# WLAN-Minder

## Wireless LAN Secure Access Enforcer

WLAN-Minder is a secure, hacker proof control centre for provision, management and administration of Wireless LAN networks. It offers enhanced Wireless LAN security by granting access only to clients possessing a personalized pre-programmed secure tokens like smart card, USB dongles and other biometric devices. Once the user token is connected to a computer, that computer is configured according to the information present on the token and the user is automatically connected and logged on to the allowed systems.

Based on years of NanoGlobes experience in communication and smart card technology, WLAN-Minder provides an open standard AAA (Authentication, Authorisation and Accounting) system by implementing a RADIUS based access, management and control centre incorporating and rigidly enforcing a hacker proof biometrics based strong two factor security tactics. All these facilities are housed within a small self contain, robust, reliable and noise free locally or remotely configurable device.

WLAN-Minder unique and simple to use solution can be deployed to support different wireless LAN topology and business models like, Enterprise solution, Hotspots solution and Community Network solution. WLAN-Minder open and standardised solution enables billing, network management and user customisation tailored to the needs of any organization.

WLAN-Minder has pre-installed software which is based on IEEE 802.1x standard allowing a wide variety of authentication and connection techniques for wireless and wired LANs. A Smart Media card is used for configuration, back up / restore. WLAN-Minder also includes a user-friendly application for issuing and management of secure tokens. The management functions can be protected by an administrator token and it's associated PIN. WLAN-Minder is an stand-alone controller and the initial configuration of the unit may be performed via USB or RS232. Once the basic network parameters have been configured, all management of the unit is performed via web browser (HTTP) using a Secure Sockets Layer (SSL) connection

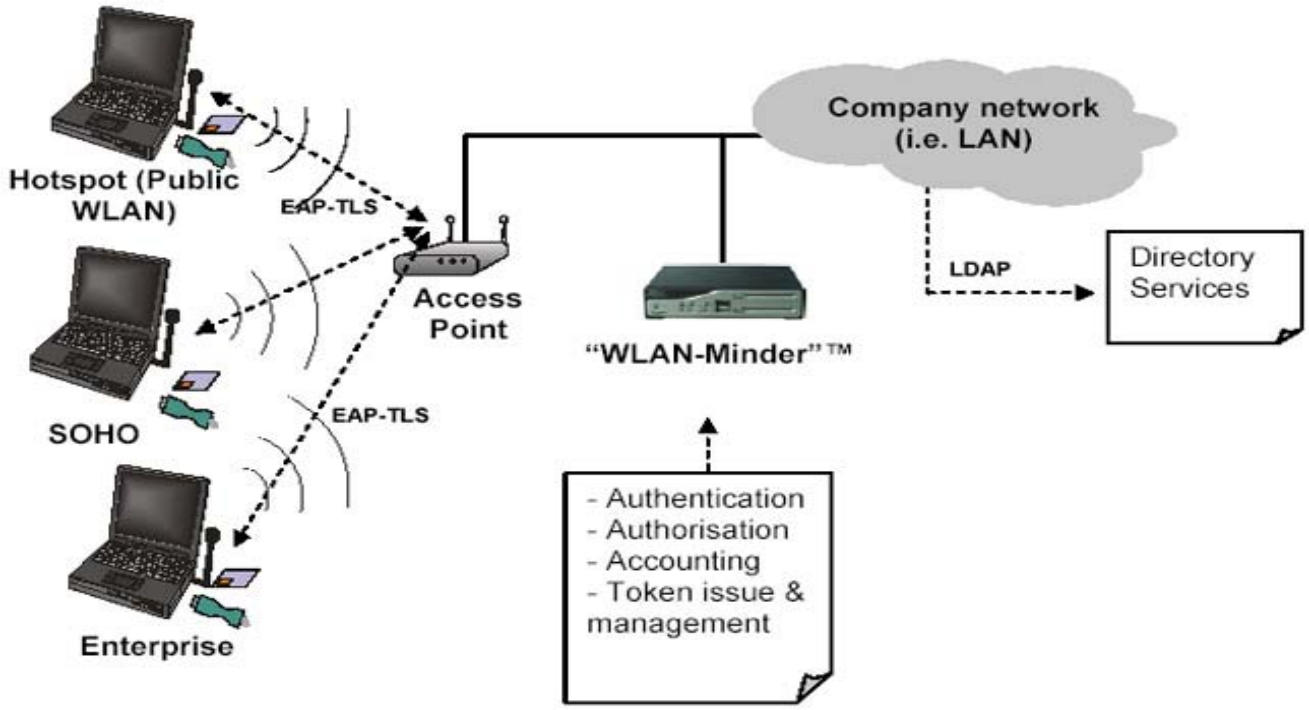
### WITHOUT THE "WLAN-Minder":

Intruders can eavesdrop and obtain wireless LAN Service Set Identifiers (SSIDs) and Media Access Control (MAC) addresses, in order to steal the credentials of an authorised user.

Hackers can force a rogue station between an authorised station and an access point and therefore route all traffic through the rogue station (man-in-the-middle attacks).

Intruders can spoof authorised users from the Wireless LAN, as well as introducing viruses and stealing valuable company information.

User's access time and information accessed cannot be controlled or monitored for security and billing purposes.




**WLAN-Minder**

**Security and Access Control for Wireless LAN**

# Benefits

## Easy to set up

WLAN-Minder unique and proprietary solution automatically sets up the Wireless LAN secure connection, so the end user doesn't need to configure the security connection. The user will only connect the pre programmed token (smart card, eToken, biometric token) to his/her PC and key in their PIN number to automate the authentication and customised authorisation. The option of just connecting via login and password is also included. WLAN-Minder protects small business as well as corporate LANs.

## Smart card / eToken personalisation

WLAN-Minder is used for issuing users smart cards or eTokens which ensure automatic and secure Wireless LAN set up. The management system is accessed via HTTP (web browser).

## Use of PKI

The security mechanism in the WLAN-Minder authentication solution is based on Public Key Infrastructure (PKI) and digital certificates. Protecting the end-user's private key is essential to the integrity of a PKI. The highest degree of protection available against malicious use is offered by a physical cryptographic token such as a smart card or an eToken. These tokens are used to store keys so that they can never be retrieved, duplicated or tampered with.

## Stand-alone self-contained system

WLAN-Minder is a dedicated AAA (Authentication, Authorisation, Accounting) radius server based on open standards. The WLAN-Minder includes a Smart Media card for configuration back up / restore, keeping system downtime to a minimum.

## Strong security

Strong 2-factor security (smart card or eToken) plus PIN entry in combination with mutual authentication (user and WLAN-Minder) using the innovative EAP-TLS security protocol. Data is protected against wireless eavesdroppers and man-in-the-middle attacks.

## Key Generation

WLAN-Minder control centre has a built-in key generation capability that offers a high integrity but economical default solution including support for on-board key generation for smart cards and eTokens.

## PIN and PUK management

When the private keys have been placed on the smart card, they are protected by the PIN and PUK codes. The WLAN-Minder PIN security solution automatically generates and sets the card's PIN, PUK, and codes.

## Audit

All actions by the system operators are always securely logged, providing a tamper resistant audit trail. All communication between administrator and the WLAN-Minder control centre is based on SSL v3 using strong authentication and encryption. WLAN-Minder control centre administrators use individual smart cards, permitting varying levels of access to system functions and procedures.

## Multi-vendor and multi-platform support

WLAN-Minder can be used with any other 3rd party Access Points and Wireless LAN adapters that support 802.1x authentication standard. It supports clients using Windows XP/2000 platforms.

## Multi application support

Via smart cards and eTokens.

## Reliable hardware

No moving parts fans / disks. Designed and manufactured in UK.


## Features

- Realises the complete Wireless LAN authentication and management, including key generation and smart token personalisation.
- Provides keys and certificates for smart cards and eTokens.
- Central management of authentication policies and procedures in a standalone RADIUS based controller.
- Generates ITU X.509 certificate format.
- Supports the PKCS#12 and PKCS#15, standards for PIN and certificate storage.
- Supports EAP and TLS.
- Support for LDAP v3 directories, for example, Microsoft Active Directory, Novell Directory Services (NDS).
- Supports PKCS#11 based eTokens / smart cards from Aladdin and Schlumberger.
- Remote Configuration using HTTP. Local Configuration using RS232 Serial Port. Access protected by Administrator smart card.
- More than one WLAN-Minder may be attached to the wired network to provide redundancy and share the authentication workload.
- Optional VPN support (CISCO VPN client, etc.).
- Optional support SNMP MIBs.
- Optional support SMTP mail event notification.
- Optional biometric based tokens.
- Optional key archiving facility.
- Optional UNIX client support.
- Optional support for Pocket PC Platform.
- Optional support for Soft Certificates.


**WLAN-Minder**

**Security and Access Control for Wireless LAN**

## How it is done

Software running on the WLAN-Minder control centre manages user Authentication and Authorisation, controlling user's access to the wired network from the wireless LANs, and monitoring all connections for auditing or billing purposes.

The Authentication task running on the WLAN-Minder control centre is responsible for checking the Wireless LAN user credentials. This is achieved using the PKI certificate and checking it against a central database or directory. WLAN-Minder allows authentication against existing Directory Services via LDAP standard protocol.

This process confirms the user is "who they claim to be". The Authorisation task consists of the provisioning or denial of user access to the wireless and wired network. Access is personalised according to permissions granted to the user – e.g. specific or group access, session time limits, time-of-day restrictions, point of access restrictions, etc. Finally, the accounting task logs connection data concerning all Wireless LAN connections (i.e. user name, time and duration of connection ...) for use in tracking, billing and auditing.

## The "WLAN-Minder" SOLUTION

The use of WALN-Minder solution together with the IEEE 802.1x standard (enabling access authentication), overcomes some of the major security drawbacks of a Wireless LAN. Threats such as intruders who pick off Service Set Identifiers (SSIDs) and Media Access Control (MAC) addresses, in order to steal the credentials of an authorised user, and man-in-the-middle attacks (where hackers can force a rogue station between an authorised station and an access point) are countered.

The protocol performing the access authentication in 802.1x is called Extensible Authentication Protocol (EAP) encapsulation over LANs (EAPOL). EAP provides a general framework for several different authentication methods (from passwords to challenge response tokens and public key infrastructure certificates). However WLAN-Minder make use of EAP-TLS, as it provides the highest level of security. EAP-TLS enables mutual authentication so users and network is protected against main-in-the-middle attacks. With EAP-TLS, both wireless and client are strongly authenticated to each other using digital certificates.

EAP-TLS (EAP -Transport Layer Security) uses PKI-issued (Public Key Infrastructure) digital certificates for strong mutual authentication. The WLAN-Minder sends its certificate to the client. The client validates the identity of the WLAN-Minder and if satisfied, it then sends the client certificate to the WLAN-Minder. The exchange of certificates is done in the open before a secured session is created.

WLAN-Minder will also dynamically change the WEP encryption key, so that the client can be re-authenticated and re-keyed automatically as often as needed without inconveniencing the end user. It also performs automatic user log on (after entering the correct PIN) to the approved Wireless LAN Access Point which is pre-configured on the security token.

**NanoGlobes Ltd.**

**www.NanoGlobes.com**

**info@NanoGlobes.com**