Security White Paper

TABLE OF CONTENTS

1. Introduction

This white paper describes all the various security and authentication methods provided by the Nokia 9210 Communicator. Hardware, software, and other types of security are dealt with in this document. However, the user should bear in mind that the device itself or even the memory card can be stolen. There are methods that can be employed to restrict the use of such stolen property.

2. Hardware / SIM security

2.1 SIM Lock

The Nokia 9210 Communicator can be programmed to allow its use only with certain SIM cards. These cards fulfil certain predefined conditions, such as a predefined operator, or the phone could be programmed to operate with one SIM card only, for example. The SIM card identification function (SIM lock) can be automatically activated before the phone is delivered to the end user or at any other suitable time. The activated SIM lock can be disabled by entering the correct unlocking password. This password is operator and IMEI (International Mobile station Equipment Identity) specific.

If the SIM lock is activated and an incorrect SIM card is inserted, a note is shown each time the user switches on the device, or tries to access the SIM card to change the PIN (Personal Identification Number) code. The phone interface on the display cover displays the message ‘SIM card not accepted’ if the inserted SIM card is not acceptable. Emergency calls can be made at any time, however.

2.2 SIM Change Security

If the SIM change security setting is set to 'On' and a new SIM card is inserted (and the IMSI (International Mobile Subscriber Identification) code of the new SIM card is not in the IMSI list in the phone's memory), the user is prompted for a lock code. (see section 2.4 below, ‘Locking the device’).

2.3 PIN Code

The SIM card can be protected from unauthorised use with a PIN code. If the PIN code request is set to ‘On’, the code will be requested every time the phone is switched on. If an incorrect PIN code is entered three times, the SIM will request an eight digit PUK (Personal Unblocking Key) code. If an incorrect PUK code is inserted ten times, then the SIM card can be used only for emergency calls in which the user must contact the operator.

The PIN2 code is used as an added means of security for some features. For example, the PIN2 code must be entered if the user wants to reset the accumulated call meter or change the fixed dialling numbers. Incorrectly entering the PIN2 code three times causes the PUK2 code to be requested. Like the PIN code, the PIN2 code is 8 digits long. If the PUK2 code is entered incorrectly 10 times, the communicator will display the message ‘PIN2 code rejected’.

If the PIN2 code is entered incorrectly three times and the PUK2 code is entered incorrectly 10 times, only those features that do not depend on the PIN2 code can still be used. It is not possible to disable the PIN2 code.

2.4 Locking The Device

The Nokia 9210 Communicator has a feature that enables the locking of the whole device. In this locked state, the device and its data can only be accessed by entering the special lock code. Incoming faxes and data calls are accepted, and voice calls are accepted, and voice calls can be answered when the device cover is closed. The communicator can be set to be locked automatically within a certain time interval (1-15 minutes), or it can be locked manually, whenever the user wishes. If the phone’s power is off and the communicator interface is locked manually or by time-

out, the phone will also be in locked mode. In this case, the lock code must be entered before the PIN code when the phone is turned on.

The lock code state cannot be removed by formatting the device (all the user data and applications installed by the user will be deleted). Formatting the device does not remove the security settings. To get the lock code, the user must contact a service centre. If the lock code is entered incorrectly five times in a row, the communicator is locked for five minutes. During this period, the communicator will not even accept the correct lock code.

Note that the memory card is not locked if the card does not support locking. Theft of the memory card is possible even if the communicator itself is locked, and the card can be read with a PC memory card reader for example.

If your MultiMediaCard supports password locking (most older cards do not), you can optionally lock the card against unauthorised use. The card needs to be locked and unlocked manually. When in locked state, the information on the card cannot be accessed without reverse-engineering the card itself. Some of the Nokia 9210 Communicator software are stored on the MultiMediaCard. In order to be able to use this software, the card needs to be unlocked. The locking of the MultiMediaCard is independent from device locking discussed above.

2.5 Blacklisting SIM Cards and Devices

If your device or SIM card is stolen or lost, you should immediately report the loss to your operator. Your operator will close your SIM card. Most operators also maintain a list of stolen and lost devices. When such a mobile device appears on the network, it cannot be used to make calls, no matter which SIM card is inserted. You should therefore make note of your device's IMEI code and report it to your operator if you lose your mobile device.

Keeping the PIN prompt on your SIM on and having the automatic locking of the device on will greatly help to protect you from unwanted costs, should your communicator or SIM card ever fall into the wrong hands.

2.6 Call Barring

With a barring password you can block calls to unwanted numbers. This means that the cellular provider blocks certain numbers and the user cannot access these numbers unless the barring password is known. A user can obtain a barring password from a cellular provider. Incoming calls (voice, data, and fax) can also be blocked.

3. Radio interface security

3.1 Calls

The security of the radio connection between a GSM phone and the GSM network is specified in GSM standards. Encryption is used to protect radio transmissions. The GSM network specifies the radio interface security level, and the encryption applies to voice, data, and telefax calls. Note that encryption is only used between the GSM phone and the base station.

The level of security in radio transmissions depends on the network and local laws. Most countries use the strongest GSM encryption level. Another level of encryption is used in countries to which the export of stronger encryption is prohibited. Some networks may choose to use no encryption at all due to local laws or regulations, or for technical reasons. It is usually possible for the proper authorities to monitor any calls in a GSM network, regardless of the encryption used, depending on local wiretapping legislation.

User authentication in GSM networks is done with a SIM card. The authentication is a challenge-response type scheme as specified in GSM specifications. The strength of the authentication is network-specific. The SIM card authenticates the user based on their PIN code.

3.2 Short Messages

GSM networks have a bidirectional paging system called SMS (Short Message Service). This means that the user can send and receive short text messages using the GSM network. Short messages can be transported using GSM signalling channels, but these signalling channels are not encrypted. Therefore, short messages are not a secure way to transport data.

4. Software security

As the Nokia 9210 Communicator is a versatile and open programming environment, anyone can create new software for it. Malicious software is a security risk which should be taken into account. Fortunately, the Nokia 9210 Communicator has a secure software installation system that can be used to minimise the risks. The user must always be cautious when installing software, however.

4.1 Software Installation Security

Software is distributed in software packages called SIS files. These packages can be digitally signed. By signing a software package, the originator of the package makes sure that the package cannot be modified while it is being sent or stored to the communicator.

When installing software, the user will see the alleged originator of the package and the party that authenticates the originator's identity. For security reasons, it is recommended that software is not installed unless the user trusts both the originator (author) of the package and the authenticator (certification authority).

The questions the user should ask are: 'Do I allow software produced by *X* (the author) to be run on my device? Do I trust *Y* (the certifier) to vouch for the identity of *X* (the author)?' If either of the answers is 'no', the user should cancel the installation.

To view the currently trusted certification authorities, the user can go to the Certificate Manager tool in the Control Panel. The user can edit trust settings for each listed certificate. By giving a certificate trusted status, the user vouches that he/she knows that a given certificate really belongs to the given entity.

To summarise:

In order to maximise software security in your communicator,

- When editing trust parameters in the Certificate Manager tool, only trust those certificates whose origin you can be sure of, and only when you know that the certificate really belongs to the entity whose name is on the certificate. If you are in doubt, contact the certification authority's help desk and ask them for their certificate fingerprint. Compare the fingerprint with the one that is displayed in the Certificate Manager tool.

- Make sure that the software is intended for the Nokia 9210 Communicator.

- Only install software that comes in SIS files. Never install raw DLLs or EXEs. Be wary of requests that you 'copy file X to folder Y on your Communicator'.

- Only install software that has been signed and only install if you trust *both* the author *and* the certification authority.

- During the installation, be sure to read all dialog boxes that appear on the display. They may contain further security information.
- Nokia has a Nokia OK Logo program for third party software developers. Using software that has a 'Nokia OK' logo offers further assurance of the quality of the software.

5. Internet and intranet

Data communication over the Internet or other IP networks is not secure by default. To enable secure connections, the Nokia 9210 Communicator supports various security protocols.

5.1 Incoming Data Calls

By relying only on the factory configuration, it is not possible to access the Nokia 9210 Communicator's files from an incoming data call. However, as with any normal computer, malicious third-party software can potentially degrade the security of the device. Therefore, only install and use software that comes from a trusted source and is digitally signed by a trusted party (see section 4).

5.2 Attacks From The Internet

When connected to the Internet, it is possible to send data packets from the Internet to the communicator. As the wireless link is of low bandwidth, it is potentially possible to cause congestion by sending large amounts of useless packets to the device. Therefore, it is recommended that the dial-up link uses a firewall to filter suspicious packets. Many Internet service providers offer this service. The use of dynamic IP addresses is another recommended safety measure. Most, if not all, Internet service providers supply dial-in clients with dynamic IP addresses by default.

Also, installing defective or malicious third-party software (especially from Internet servers) in the Nokia 9210 Communicator may degrade security. Only install and use software that comes from a trusted source and is digitally signed by a trusted party.

5.3 Dial-up Security

The communicator requires a PPP (Point-to-Point Protocol) connection to allow connection to the Internet or to an intranet.

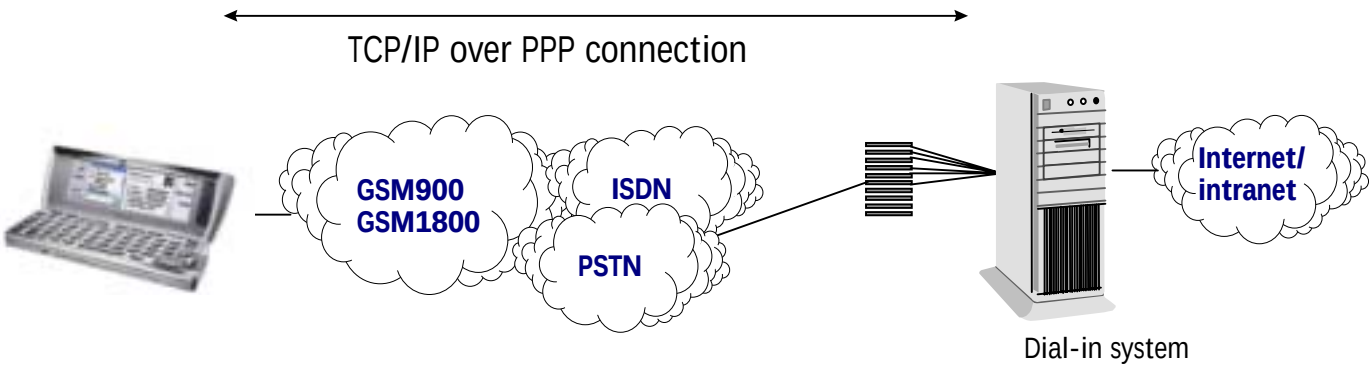

Figure 1: The communicator connection principle

The communicator supports the PPP authentication protocols PAP (Password Authentication Protocol) [RFC 1334], CHAP (Challenge Handshake Authentication Protocol) [RFC 1994] and MS-CHAP (Microsoft CHAP). Of these three, CHAP and MS-CHAP are more secure as they do not transmit the password over the network.

PAP works basically in the same way as the normal login procedure. The client authenticates itself by sending a user name and a password to the server, which the server then compares to its database.

With CHAP, the server sends a randomly generated challenge string to the client. The client combines this with its password and a one-way hash function; it then returns the result to the server. The server does the same computation and will then grant access if the client-supplied response matches that generated by the server. CHAP also sends challenges at regular intervals to ensure that an intruder has not replaced the client.

To enhance the security of PAP and CHAP, some other authentication methods are sometimes used when creating a network connection. These methods may include, for example, one-time passwords (password generators, tokens, or password lists). If the method works with normal PAP or CHAP, it can be used with the Nokia 9210 Communicator. Other login schemes can be supported using a login script. Some of the alternatives are described below.

5.3.1 Callback systems

Some dial-up servers call the user back after the user has first called the dial-up server. The number to call back can be stored on the server, and functions as an extra layer of authentication, as the attacker will have to use the phone number of the real user. Callback can also be used for reverse billing, as the caller will usually pay for the connection.

The Nokia 9210 Communicator supports three PPP callback protocols: IETF type 0 (server-supplied callback phone number) [RFC1570] and the Microsoft callback protocol in two different modes of operation (client-supplied and server-supplied callback phone numbers).

Note that the incoming callback data call (from the dial-up server to the Communicator) is expected to use the same data call parameters (normal or high speed call, analog or ISDN call) as the outgoing callback-requesting call (from the Communicator to the dial-up server). The GSM network and the dial-up systems must support this call type in both directions.

5.3.2 Centralised Security

One alternative approach is centralised security, which involves having the terminal or communications server authenticate a dial-in user's identity through a single central database, known as the authentication server. This server stores all the necessary information about users, including their passwords and access privileges. The use of a central location for authentication data allows a greater degree of security for sensitive information, a greater ease of management, and a more scaleable solution as the size of the network increases. Authentication servers can be configured in a variety of ways, depending upon the organisation’s preferred network security scheme. Common schemes for centralised security are based on RADIUS [RFC 2138] and TACACS [RFC 1492].

RADIUS and TACACS are open IETF standards, which have been adopted by many organisations. The advantage of these open standards is that they can be used between multiple vendors and shared among many products. Both RADIUS and TACACS+ provide the ability to pass security data to a variety of databases. RADIUS, TACACS, and TACACS+ can provide a single point of authentication and authorisation. Users can enter a single password and be automatically authenticated into the remote access server or even multiple servers automatically.

5.3.3 Multiple Passwords

Multiple passwords can be used to make the authentication more secure. Different passwords can be used for dial-up authentication and further access, such as mailboxes and Web pages.

5.3.4 Token-Based Security

Many of the most popular remote access security systems are based on a hardware token. As the token creates the one-time passwords, any potential attacker needs to be in possession of such a token. Often there is also a PIN code that must be entered in conjunction with the token.

Some of these products, such as SecurID by RSA Security, use a time-based token system. For example, when users dial into the server, they are prompted to enter a personal identification number (PIN), along with the six-digit number currently showing on their hand-held card. This number changes every minute at the same time as a corresponding number on the server, making it virtually impossible to gain access to the network without the card. There are also other variations of how SecurID cards are used, some of them having a built-in PIN keypad and some being pure software implementations.

5.3.5 Other one-time password systems

As the Nokia 9210 Communicator is an open software platform, it is possible to implement any kind of one-time password system (such as S/Key and OPIE) as a separate application. One-time password generators that are currently available for other Symbian operating system (EPOC32) devices can be ported to the Nokia 9210 Communicator with relative ease using the software development kit from Nokia.

5.4 SSL and TLS

The Nokia 9210 Communicator supports the SSLv3 (Secure Socket Layer) and TLSv1 (Transport Layer Security) protocols. These protocols are integrated in the socket interface, so third-party programs can easily use these protocols to offer secure Internet connections.

When using SSL or TLS, all data transferred over the secure connection will be transferred securely to the target server. This means that the security of the radio interface (GSM connection), dial-up access (PPP), and all Internet servers between your communicator and the target server are irrelevant. SSL and TLS will offer a secure channel through all of these.

If the target server is not capable of supporting strong security, security of this secure channel may be weaker than what it potentially could be. Servers that use weak security are often older servers outside the United States that use software that is of United States origin.

5.4.1 Web Browser

Web URLs (addresses), which start with 'https', are SSL -secured connections. The SSL connection is negotiated with the server and then the data is transferred over the encrypted connection. A small lock symbol is displayed as an indication that the connection is encrypted.

The encryption strength depends on the SSL server. The Nokia 9210 Communicator supports strong 128-bit encryption in SSL and TLS, but can downgrade its security to a lower level if the server is not capable of handling such strong encryption.

The authenticity of the Web server is determined by the help of certificates in the Certificate Manager tool. As discussed above in the software security chapter, the user can select which certificates are trusted and which are not. When connecting to a server, whose identity is certified by a trusted party, there will be no warning note. Otherwise, the user will be able to review the identification offered by the remote server. There is a set of certificates from major commercial certification authorities that is factory-installed and trusted by default. However, Nokia does not endorse any specific certification authority. New certificates can be added to the Certificate Manager by the user.

As a security measure, it is recommended that you never send confidential data to a server that is not trusted. Furthermore, make sure that the connection is encrypted before sending confidential data. Read the warning notes that are displayed as they may contain further security information.

The Hypertext Transfer Protocol (HTTP) also provides a simple authentication protocol which uses a username/password pair. It can be used to authenticate the user to a remote server. This method can be used over the SSL for additional security.

5.4.2 Reading and Sending Mail

Access to remote mailboxes (IMAP and POP) and sending mail (SMTP) can also be secured using the SSL/TLS. You can request a secure connection by ticking the appropriate box in the settings.

In order to use secure connections with electronic mail, the mail server has to support the “starttls” command (IMAP, SMTP) or the “stls” command (POP). In this model, the client first connects to the remote mailbox over an insecure port, and then negotiates the secure connection using the same TCP connection. This is the model that is currently supported by the IETF.

Note that sending electronic mail over a secure connection does not encrypt the mail itself, only the connection to the first mail server. After the mail continues to its destination from the first mail server, it is not encrypted. This feature is most useful when accessing mail servers in a secure intranet through a public Internet service provider.

In general, all Internet mail is insecure unless the mail itself is encrypted and/or digitally signed. The TLS connection only offers security for remote mailbox access and sending mail. Be cautious of sending confidential information in Internet mail.

5.4.3 Supported Encryption Algorithms

The selection of algorithms depends on the protocol being used. It is advisable to avoid the use of “export-grade” algorithms (RC4 with 40 secret bits and DES) for security reasons. The selection of the algorithms is done by the server, and the user cannot influence this. The Nokia 9210 Communicator supports the following cryptographic algorithms in SSL and TLS:

For server authentication and/or key exchange: RSA, DSA, and Diffie-Hellman. For data encryption: RC4™ (plus the “export” version with 40 secret bits), DES, and Triple-DES.

5.5 Other Internet Security Systems

Different applications can also be protected using passwords, e.g. after logging onto the Intranet, a password is required in order to use e-mail, the WWW, etc. The communicator supports these security mechanisms as long as they use the standards supported by the communicator.

6. WAP security

6.1 Dial-Up Security

When using WAP for a data call, dial-up security is the same as with Internet services. Please refer to the chapter above.

6.2 Connection Security

WAP uses an optional security layer called WTLS. This can be turned on in the settings, or the server can mandate it. WTLS security ends at the WAP gateway. Connections to the target server from the WAP gateway might not be encrypted.

The WAP Forum specifies WTLS. The Nokia 9210 Communicator supports strong 128-bit encryption in WTLS, but is able to lower the security level if required by the server. The Nokia 9210 Communicator supports server authentication and key exchange using the RSA algorithm and data encryption using the RC5™ algorithm.

Server authentication is done using a set of factory-installed certificates.