

BENEFITS:

- 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 Local Area Networks

Problem:

The Local Area Network (LAN) is one of the most common means of information and application sharing with server or processor and is one of the most difficult to secure. Whether Ethernet, FDDI or Token Ring, the shared source and communications amount to a mass entity that is difficult to audit for individual attacks. This makes any computer connected, or that can be connected, to the LAN a security liability.

Solution:

The surest method of LAN security is through user authentication. An unauthorized user can seize control of certain LAN features if the profile is not specific to a particular type of discretion, which is why LAN security has many loopholes.

The Authenex Strong Authentication System (ASAS®) provides simple and secure LAN authentication. 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 requires LAN access will need to use both factors.

With the ASAS solution, a LAN 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, which lends itself to an ease-of-deployment for administrators.