr>
<td>ID PAD</td>
<td>256-byte randomnumber matrix for puzzle-based authentication protocol</td>
</tr>
<tr>
<td>AES Keys</td>
<td>16 discrete keys applicable to different enterprises, applications or resources</td>
</tr>
<tr>
<td>Password</td>
<td>Personal Identifier Number set by user during initialization</td>
</tr>
<tr>
<td>Password Secured Memory</td>
<td>15K of Password-secured programmable memory to hold cryptographic keys (for PKI) or other data</td>
</tr>
</tbody>
</table>

The organizing principal behind the architecture of the A-Key is to limit access to the chip's data by eliminating the attacker's access to the logic in the A-Key's ASIC chip containing the user data. The ASIC chip's logic set only contains 9 commands, leaving a small number of hooks for attacks. In critical logic areas with secret data such as the ID Pad, the chip does not provide "read" commands, precluding a software-based attack by isolating data.

Further, if an A-Key is lost or stolen, the token is protected against dictionary attacks or exhaustive search attacks in which every possible alphanumeric string combination is attempted. A-Key requires a one to two -second cycle period for every password entry, forcing attackers to wait a full second every time they enter a wrong password. The delay effectively adds years to a full-blown brute force attack.

The chip itself is impervious to a decap attack - a method by which an antagonist peels the silicon off the chip itself, layer by layer. If such an attack is conducted, the password data and ID Pad will be destroyed as they are held in memory, denying the attacker any secret data useful for impersonating the user and executing a bogus authentication.

Each A-Key's 16 AES Keys and ID Pad can be leveraged for different applications within an enterprise or used to operate across multiple enterprises to authenticate a user. For example, KEY 1 of an A-Key could be used by one department, and KEY 2 by yet another department within the same enterprise. Or, KEY 1 could be used to authenticate a user to his own company and KEY 2 used to authenticate him to an Extranet deployed by one of the company's vendors.

In this last example, the vendor would be provided with a copy of the ID Pad and KEY 2 which would be employed to authenticate the user through the vendor's own A-Guard system. That information would give the vendor no useful information for copying and impersonating the user's identity on his own enterprise network as there, he is authenticated using KEY 1.
The A-Guard server sits on the network behind the corporate firewall, providing authentication services for users anywhere throughout the enterprise network, external networks and access points through which customers, vendors and employees connect with the network. Here, in the Secured Zone, the A-Guard authentication server manages and coordinates authentication with the corporate account database and the corporate application server.

The A-Guard is RADIUS compliant and, for ease of deploying remote access schemes, also incorporates the Extensible Authentication Protocol (EAP). (For enterprises operating Windows networks, the inclusion of EAP makes development of remote access schemes a straight-forward operation because Microsoft has integrated an EAP infrastructure into Windows 2000 and later releases of its operating systems.)

The Authenex A-Guard package includes APIs for Windows Internet Information Server (IIS) and - for the Java world - a package of servelets. These components speed the integration of Authenex's authentication suite into practically any application in the enterprise. With them, any application accessible through the LAN, Intranets, Extranets or via remote logon can be quickly Authenex-enabled with minimal disruption of the existing IT infrastructure.

The A-Key/A-Guard suite is called a two-factor system but the authentication protocol is actually a multi-part procedure. Once the user has entered the correct PIN, the A-Key unlocks the user data and activates the authentication routine, which entails a number of rounds of data trading and computation as follows:

The A-Key reports out its ESN to the A-Guard. If the system recognizes the ESN, the A-Guard will send out a 128-bit randomly generated unencrypted string to the A-Key. That string is essentially an instruction for numbers contained in the ID Pad to be transposed into a new configuration.

An internal algorithm on the A-Key performs a calculation using the numbers that precipitated from the transposition. The A-Key then takes the product of that calculation - the answer to the puzzle - and encrypts it with its AES key. Now it will perform a second round of AES encryption by using the result of the first encryption round as the second AES key and encrypts a session ID from the server.

That encrypted message is sent to the A-Guard which performs its own calculation. The A-Guard doesn't have the user's PIN - but it has the ID Pad and one or more AES keys that the user has on the A-key. With that data, the A-Guard takes the puzzle string, performs its own calculation and decrypts the encrypted message it received from the A-Key.

If the answers match, the user is authenticated.

Why is this an important advance in the cryptographic arts? First, by encrypting a unique session identifier from the server as the answer, it insures that the answer cannot be replayed by an attacker for access into the network in a new session.
Second, the system is a symmetric key system that has managed to solve the long-standing problem of key distribution. A basic problem with other symmetric key systems is that any leakage of data about the key will compromise security. An attacker who intercepts your key can decrypt all your communications.

Public key cryptographic systems sought to solve this problem by splitting the key into two parts. Correspondents exchange public keys to encrypt communications. Those communications can be decrypted by correlative private keys held and used by the parties to whom the communications were addressed. (Alice uses her private key to decrypt messages sent to her from Bob that Bob has encrypted with Alice's public key that is published and distributed by Alice for easy access.) Although public key cryptographic systems offer a wealth of functionality, they also present a huge management burdens and exact high computational demands.

The Authenex system's breakthrough in this area is that it allows correspondents to use symmetric key cryptography, with all its inherent advantages in low computational burden and simple management, without exposing any data about the keys to interception.

No secret key data traverses the network, eliminating a vexing class of security exposures entirely. By design, the Authenex system has no exposure to so-called Man in the Middle (MITM) attacks or replay attacks because a hacker cannot glean information from authentication messages and because every authentication event uses a new and unique puzzle.

Work station attacks in which an attacker gains control of the computer and copies the private keys are also neutralized as the user's keys all reside in the highly secure, password-protected hardware token.

For users, the browser-based registration process for the A-Key is almost entirely automated. After receiving their A-Keys, users can take themselves step by step through the initialization process. Even computer novices can sign-up for authentication services remotely in self-service mode.

Drivers for the A-Key are self-installing on any Windows machine. Push the new A-Key into the USB port and they'll fire as soon as the Windows Plug and Play system detects them. (Drivers for A-Key authentication and Secure Privacy encryption applications are available via download from www.Authenex.com.) Once the drivers are installed, the initialization software boots and guides the user through a simple sign-up procedure to authenticate the user. Then he/she can proceed to choose his password and initialize his A-Key.

Post-initialization, the enterprise matches the ESN to the profile of the user to manage access. The user enjoys quick authentication and the network manager can update the user's privileges in their current point of network administration. The user's access privileges are automatically replicated to the A-Guard server, making the administration of all A-Keys a transparent and simple.
Establishing authentication routines for users are almost as easy for administrators as they are for users. Administrators send out keys to users with the authorization profiles pre-set and mapped to an Electronic Serial Number (ESN) assigned to a user's A-Key. After the authentication routine is complete, the user's access privileges and resource allocations are controlled by the existing domain controller or AAA server.

The ASAS suite, Authenex’s authentication system, is distinguished as much by what it offers in the network administrator’s domain as it is by the cutting-edge technology it contains. USB ports are on all PCs being shipped today, eliminating the need for a reader. The system employs MS 2000 and SQL databases (Linux in late 2002). With a built-in LDAP slave directory, it can easily integrate with both Active Directory and LDAP directory.

For the security manager, Authenex ASAS offers maximum flexibility in developing authentication services for a perimeter security implementation. ASAS integrates seamlessly with RADIUS servers (commonly used by firewall and VPN systems) and can be employed in tandem with firewall and VPN technologies for greater strength and mobility. PKI can also be made more manageable with an A-Key token employed to carry digital certificates.

The ASAS feature set is also expansive enough to contribute to deployment scenarios that animate perimeter-based security and/or host-based security schema. (Perimeter security protects network resources by controlling access to all entry and exit points of the network; host-based security is the technique of securing an individual system and all its applications and resources from attack.)

Each approach has its proponents and each has made important contributions to the thinking that informs the larger security disciplines, yet these philosophies are often at odds due to limited corporate security resources. With the Authenex system, corporate security managers will be able to choose the techniques that best serve their companies' needs, without draining their IT budgets.

Administrator’s Perspective: Resource Maximizes Flexibility
Three Deployment Models for Maximum Flexibility

Authenex strives to make the authentication process as flexible and as easy to administer as any other enterprise application. Towards that end, Authenex offers the A-Key/A-Guard system in three different deployment configurations: the **Enterprise Turn-Key Package**, the **Enterprise Production Package** and the **Authenex EDSKI Subscription Service**.

**Enterprise Turn-Key Package**

In the **Enterprise Turn-Key Package**, the enterprise acts as its own administrator of ASAS and EDSKI and maintains the technology entirely on-site with fully enabled technology delivered in a turn-key package from Authenex. Authenex licenses the server software and sells the A-Keys pre-programmed with unique Electronic Serial Numbers (ESN), AES keys and ID Pads - the basis of the puzzles - as the enterprise requires, providing updates and support through an annualized maintenance fee based on the numbers of A-Keys issued.

**Enterprise Production Package**

In the **Enterprise Production Package**, the enterprise finishes the development of the A-Key tokens and manages the deployment and maintenance of its authentication system. Authenex provides blank A-Keys with an assigned ESN and A-Key programming software to embed the ID Pad and the AES Keys. In effect, the enterprise custom programs their own shared secrets. Authenex licenses the A-Guard server software and the A-Key Production Software and sells the A-Keys as the enterprise requires, providing updates and support through an annualized maintenance fee.

**Authenex EDSKI Subscription Service**

For a low annual fee, users can transfer encrypted files and make use of Authenex EDSKI server. The file itself is never transmitted through Authenex; therefore, Authenex will never have access to the actual transmitted files. After the encrypted file is transmitted to a recipient, only the information in the file header is sent to Authenex and used for the key exchange to enable the recipient to decrypt file. For enterprise customers, a complete online management and reporting console will be available.
When it comes to network security, experts agree on one point: A lot of the problems associated with authentication go away when correspondents and network users are authenticated with hardware devices. This point is clearly demonstrated by the success and near-ubiquitous deployment and acceptance of ATM cards throughout the developed world.

Until now, two-factor systems were designed and marketed as high-cost, high-margin items. Authenex now provides a two-factor solution that can be mass-distributed, bringing the security of this technology to almost any network and application scenario and enabling strong two-factor authentication in applications where it was previously cost-prohibitive.

Authenex has created a new class of Hand-held Authenticator (HHA) technology. Authenex combines the best characteristics of two-factor identification systems and challenge-response schemes with a suite of cryptographic services, all in one user-friendly device. The solution is built on a foundation of proven technology that delivers the power of other available solutions, but at a mere fraction of their cost. In fact, the Authenex system is so effective and low-cost that it makes authentication services a value-adding proposition by creating new application scenarios that would not be economically feasible without an inexpensive, strong authentication system.

Now it's your turn to build those compelling online applications and security regimes and to dream up the value-adding services that can put your enterprise ahead of the competition. START HERE: Think of what changes when everyone in the developed world can have a strong network authenticator the way everyone has an ATM card.