



# NOKIA D211

## DATA SECURITY

NOKIA





# Contents

1. INTRODUCTION .....	3
2. REMOTE ACCESS ARCHITECTURES .....	3
2.1 DIAL-UP MODEM ACCESS .....	3
2.2 SECURE INTERNET ACCESS (GPRS, WLAN).....	3
2.2.1 INTERNET SECURITY REQUIREMENTS.....	4
2.2.2 VIRTUAL PRIVATE NETWORKING TECHNOLOGY IN BRIEF.....	5
2.2.3 COMMERCIAL VPN APPLIANCES .....	6
2.2.4 PERSONAL FIREWALL.....	6
2.3 APPLICATION LEVEL SECURITY FOR INTERNET BROWSING .....	6
3. SECURE GPRS ACCESS TO CORPORATE NETWORK .....	7
4. SECURE WIRELESS LAN ACCESS .....	9
4.1 WIRELESS LAN ACCESS IN THE OFFICE .....	9
4.2 REMOTE WIRELESS LAN ACCESS .....	10
5. SUMMARY – SECURE CORPORATE ACCESS WITH THE NOKIA D211.....	11

## Legal Notice

Copyright © Nokia Corporation 2002. All rights reserved.

Reproduction, transfer, distribution or storage of part or all of the contents in this document in any form without the prior written permission of Nokia is prohibited.

Nokia and Nokia Connecting People are registered trademarks of Nokia Corporation. Other product and company names mentioned herein may be trademarks or tradenames of their respective owners.

Nokia operates a policy of continuous development. Nokia reserves the right to make changes and improvements to any of the products described in this document without prior notice.

Under no circumstances shall Nokia be responsible for any loss of data or income or any special, incidental, consequential or indirect damages howsoever caused.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy, reliability or contents of this document. Nokia reserves the right to revise this document or withdraw it at any time without prior notice.



## 1. INTRODUCTION

---

The new Nokia D211 multimode radio card is an ideal solution for mobile business users who desire to access the corporate network while on the move. The transferred information is often critical to a company's business, and such information should not be leaked to outsiders. Therefore, security has an important role when using the Nokia D211 for remote access services.

This document explains how security should be considered when using the Nokia D211. It introduces the basics of Internet security and illustrates a few reference architectures that enable a secure access to a corporate network over the General Packet Radio Service (GPRS) networks and Wireless Local Area Networks (WLANs).

## 2. REMOTE ACCESS ARCHITECTURES

---

### 2.1 DIAL-UP MODEM ACCESS

Until recently, remote access services have been mostly implemented using leased lines, dial-up modems, and remote access servers. The connection is established using public telephony network and well-known point-to-point protocol (PPP) available in almost each terminal software. The dial-up connection is established using a fixed phone or a wireless terminal. The remote access server authenticates the user with a password; typically no other special security mechanisms are deployed.

The Nokia D211 offers two alternatives for dial-up: GSM data and High Speed Circuit Switched Data (HSCSD). In this set-up, the GSM network protects the user data over the air interface. Thus the wireless access will not require any extra security extensions but can be used just like a fixed dial-up modem. The dial-up connection is typically established using Microsoft Windows dial-up functionality.

### 2.2 SECURE INTERNET ACCESS (GPRS, WLAN)

The new wireless Internet technologies, such as GPRS and wireless LAN, offer a faster and more cost-efficient way for accessing corporate data. The new access mechanisms require a few enhancements for the corporate remote access services platform to guarantee the confidentiality of data.

Figure 1 depicts the dial-up and remote Internet access architectures. The principal difference is that instead of a telephony network, GPRS and wireless LAN deploy the Internet backbone as a gateway to the company network. The user data is transmitted from the cellular network via the insecure Internet to the corporate network using Internet protocols.

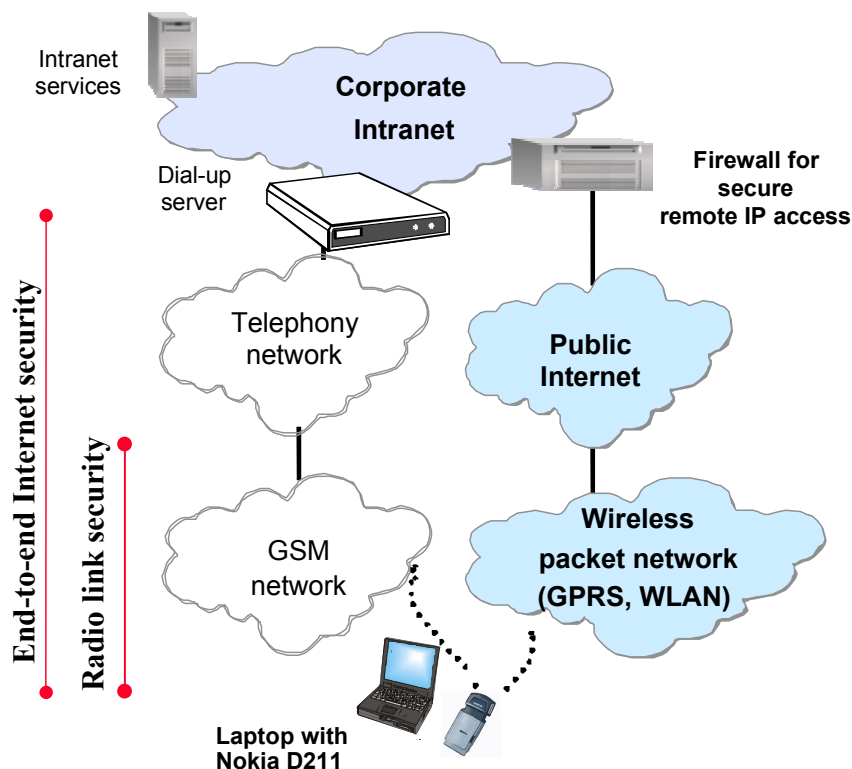
The public Internet is exposed to numerous security risks. One major security weakness is that, unlike in a point-to-point dial-up connection, Internet packets are readable to anyone

having access to the network. IP packets also tend to follow the same route, so the potential intruder most likely has an access to all IP packets. The wireless network security functions (GPRS and WLAN) alone are not enough for guaranteeing confidentiality. A highly reliable remote access system can be created by combining wireless access with an end-to-end Internet (IP) security solution.



**Note:** For secure GPRS / WLAN access, Nokia recommends using a widely adopted IP-level VPN (Virtual Private Network) security solution.

The following paragraphs illustrate how this technology can be used for GPRS access, wireless LAN office connectivity, and home connectivity.



**Figure 1: Alternative remote access mechanisms: dial-up and Internet access**

### 2.2.1 Internet security requirements

An Internet security solution should offer the following critical functions to ensure the security of data and the corporate network:

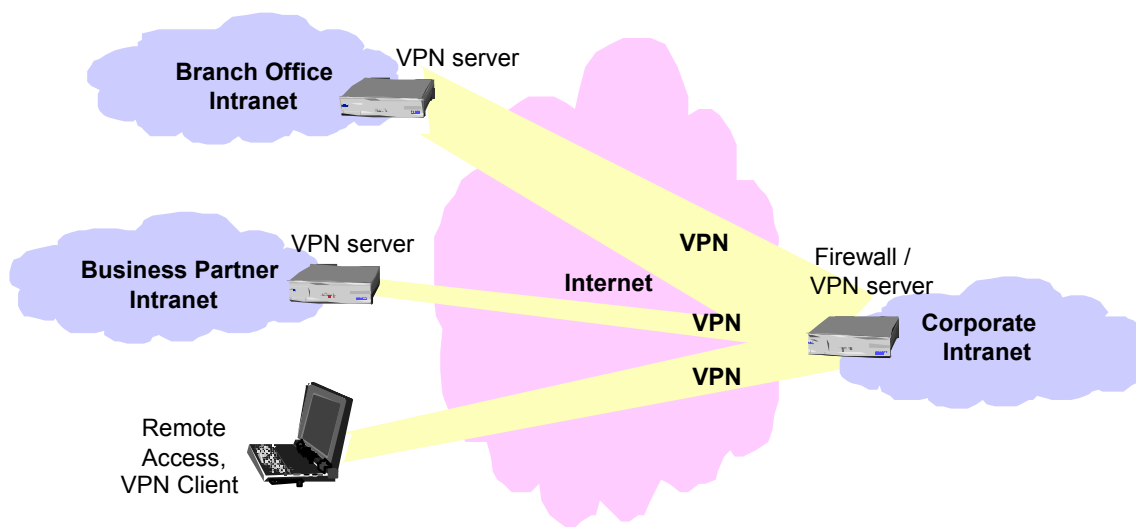
- Access control restricting unauthorised users from accessing the corporate network.
- Encryption preventing anyone from reading or copying data as it travels across the Internet. Data encryption is used to protect data from unauthorised users by encoding the content. There are many encryption methods available, which differentiate themselves mainly by their encryption algorithms.

- Authentication ensuring that the data originates from the source that it claims.

The virtual private network (VPN) technology is widely used for linking corporate LANs between sites, or external business partners to the corporate network.

### 2.2.2 Virtual Private Networking technology in brief

Figure 2 illustrates a typical VPN configuration. The same technology and platform can be used also for providing a secure remote access for GPRS and wireless LAN users.




**Figure 2: Virtual Private Network**

The VPN solution consists of a network server and client software. The VPN server protects unwanted and unauthorised communication into or out of the protected network. All traffic to the private network is forced to pass through the VPN server. A tunnel is created between the terminal and the VPN server, and the user data is authenticated, encrypted, and transmitted inside the tunnel to the host.

The advantage of the VPN is that it protects the information transmitted to and from the intranet, and that unauthorised access is prevented. VPNs do not maintain permanent links between the end points. Instead, when a connection between a terminal and the corporate network is needed, it is created and then torn down when the connection is closed. The client initiates the secure tunnel and the network authenticates the remote user. User authentication confirms the identities of all remote users. The access to the corporate network is granted only after the authentication has been completed successfully. There are various alternative authentication mechanisms, such as passwords, security tokens (stored on a smart card, for example), and certificates.

The end-to-end tunnelling protects the data transmission against security attacks. Often the VPN clients and servers also include an embedded firewall. A so-called personal firewall



filters the incoming data and allows Internet connections only from the pre-defined hosts. This prevents a hostile attacker from accessing the remote terminal.

Integrated encryption ensures that it is practically impossible for unauthorised parties to read data. Most VPN devices automatically negotiate the use of the strongest possible encryption and data-authentication algorithms between the communicating parties. The encryption is transparent for all applications, such as e-mail and Web browser, that use IP protocols. The only significant effect is that VPN encapsulation adds a little extra overhead data that has to be submitted over the wireless link.

### **2.2.3 Commercial VPN appliances**

There is a wide range of commercial VPN solutions on the market. A VPN security gateway may fit any of the following categories: high-performance VPN routers, firewalls, integrated VPN hardware, and inexpensive VPN software. Packet encryption is normally included in routers either as an add-on software or an additional circuit board. The latter is best for situations that require greater throughput. Combining tunnelling and encryption with firewalls is probably the best solution for small networks with low volumes of traffic.

In most cases the corporate IT manager selects and administrates the VPN system. The available product range is wide. The main criterion for selecting the proper solution is the requested capacity, which in practice is the number of remote access users. Typically, the VPN has to make a conversion between the corporate network and the operator network IP addressing scheme. Therefore, it is recommended to select a solution that supports network address translation (NAT) traversal.

The standardised interoperability between different VPN devices guarantees the interoperability of the VPN client and a number of VPN servers. The Nokia D211 is interoperability tested with leading VPN client and server products. A detailed list of the tested products can be found at: [www.nokia.com](http://www.nokia.com).

### **2.2.4 Personal firewall**

Personal firewall is a software with a set of rules that allows and denies network traffic through a computer. It also monitors or controls applications in order to protect them against trojans and keyloggers. Primary use is to enhance security when a VPN client is used. A personal firewall controls access into the user's PC. When your laptop is used in an insecure network, the protection level should be configured to be very high. In fact, all connection attempts to your computer should be denied. When the firewall engine detects an intrusion, it commands the software to block the hacker's IP address. Since the firewall controls transmission at the network's TCP/IP stack level, hackers cannot circumnavigate a block in the firewall. This kind of protection should always be activated, regardless of location.

## **2.3 APPLICATION LEVEL SECURITY FOR INTERNET BROWSING**

Some Internet applications, such as Web browsers, offer an additional level of security. The current Netscape and Internet Explorer applications utilise application-level security protocols, such as Transport Layer Security and SSL (Secure Socket Layer), which offer



user data protection between the client application and the server. These mechanisms are widely deployed for example in Internet banking and electronic transactions.

The application-level security ensures an additional security level, which may be used for Internet access when company confidential data is not concerned and the mobile terminal does not contain confidential information. In such cases the user may use the Nokia D211 without VPN services. However, application level security mechanisms do not protect the mobile terminal against external attacks. In addition, the level of encryption is often lower than in the VPN connection.



**Note:** With company data applications, the user should always deploy end-to-end VPN tunnelling; application-level security then offers an additional level of security on top of VPN tunnelling.

### 3. SECURE GPRS ACCESS TO CORPORATE NETWORK

---

The standard GPRS network offers over-the-air data protection but does not offer an end-to-end Internet security solution for mobile access to a corporate LAN. The GPRS network provides two security functions: *subscriber authentication* and *data encryption*. The user authentication procedures in GPRS are similar to the GSM network. All security functions are based on the secret key Ki that is stored both on the SIM (Subscriber Identification Module) card and in the operators' home location register. In GPRS, data and signalling are ciphered between the terminal and the Internet.

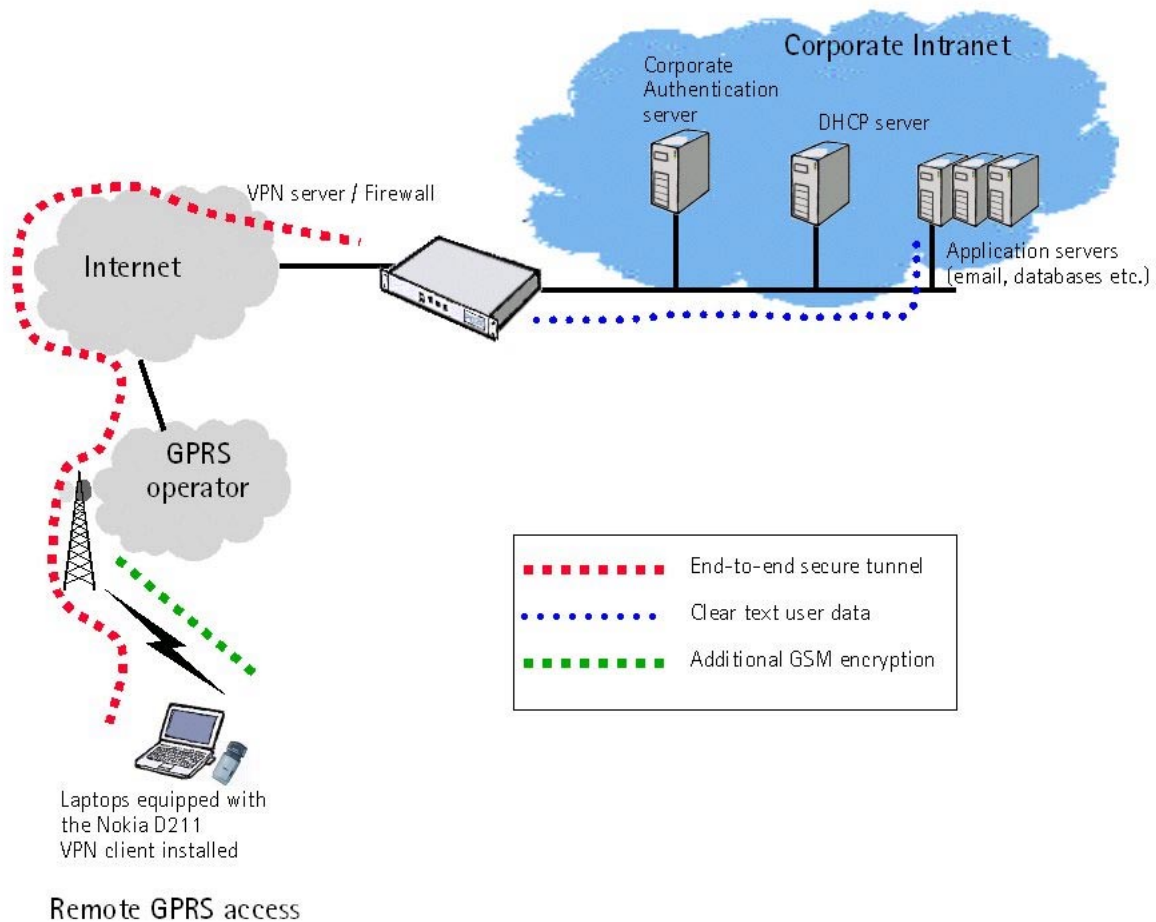


**Note:** When using a GPRS connection with the Nokia D211 for corporate connectivity, it is recommend to deploy a VPN security solution which offers end-to-end authentication and data encryption.

VPN is not necessary if GPRS is used for non-confidential applications, such as browsing the Internet. Typically, the VPN service is provided by the corporate IM or by the mobile operator. The system, depicted in Figure 3, works as follows:

1. The user activates the GPRS connection.
2. The GPRS network authenticates the mobile terminal with the SIM card and establishes a secure wireless GPRS link to the Internet (GPRS encryption).
3. The user launches the VPN client on the mobile terminal, which establishes an end-to-end encrypted IP tunnel to the company network (Internet data encryption).

The solution is extremely reliable and secure as all traffic is encrypted all the way from the mobile terminal to the corporate VPN server, and VPN offers a high level of security. The user can access the Intranet from any GPRS operator network.



**Figure 3: Secure GPRS access to corporate data**

An alternative configuration is to use a dedicated connection from the mobile operator's GPRS network to the corporate intranet and bypass the public Internet completely. In this model, the mobile terminal does not require a VPN client. The GPRS network security functions protect the data between the terminal and the GPRS core. The mobile operator then establishes a secure tunnel between the operator network and the corporate network. In this approach, the corporate customer has to trust the mobile operator, who offers the secure tunnelling. A few mobile operators offer this kind of solution for their large corporate customers. For details, contact your mobile operator.



## 4. SECURE WIRELESS LAN ACCESS

---

Wireless LAN is typically deployed in the office, home, or public access zone, such as hotels, airports, etc. With wireless LAN people can flexibly move around the office and meeting rooms, or work at home and still be in touch with the latest information in the company network. Like GPRS, wireless LAN also utilises the Internet backbone. Consequently, the same secure VPN remote access platform supports both GPRS and wireless LAN. The Nokia D211 user may select between GPRS or wireless LAN link, and then utilise the same VPN configuration for connecting to the company network.

WLAN can create a security risk, as the radio signals flow outside the office building. Security risks in a wireless LAN can be avoided by using proper authentication and encryption.



**Note:** Nokia recommends deploying an end-to-end VPN solution when accessing corporate data over the wireless LAN.

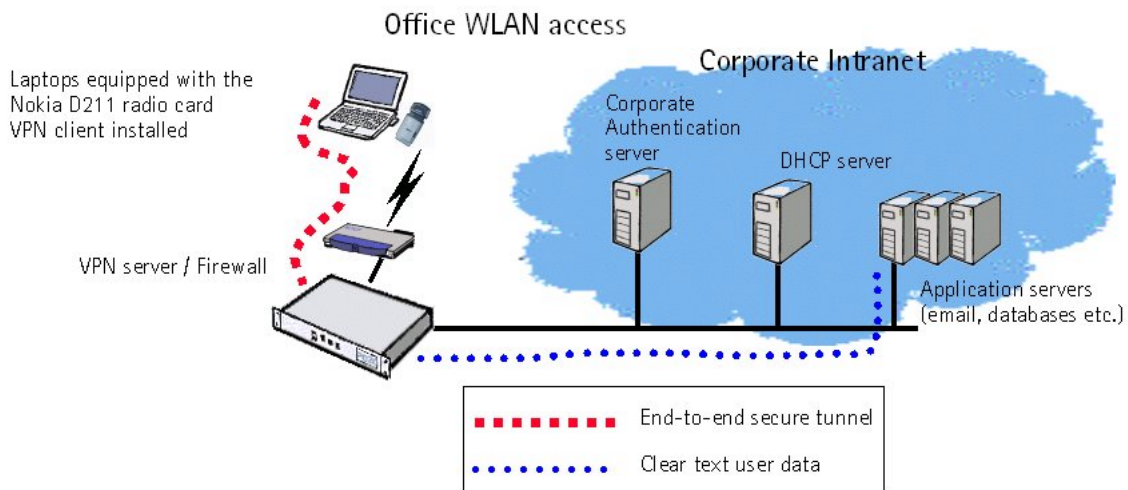
The wireless LAN (IEEE 802.11b) specification contains the Wired Equivalent Privacy (WEP) security algorithm, which can be used for authenticating the terminals in the WLAN as well as for encrypting the data on the radio link. The security level of WEP is low compared to IP security (VPN). WEP can be activated as an additional security layer, which is used for controlling the access to the wireless LAN, for example at home, but it is not the right choice for controlling access to a corporate network or protecting confidential data.

Some vendors have implemented proprietary enhancements, such as 802.1x enhancements, for WEP security and claim that these are enough for guaranteeing corporate network security. However, the security level of these non-standard solutions is significantly lower compared to an end-to-end VPN solution. The combination of a wireless LAN and properly configured VPN is highly secure and is an excellent solution for all WLAN environments.

### 4.1 WIRELESS LAN ACCESS IN THE OFFICE

The most typical place for a wireless LAN is office premises. The user may freely and easily move around the office, from the desk to the meeting room or even between two neighbouring buildings, and maintain a connection to the network all the time. Figure 4 illustrates a typical secure wireless LAN office configuration.

The wireless LAN access points are separated from the company network with a VPN server. A VPN tunnel is created between the wireless terminal and the VPN server, which protects the information transmitted to and from the intranet and prevents unauthorised access. The user may be authenticated with a password, a one-time password, such as hardware tokens, or certificates.

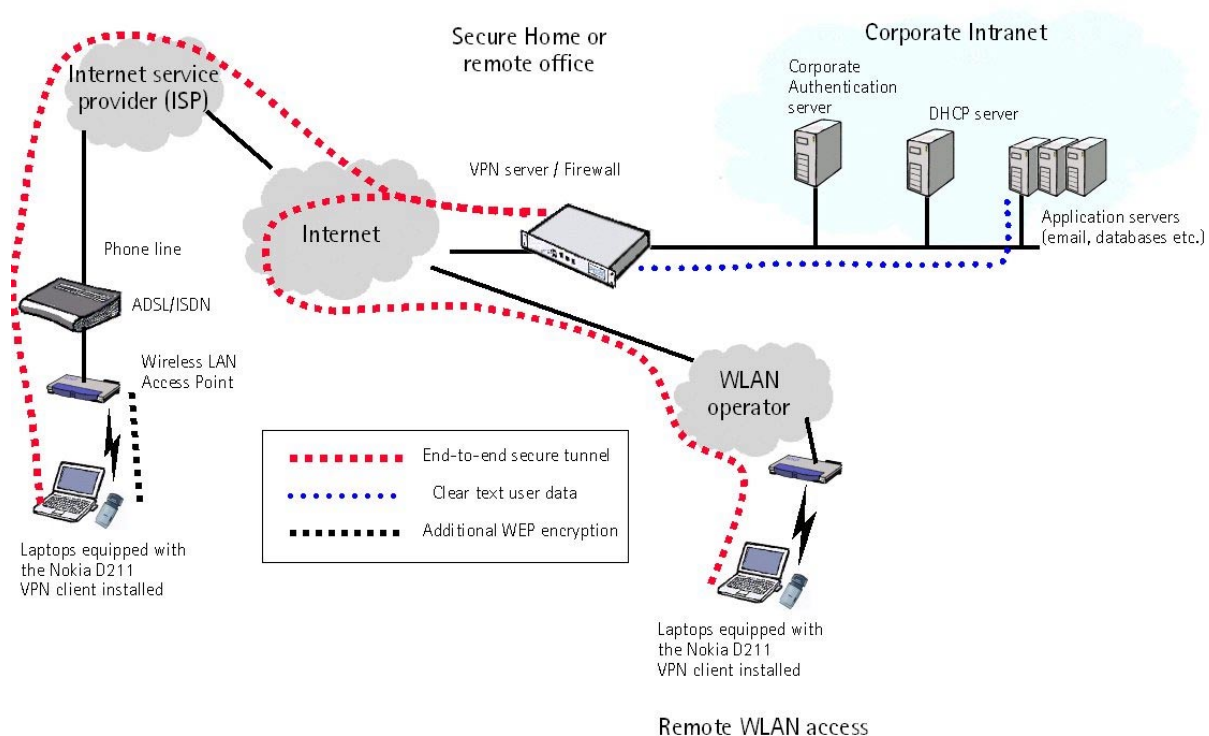


**Figure 4: Secure wireless LAN office**

## 4.2 REMOTE WIRELESS LAN ACCESS

Mobile professionals may deploy wireless LAN equipment also when out of the office. Many ISPs and mobile operators have launched public WLAN access services at airports, hotels, and other public places. In addition, people may have wireless LAN at home. The users of the Nokia D211 can have a secure remote wireless LAN connection to the corporate network from all these locations.

The architecture of a remote WLAN resembles the office WLAN. The only significant difference is that in the office the traffic is routed via a private network directly to the VPN server. In the case of a public access zone or home wireless LAN, the user data is routed via the public Internet. From the security perspective, both of these require the usage of VPN. The same terminal security configuration can be used for both remote access and office access. Figure 5 shows the remote access architecture. The Nokia D211 user is first authenticated by the public wireless LAN; then the user launches the VPN client, which automatically establishes a secure tunnel to the corporate network.



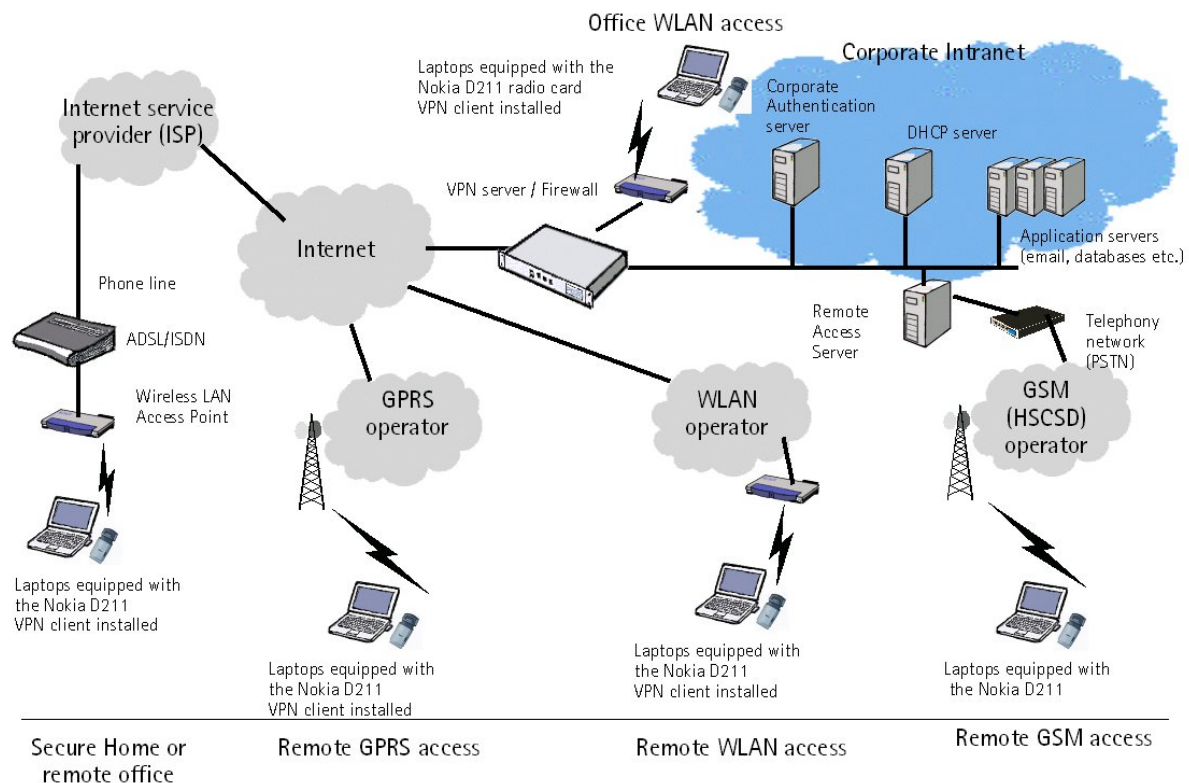
**Figure 5: Remote WLAN access**

## 5. SUMMARY – SECURE CORPORATE ACCESS WITH THE NOKIA D211

The Nokia D211 allows the user to deploy conventional dial-up networking (Figure 1). In this configuration, the VPN client is not required, but the connection is established using standard Microsoft Windows dial-up functions.

The introduced remote access architecture, depicted in Figure 6, is composed of two main parts: the VPN server and the VPN client. The VPN server extends the corporate network with Internet access and offers a secure access to the corporate network resources from all alternative wireless networks: GPRS, HSCSD, or wireless LAN. The same server offers remote access services for all kinds of remote users: home workers, GPRS roamers, public wireless LAN users, etc. This reduces administration costs and simplifies the network architecture. Typically, the company IT department administrates the VPN server.

The VPN client software is installed on the user's PC and run on top of the Nokia D211 software. The same standard client configuration is used together with both GPRS and WLAN. The client automatically establishes a secure tunnel to the company VPN server. In addition, it may offer a personal firewall, which protects the PC against attacks. The company may select the most suitable VPN client, as the Nokia D211 is compliant with leading VPN clients.



**Figure 6: Summary of the secure remote access architecture**

VPN is the correct way to build a secure, private communication infrastructure on top of the Internet. There are a number of benefits with using Internet connectivity, GPRS, and WLAN whenever available:

- Rather than having the user making long distance phone calls to dial the company directly, the GPRS and wireless LAN allow the user to utilise the public Internet connection.
- Typically the charging in WLAN and GPRS is based on the data volume transmitted, not on the connection time. Thus, e-mail and browsing may be significantly cheaper over this kind of connection.
- With VPN, the companies get rid of their modem pools, expensive leased lines, and remote-access servers.
- Further savings come from reducing the operational costs associated with supporting remote users.

The Nokia D211 multimode radio card sets a new reference for PC connectivity offering both dial-up as well as GPRS and WLAN connectivity in a single device. The security aspects have been considered in the product design. The Nokia D211 is interoperability tested in depicted reference designs with leading VPN client manufacturers' software and with Microsoft's embedded Internet security (IPSEC) solutions. Detailed information of the security issues can be found at [www.nokia.com](http://www.nokia.com).