

BENEFITS:

- Increased productivity for a mobile workforce
- Simple, secure and easy to use for mobile employees
- Strong two-factor authentication
- Integrates seamlessly with existing infrastructure
- Combined authentication methods for a convenient and flexible user experience
- Ease of deployment with no user software installation
- Eliminates “password only” vulnerabilities
- Simplified management of user accounts
- The most affordable solution available
- Same A-Key token will work in conjunction with an entire suite of security applications

Strong Authentication for Virtual Private Network Technology

Problem:

Maintaining a balance of strong security for enterprise networks while allowing employees access from remote locations is essential for a successful business. The preferred means for companies to allow secure remote access is through a Virtual Private Network (VPN). Although VPN technology protects data in transit over public domain by creating an encrypted “tunnel” through the public network at a very affordable overall cost, it does not protect the access point itself by authenticating the person requesting access. Information that is secure while in transit may just be ending up in the wrong hands at its final destination.

Solution:

The Authenex Strong Authentication System (ASAS®) provides simple and secure remote access to company networks using VPN technology. ASAS is a two-factor authentication solution that utilizes the Authenex A-Key® token for security far beyond password only solutions that are inherently vulnerable to attacks. The ASAS two-factor authentication process is based on identifying a user by something they have (the A-Key) and something they know (a PIN) – just like a bank ATM card system. Anyone who uses the VPN for network access will need to use both factors.

With the ASAS solution, a VPN user can use stand-alone One-Time Password (OTP) or USB-based authentication from the same device. Users will generate a One-Time Password (OTP) from the A-Key and enter it along with their PIN. Each time an OTP is generated, it is a unique value that cannot be used again. Every session will require a unique OTP value so that even if someone were monitoring the login process, they would not be able to use that login information again. The A-Key is a hybrid token that also contains a USB interface that offers a “driverless” experience without having to install software on the computer that’s being used.

The ASAS VPN solution is designed to integrate with your existing infrastructure to minimize downtime and avoid exorbitant deployment costs that other solutions have. ASAS works with all of the top VPN providers, including Check Point Software Technologies, Juniper Networks/Netscreen technology and Cisco Systems. Plus, the convenient Web Management Console gives administrators an added tool that makes managing accounts easier.