WIRED EQUIVALENT PRIVACY IN THE NOKIA A032

QUICK GUIDE

INTERNET

Contents

1. INTRODUCTION

This guide explains the different types of Wired Equivalent Privacy (WEP) that is used in the Nokia A032. After reading this quick guide you should understand the concepts of WEP and how it is implemented in the Nokia A032.

Nokia wireless LAN products and specific network planning are not explained in this guide. Wireless LAN security is not covered in this guide but is available in a separate Nokia wireless LAN security document.

2. CONCEPT OF WEP

2.1 IEEE 802.11 WEP

WEP is not a mandatory requirement in the IEEE 802.11 standard but it is defined in the standard to prevent possible security breaches by

1. Denying access to the Network by unauthorised users with similar Wireless LAN equipment. This is achieved in the standard by the use of authentication
2. Stopping the capture of wireless LAN traffic through eavesdropping. This is achieved in the standard by the use encryption

2.2 AUTHENTICATION

IEEE 802.11 defines two types of authentication methods:

Open System Authentication: This is a simple request and reply authentication and is used when it is not necessary for station to positively validate itself. Although no WEP encryption is used in authentication process any traffic passed is encrypted.

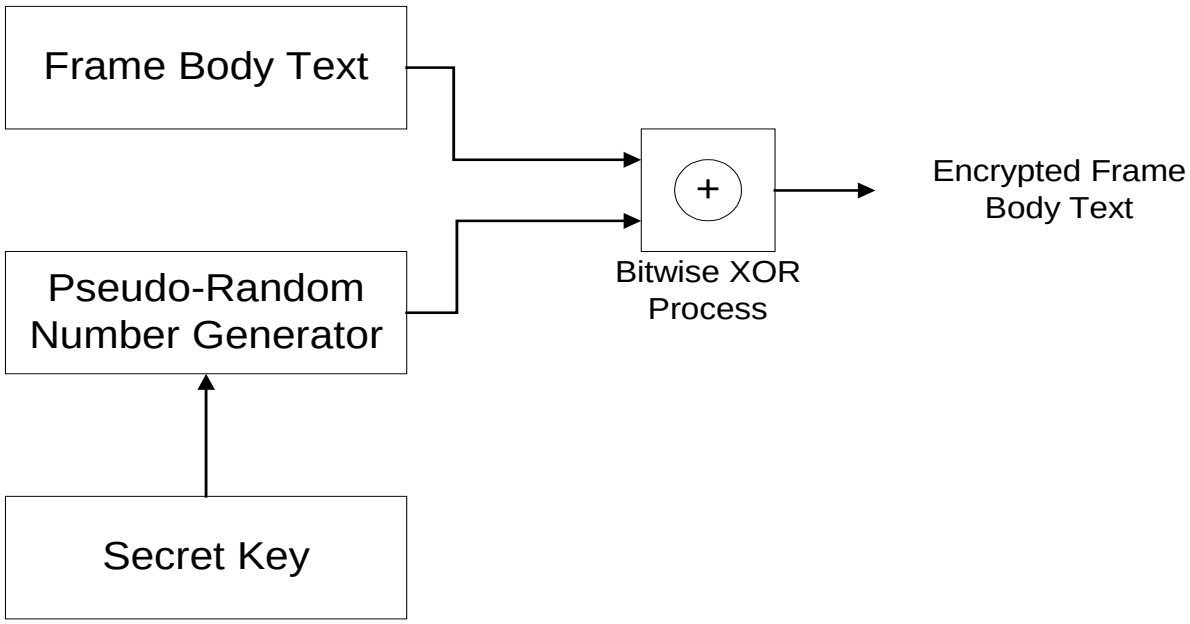
Shared Key Authentication: This is a more complicated method of authentication involves the encryption of text in the authentication operation.

1. The requesting station transmits an authentication frame stating shared key authentication.
2. The receiving station replies including 128 octets of challenge text.
3. The requesting station encrypts the challenge text and transmits it back
4. The receiving station de-crypts the text and checks it against the text it originally transmitted. The authentication is then rejected or accepted.

Note: The shared key is not passed over airwaves and therefor must be known by all stations beforehand and is a symmetric key.

2.3 ENCRYPTION

WEP Keys are used for the encryption process, implementation is purely optional under the IEEE 802.11 standard.



1. The plain text data is firstly run through an integrity algorithm so that the received data can be checked against modification

2. A key sequence is generated by inputting the shared secret key into a pseudo-random number generator

3. The plain text is bitwise XOR'd with the key sequence to create encrypted text, this is also known as cipher text.

4. The same key sequence is generated at the receiving station and the text is deciphered

5. The deciphered text is then run through an integrity algorithm and the integrity values are checked. If this check fails the frame is disregarded and failure message is sent.

The encrypted text is generated using a symmetric algorithm with the shared secret key consisting of 40 or 128 bits.

Note: Although implementation of WEP in Wireless LAN equipment is purely optional all manufacturers implement it. It is also a mandatory requirement for Wi-Fi certification.

3. WEP MODES IN THE NOKIA A032

There are 4 WEP Modes that can be used in the Nokia A032.

3.1 OPEN

This is not to be confused with open system authentication. Open Mode lets wireless stations associate with the access point using shared key authentication or no WEP authentication at all. All traffic that is sent to the associated stations is done without any encryption.

3.2 WEP

WEP Mode only allows shared key authentication. The shared key authentication is carried out using either a shared secret key or a personal key. All data is encrypted before transmission

3.3 PERSONAL.

Authentication is carried out using Shared Key Authentication using personal keys only. The personal keys can be stored locally on the access point or on a remote database, i.e. a radius server. All transmitted data is encrypted

3.4 WIFI.

This Mode Allows either open system or shared key authentication but all data is passed encrypted using a shared secret key.

4. WEP KEYS

4.1 SHARED KEYS

Both the access point and the wireless station can hold up to four shared keys, these keys are stored in ‘slots’, each slot numbered from 1 to 4. Only one of the four keys can be an active key in either the access point or station, the active key determines the key used for the transmission of data from that access point or station. The same key need not be active on both the access point and station but the corresponding key must be in the same slot otherwise the receiving station will ignore the transmission.

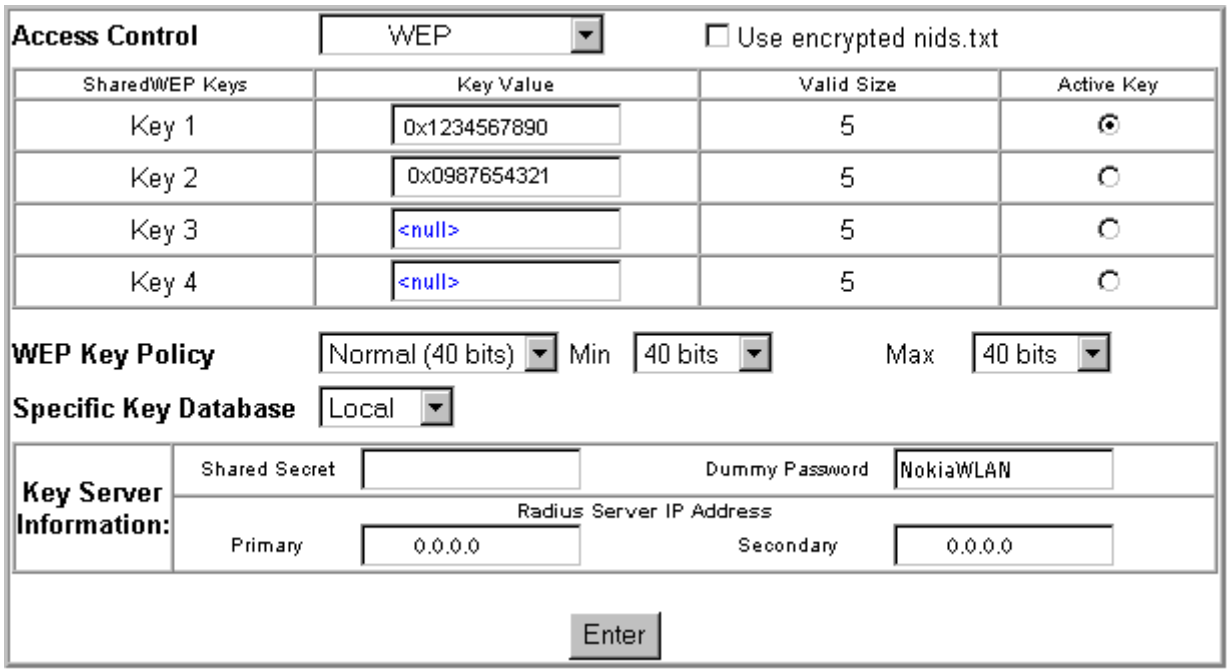


Figure 1. Web based management screen for shared WEP Keys.

4.2 PERSONAL KEYS

Personal Keys are implemented into the encryption process in exactly the same way as shared keys.

With a Shared key all the stations on the network have the same set of secret keys in the same slots, personal keys are stored on a Specific key database. The database can be defined as

Local - The keys are stored on the Access Point on the NID list along with the MAC addresses

Radius - The Keys are stored externally on a radius server.

Either - The Access Point checks the NID list then the Radius server.

4.2.1 Radius Server Database

The disadvantages of using a local database (on the access point) are that there is a maximum of 200 entries on the database and every access point on the Network must carry the same list. Storing the keys externally on an authentication server overcomes these disadvantages.

Note: All data that is passed between the Radius server and the Access Point is encrypted using a shared Secret.

The sequence for retrieving the key is as follows

1. The Access Point sends a RADIUS request to the authentication server containing a username and pre-defined dummy password in the WEP key field.

2. The RADIUS server looks up the username (usually the MAC address) and sends back either a reject message or an accept message. The accept message contains the WEP key (where the dummy key was)

3. The Access Point now uses the WEP key to challenge the station.

4.3 CUSTOM KEYS

The IEEE 802.11 Standard defines the length of the secret WEP keys as either 40 or 128 bits but the Nokia A032 allows you define the keys to be any length between these two parameters. Setting the WEP key Policy to custom enables the user to define the smallest number of bits that can be used for a key and the largest number of bits that can be used for a key allowing different keys to have different lengths.