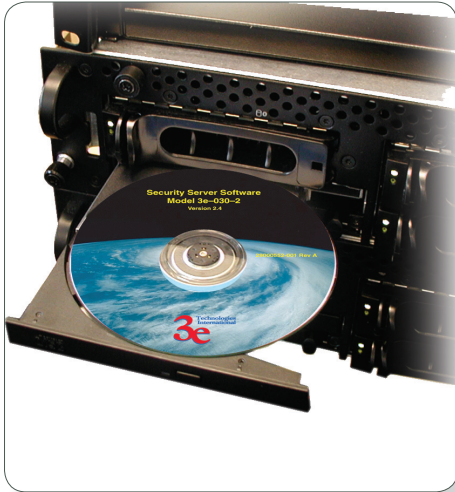


UltraView Security Server

3e-030-2



The UltraView™ security server is an integral component of 3e TI's WLAN security suite. The security server software runs on a Windows™ 2000, 2003, or NT server and creates, distributes and manages “dynamic” per session keys for each user, each time they log into the network. It also authenticates each user by distributing and managing digital certificates.

The industry standard digital certificates provided by the UltraView server are highly secure. They use two-factor authentication and meet the stringent security requirements for wireless access.

3eTI's WLAN security suite utilizes the strong government AES standard for wireless encryption. This encryption algorithm is sufficient for most high security needs. However, since the security server provides dynamic session key management, users get the ultimate wireless security.

The UltraView security server can be scaled to your environment. It is simple to install and it can run as a service. Since it has a small memory and CPU footprint, it can also coexist with other server applications. This makes it ideal for both small and large operations.

BENEFITS

- Per session dynamic key generation
- Facilitates distributed encryption
- Secure X.509 certificate authentication
- Seamless connectivity
- Supports CRLs
- Enables 802.11i
- Small footprint, runs as service

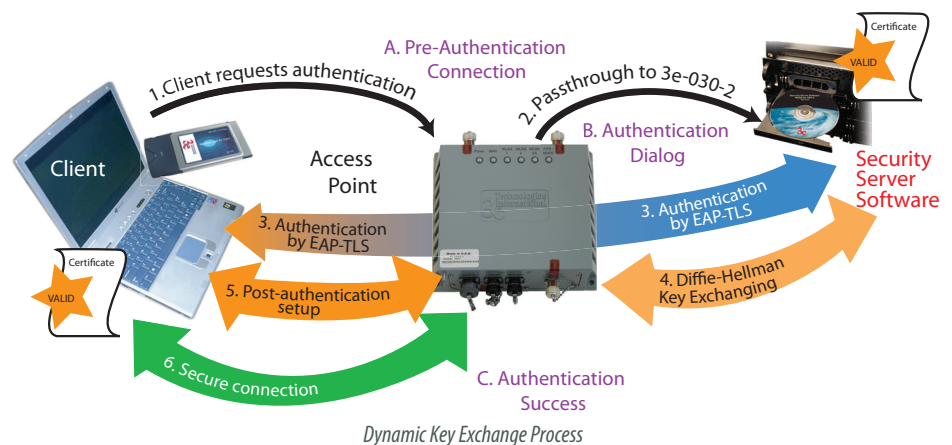
FEATURES

- Radius 802.1x/EAP-TLS for authentication
- Diffie-Hellman and RSA for key exchange
- X.509 certificate-based authentication using PKI infrastructure

Overview

Once the security server is installed and configured on a separate server, the security officer employs the Windows certificate authority to request and issue a certificate for each client device accessing the wireless LAN.

The security server then utilizes dynamic key management, the preferred configuration for very secure authentication, to automatically authenticate all clients, using a root certificate. Once authenticated, the client is issued a per session key, good only for the duration of that session.



3eTI's security solution operates at Layer 2 of the OSI Model. With the 3e WLAN security suite, each AP encrypts multiple clients. Therefore, each AP carries a small amount of the load. The 3e-030-2 security server will authenticate prior to user login, so connection is seamless.

The security server centralizes authentication while encryption is distributed. It employs a distributed encryption scheme such that the loss of one or more APs may reduce coverage but not security.

The 3eTI solution is also simple to implement and does not require changes to your existing network topology.

The dynamic key exchange techniques (Diffie-Hellman and RSA) used by the security server improve on 802.1x weaknesses in several places. For example, the security server uses the Diffie Hellman algorithm to perform key exchanging between itself and the access points instead using a non-standard algorithm, such as the MS-MPPE-SEND-KEY algorithm. It also uses HMAC-SHA1 for packet authentication instead of HMAC-MD5. This results in higher security.

The UltraView security server uses X.509 certificates to authenticate wireless devices and users. The system utilizes the certificate structure established by public key infrastructure (PKI) technologies.

In the PKI certificate structure, all certificates form a tree-like hierarchy. The trust point certificate is at the top, or "root", of the hierarchy, and is signed by itself. Intermediate certificate authority (CA) are signed by the trust point or another CA above the tree hierarchy. Intermediate CA certificates can then be used to sign other certificates. At the bottom level of the hierarchy are end certificates, which are not used to sign other certificates. In order for the 3e-030-2 security server to function, one or more trust point certificates must first be installed. For each trust point, an associated certificate revocation list (CRL) certificate must also be imported into the system. All intermediate CA certificates should also be installed, with their corresponding CRL certificates.

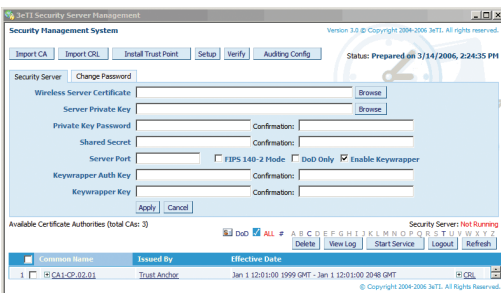
APPLICATIONS

In addition to providing excellent security for wireless applications within the federal government, Department of Defense (DoD), and civilian agencies, the 3eTI security

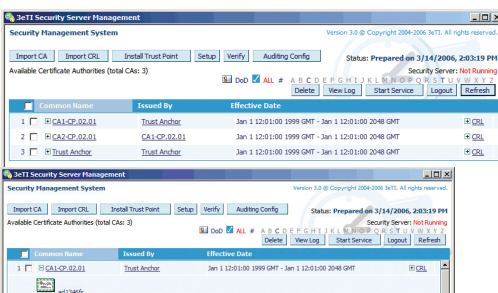
solution is ideal for the commercial market where security plays an important role. In industries such as financial services and health care (where HIPPA regulations require health information privacy and data integrity), separation of customers' data are not optional features — security is, in fact and by law, critical.

ABOUT 3eTI

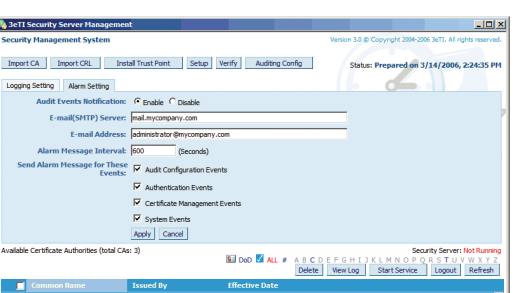
3e Technologies International (3eTI), an Ultra Electronics company, is a leading provider of highly secure wireless networks that enable critical systems security, infrastructure security and industrial automation for the military, government, industrial and utility markets. Its product portfolio includes proven and robust secure wireless mesh networks, sensor networks, cyber security, and perimeter security solutions, deployed for a range of applications, including military base security, onboard military ship communications, rapidly deployable public safety communications, and advanced metering infrastructure for SmartGrid programs. 3eTI's platforms are approved for use by the most stringent and demanding customers: the U.S. military.



Configuring the Security Server



Viewing Certificates



Audit Logging



Ultra Electronics
 3e Technologies International (3eTI)
 9715 Key West Avenue, Suite 500
 Rockville, MD 20850
 (800) 449-3384
 sales@3eTI.com
 www.ultra-3eTI.com
 www.ultra-electronics.com