

White Paper:

The Evolution of VPN  
and its Implications for Mobile Phone Security

---

April 2003



## Introduction

This white paper describes how Virtual Private Networking (VPN) technology is evolving for use in mobile phones. Mobile VPNs enable enterprises to extend their network to mobile employees, partners, and customers without the risk of compromising their existing security standards. This white paper highlights drivers for mobile security, specifically mobile IPSec VPNs, and discusses some implementations.

## VPNs, Including Mobile VPNs, Defined

Traditionally, Virtual Private Networking (VPN) is discussed in the context of creating a private network using the infrastructure of the public Internet. The public Internet was specifically designed to quickly route traffic between any two connected points to solve the scalability problems encountered when using site-to-site links to connect networks. The Internet is composed of countless network devices that are administered by different organizations. No one organization can control or be responsible for the privacy and integrity of data as it travels over the Internet. The Internet is sometimes viewed as an insecure means of transmitting data because there are opportunities for modification and deletion of data. A variety of well publicized attacks and viruses have made it painfully obvious that the Internet is insecure.

A VPN can take advantage of the strengths of the Internet infrastructure because it provides encryption and authentication features to address the lack of security on the Internet. VPNs can be built on tunneling protocols that are implemented at different layers of the OSI seven-layer model. Tunnel characteristics are determined by the protocol the tunnel is built upon. Tunnels can be established at the following layers of the OSI model:

- Layer 2, the Data Link layer, uses L2TP and PPTP tunneling protocols. These protocols use password authentication to prevent unauthorized dial-up connections.
- Layer 3, the Network layer, uses IPSec tunneling protocol built over IP. This protocol authenticates and encrypts data transmission by adding network layer information to each packet.

IPSec (Internet Protocol Security) was developed as a standard by the IETF to address the authentication and encryption limitations of the Layer 2 tunneling protocols. IPSec provides message integrity, privacy, authentication, and replay protection. An IPSec tunnel can be created between two IPSec gateways or between an IPSec gateway and a remote user who has an IPSec VPN client installed.

A mobile VPN client extends the VPN concept to mobile employees, partners, and customers who instead of laptops now carry pocket-sized devices. These devices combine a cellular phone with a small computer that can work with common office applications such as email. Mobile users establish an IPSec VPN tunnel from mobile phones to an IPSec gateway over the Internet using wireless connection such as Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), or wireless LAN (WLAN). This wireless VPN tunnel gives mobile users secure, reliable access to an enterprise.

## Drivers for Mobile VPN

Mobile VPN technology enables mobile users to connect to secured services. Today, the need for mobile VPN comes mainly from the corporate world where the number of mobile employees as well as partners and customers who need access to the enterprise is increasing. The business advantages that are gained from mobility continue to grow in concept and practice, which is changing the enterprise landscape. Ultimately, the availability of mobile devices that are data-enabled coupled with development of 2.5 and 3G networks will drive requirements for secure connections to enterprises.

## Mobile Phone Market

The evolution of technology is responding to user demand to have mobile phones that can be used for business. The demand for mobile business phones is increasing, thus giving way to increased shipments around the world. With the exception of Palm OS and Windows CE based phones, most shipping models are built around the Crystal-reference design of Symbian OS. Symbian OS is a driving force behind the mobile phone momentum, which will grow stronger as 2.5-generation (2.5G) and third-generation (3G) wireless networks and services begin to emerge. Nokia and Sony-Ericsson have already announced several new smart phone models based on Symbian OS and other manufacturers (Siemens, Motorola, Samsung) are following.

In the short term, the smart phone market is driven by major OS manufacturers, such as Symbian, Microsoft, and Palm giving strong support to development of these platforms. In addition, hardware manufacturers like Nokia, Ericsson, Motorola, and Siemens are committed to ensure a wide range of product offerings. Mobile phones for business use will continue to gain popularity as the wireless technology evolves toward more mature networks and wider coverage areas. At the same time, the usage of Internet and demand for wireless connectivity to enterprise resources, including email and data applications like Customer Relationship Management (CRM) and Employee Resources Planning (ERP), will increase.

## Mobile Connectivity

The latest developments in mobile network technology have enabled mobile devices to connect to the Internet. Deployment of next-generation mobile networks creates a true revolution in the Wireless WAN (wide area network) era, enabling full connectivity for mobile users. Today, existing wireless technologies such as GSM HSCSD (Global System for Mobile Communications using High Speed Circuit Switched Data), GPRS (General Packet Radio Service), and CDMA (Code Division Multiple Access) IS-95B, allow mobile users to access the Internet via a reliable and relatively fast 40kpbs wireless link.

## Mobilizing the Enterprise

Mobile phones are fast becoming a centerpiece of business. Email has become the foremost communication in the enterprise, surpassing voicemail in importance. In addition, the number of daily tasks employees are expected to perform is trending upward while the time allotted per task is trending downward. While mobile users' method and device used for connectivity may range from wired to true wireless, the content being accessed and the infrastructure where it resides are still very much wired and IP-based. The same security applied in the wired IP world is required for secure communications via mobile communications with some additional protocol support, traffic and service awareness, and security vulnerability preparedness. An IPSec VPN is a perfect solution to address this enterprise-level security challenge. An IPSec VPN provides a scalable, flexible enterprise-level security infrastructure on top of which they can build and extend their mobile applications and services.

## Uses of Virtual Private Networks

A VPN is a way to build a secure, private communication infrastructure on top of a public network. VPNs are logical networks that connect physical networks or single hosts to each other by forming encrypted tunnels over public networks. VPNs guarantee privacy and security, allowing companies to communicate information—no matter how sensitive it is—over the Internet inexpensively.

VPNs allow companies to communicate with their branch offices, customers, partners, employees, and suppliers securely. Through VPNs, the Internet has become a means of providing more cost effective access to business critical information virtually from anywhere. IKE (Internet Key Exchange) and IPSec (Internet Security Protocol) are standardized protocols that negotiate secure communications between two IPSec devices, for example two gateways or a gateway and a wireless terminal. VPNs address the following issues in Internet security during IKE and IPSec operations:

- **Message integrity:** Message integrity means that the recipient is assured that what they receive is exactly what the sender transmitted. The messages are protected against any undetected alterations during the transmission using HMAC SHA-1 or MD5. Message integrity is achieved by digitally signing the messages. If there are any changes to data, they are detected immediately.
- **Privacy:** Privacy prevents unauthorized network users to eavesdrop on data sent to and from the network by encrypting it, thereby assuring confidentiality to authorized users.
- **Authentication:** So that each party can be sure of whom they are communicating with, authentication identifies the parties exchanging information. Common methods of authentication include digital certificates, shared secrets in the form of usernames and passwords, and tokens.
- **Replay protection:** Replay protection ensures that transmitted data cannot be captured and replayed at another time.

There are several variants on how VPNs can be used. The sections below describe some basic VPN implementations used by corporations.

### Site-to-Site VPNs

Site-to-site VPNs often replace leased lines connecting corporate office networks. These VPNs provide the same or better level of security, but are usually faster to set up, more flexible to use and cost less.

The IPSec protocol has two main sub-protocols: 1) AH (authentication header); and 2) ESP (encapsulated security protocol). During IKE negotiation, the two IPSec devices determine how they are going to communicate. If IPSec AH is used, the two devices will choose an authentication method (for example, MD5 or SHA-1). If IPSec ESP is used, the two devices will choose both an authentication method and encryption algorithm (for example, DES or 3DES). IPSec ESP is more often implemented as a tunnel between two IPSec gateways or between an IPSec gateway and an IPSec client because it provides authentication and encryption.

Consider this example: A person at the branch office behind gateway 1 wants to send data to a person at the corporate headquarters behind gateway 2. The following steps would occur to establish and build an IPSec tunnel:

1. A person at the branch office attempts to send data to a person at corporate headquarters. The data are routed through gateway 1.
2. Gateway 1 reviews its security policy and determines that an IPSec tunnel is required between gateway 1 and gateway 2 to protect traffic as it travels over the Internet.
3. Gateway 1 contacts gateway 2 and says "let's do IKE" if an IKE SA does not already exist between them.
4. Gateway 1 and gateway 2 establish an IKE tunnel so they have a safe channel for discussing how data is going to be transmitted between them. During this time, they exchange keys as well as negotiate protocols and algorithms.
5. Once an IKE SA is set up, they use it to create a new IPSec SA. This IPSec SA is the tunnel that protects all data as they travel between the person at the branch office and the person at corporate headquarters.

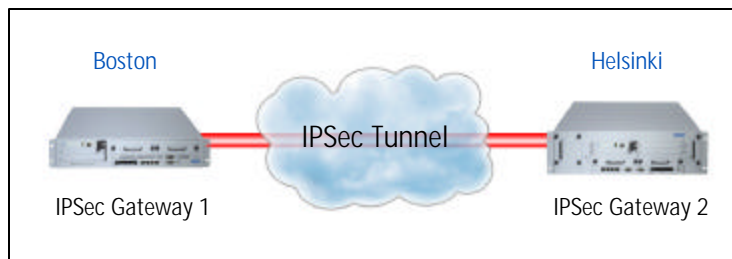


Figure 1

Figure 1 illustrates how a corporation can connect a remote office (Boston) located anywhere in the world with an Internet access to their headquarters (Helsinki). The Internet is used as transport media and an IPSec VPN solution (two VPN gateways) is applied to provide the necessary security solution over the public network.

### Remote Access VPNs

A remote access VPN extends the VPN functionality to cover remote workers who are usually equipped with a laptop computer and an Internet connection while they are out of the office. IPSec is becoming the protocol of choice for establishing tunnels to send data since it provides message integrity, authentication, encryption, and replay protection. Furthermore, protocols like CRACK (challenge response authentication for cryptographic keys) have been developed recently to allow common legacy user authentication methods like passwords and SecurID cards to be used with IPSec tunnels. Protocols have also been developed to allow remote users to be assigned an internal IP address when using IPSec protocol.

Organizations can maintain their own remote access servers and allow direct dial-up connections, but this many require too much equipment and administrative overhead. Often, organizations rely on Internet service providers (ISPs) to manage dial-up connections and to route traffic over the Internet. A number of strategies are possible for using an ISP to manage remote access, including IPSec remote access and L2TP with IPSec.

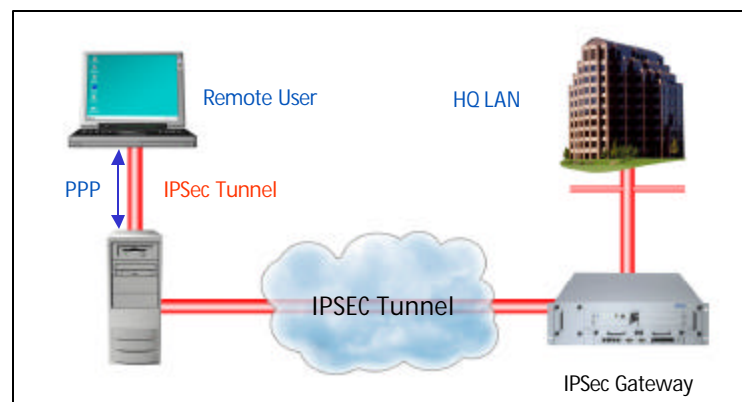


Figure 2

Managing remote access with pure IPsec requires that each remote client have IPsec client software installed on their machine and a security policy for it. In this case, IPsec by itself is a secure method of establishing remote access to a VPN. Data is encrypted by the IPsec client before being transmitted over the public telecommunications network. The IPsec gateway resides at the edge of the enterprise network. It decodes encrypted traffic before forwarding it to the organization's internal network, and encrypts traffic before forwarding it from the internal network to the Internet. (This is shown in Figure 2.)

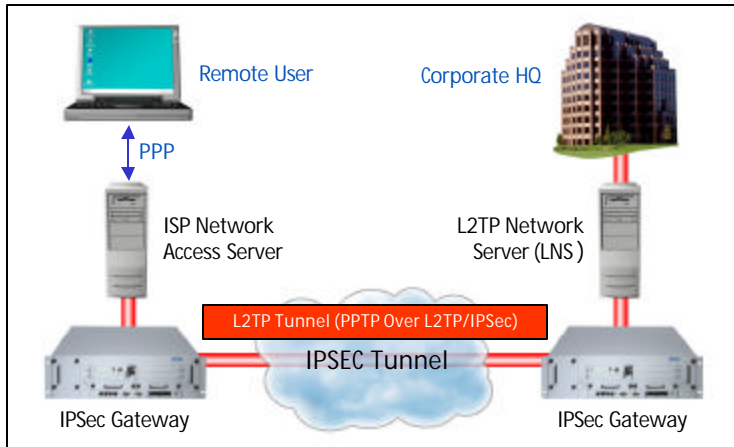


Figure 3

L2TP is often used for remote access. L2TP lacks encryption over the Internet, and for this reason is not recommended without combining it with some other form of protection such as IPsec. IPsec can be implemented, for instance, using L2TP with an IPsec gateway at the ISP or with an IPsec remote client. If L2TP is implemented with a gateway at the ISP, this gateway establishes an IPsec SA over the Internet to the enterprise IPsec gateway. The remote client simply establishes a normal PPP connection without requiring any special software or configuration. This arrangement protects data in transit over the public Internet. However, it does not protect the dial-up line to the ISP. (This is shown in Figure 3.)

To protect the dial-up line, an IPsec client must be installed on the remote client. In this scenario, the ISP does not require any special equipment and data is encrypted all the way from the client machine to the gateway at the corporate network. (This is shown in Figure 4.)

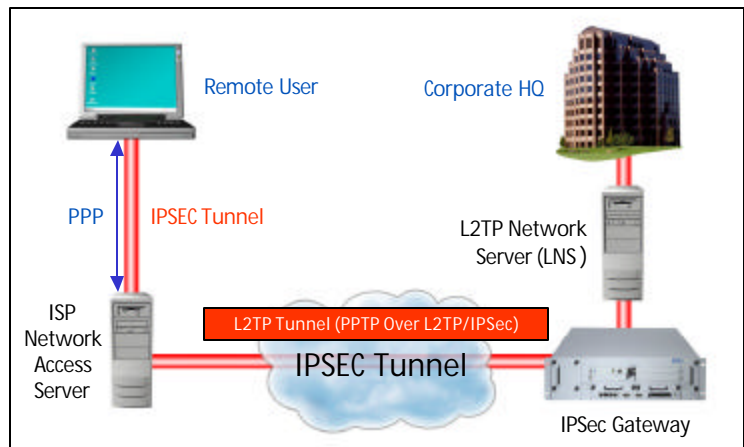


Figure 4

**Mobile VPNs**

While mobile VPN is conceptually similar to a remote access VPN, the mobility of the remote device, diversity of the underlying network infrastructure, and resource availability of the mobile phones introduce many challenges to the VPN solution. In this case, the remote user is a mobile user who can access enterprise network from either outside or inside the corporate premises using a wireless connection. The laptop computer is replaced with a mobile phone that has VPN client software installed on it.

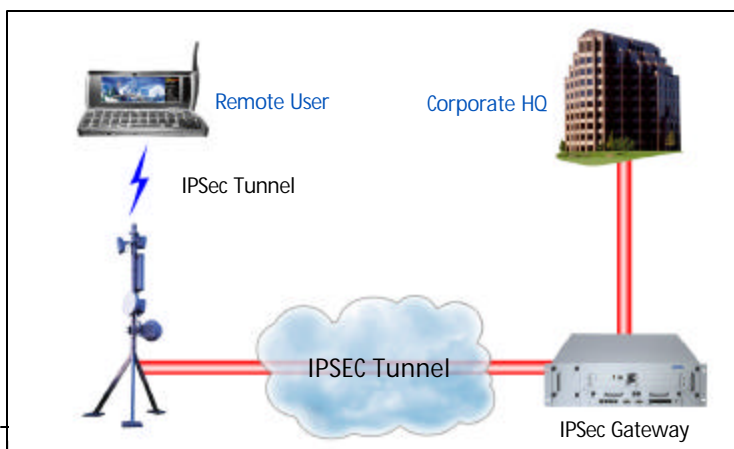


Figure 5

In both mobile and remote access VPNs, users are allowed virtual connections to the corporate network. Mobile users access the same corporate network as they would if they were on-site connecting to the local area network (LAN). To attain this kind of transparency, the network parameters (internal network address, DNS, and WINS information) are negotiated with the remote clients. The mobile user initiates an IPsec VPN connection to the corporate gateway. After successful authentication, the mobile user is

granted access to the corporate network and provided security in the same way as the laptop user of a remote access VPN.

## Implementing Mobile VPNs: Considerations

There are unique characteristics of mobility that should be taken into consideration when implementing mobile VPNs. Some of them are described in the sections below.

### **Characteristics of Mobile Networks**

Mobile networks create some technical issues that need to be addressed when planning mobile solutions. Mobile networks today, although fast, do have some delay and speed issues that can lead to timeout problems if applications are not prepared to accept long delays (for example, authentication).

The sporadic occurrence and nomadic nature of connections from mobile phones makes managing security on them challenging. When a mobile user establishes a secure connection to the enterprise, the management backend needs to make the required checks upon the validity of the security profiles. This should be done prior to each connection and without the mobile user noticing a substantial delay in the connection establishment phase. In addition, a private address must be issued to mobile devices and NAT (Network Address Translation) must be used before forwarding IP packets to the public networks.

### **Inherent Properties of Mobile Handheld Devices**

- Limited Memory and Resources

Mobile phones have less available memory than personal computers. Phones typically come standard with 4-16MB of available memory for applications and more "business-enabled" phones with 8-64MB. The amount of upgradeable and standard memory is constantly increasing, however, the number of applications and feature requirements for these phones is increasing too.

- Processing Power

Typical mobile phones are powered by a CPU, which provides only a fraction of the computing power compared to a typical desktop PC (206Mhz ARM vs. 2Ghz Pentium IV). This means that the computation intensive tasks like key material generation and encryption take more time on a phone than on a desktop computer. With slow connection speeds (below 100kbps), encryption is not so much an issue. However, generating long keys (>1024bit) from equally strong key material can take several seconds.

- Limited Battery Power

Mobile phones are usually powered by a chargeable battery, which lasts from hours to days in normal usage. Because VPNs usually require heavy computation to do the necessary encryption, they keep the phone's CPU busy and hence require more power.

- Phone Security

Phone security is a critical component in an enterprise solution. VPNs allow sensitive data to be exchanged between the phone and enterprise, which usually means that some of that data is stored to the phone itself. Therefore, technologies like file encryption and terminal lock-up should be in place when sensitive data is stored to a mobile device.

### **Number of Mobile Users**

In the mobile world, the sheer number of clients can create problems for the existing infrastructure. The number of client set requirements for the number of concurrent connections (or tunnels) that the gateway must be able to handle as well as the number of users the gateway must be able to authenticate simultaneously. The amount of

concurrent connections and simultaneous authentication requests must be estimated. Then, gateway equipment that can handle the required load should be implemented in the network infrastructure.

### **Deploying Mobile Clients**

Mobile VPN Client configurations (or policies), certificates, and private/public key pairs need to be configured centrally by network or security managers. Mobility presents a special challenge during the deployment of this information to the clients, especially during the initial deployment of the client software and policies.

Additionally, mobile clients are always connected through an unsecured or hostile network (wireless), requiring secure deployment of software and policies. The initial trust relationship between the intranet and the mobile handheld device has to be established prior to downloading VPN related trust, such as certificates, to the handheld device.

Nokia has developed the Nokia Security Service Manager (SSM), a product to address the needs of secure deployment. With Nokia SSM the administrators can do the initial provision wirelessly (maintaining strong security) and automating the updates to client policies and settings.

### **Nokia Mobile VPN Technology**

Nokia provides end-to-end mobile security solutions for the wireless world. Nokia Mobile VPN Client is based on the IPSec protocol and supports the relevant IETF standards, drafts, and RFC's (e.g. RFC2401-2410). By adhering to these standards and open architecture, Nokia can truly enable the creation of new services on top of a secure platform infrastructure. The sections below describe how Nokia is implementing mobile VPN technology.

### **Mobile Phones: The Operating System**

Nokia Mobile VPN Client is designed for phones running the Symbian Operating System (Symbian OS), formerly also known as EPOC. Nokia is one of the founding members of Symbian, which strives to integrate the power of computing with telephony, bringing advanced data services—using voice, messaging and on-board processing power—to the mass market.

Symbian OS addresses the issues of limited memory and low power consumption at the operating system level. In addition, Symbian OS provides necessary components for building an enterprise level application platform with support for secure computing. The Nokia Mobile VPN Client is tightly integrated with the operating system itself using as much of the available OS components as possible thus helping to reduce the overall overhead and enhance the user experience.

### **VPN Policy: Encryption and Authentication Support**

Nokia Mobile VPN Client supports multiple encryption and public key algorithms as well as several key-management protocols including support for industry standard IKE (Internet Key Exchange), also referred to as ISAKMP/Oakley protocols. Nokia VPN Clients can automatically negotiate the strongest possible encryption and data authentication algorithms available between the communicating parties. This includes both DES and Triple DES (3DES) for data encryption and SHA-1 and MD5 for data authentication. In addition, encryption keys are updated frequently, ensuring maximum security.

In large-scale VPN deployments, automated key management is necessary to reduce the number of encryption keys to a manageable level. Rather than issuing a unique encryption key for each pair of VPN connections, Public Key Infrastructure (PKI) generates a public/private key pair for each individual user. One key is publicly known and the other key is private. The private key is accessible to its owner only. To keep the private key secret it is best to generate the public/private key pair in the mobile terminal itself and have the public key certified by a Certificate Authority (CA). This way the private key never leaves the terminal, which increases the overall security and takes much of the key-generation load away from servers thus helping the scalability of mobile solution.

Technically, the key pair is mathematically generated so that whatever you encrypt by using the private key can be decrypted by using the respective public key, and vice versa. PKI is then used to verify the identity of the communicating parties and create the necessary encryption keys for each session. The beauty of PKI is its scalability and manageability—you do not have to distribute the secret encryption keys between all the communicating parties. Instead, you distribute a digital certificate.

PKI relies on digital certificates to certify the generated private/public keys. Each certificate carries information about a particular VPN user, including that user's public key, which is used to verify the user's identity and to calculate the keys for actual encryption. Nokia VPN solutions support open, scalable PKI utilizing X.509 digital certificates and CA technology. Several CA vendors can be utilized as a trusted CA including Verisign, Baltimore, and Entrust.

In addition to PKI authentication, Nokia supports legacy authentication methods such as shared secrets, one-time passwords, and tokens. Thus, corporations can utilize the existing infrastructure (for instance, SecurID cards and RADIUS servers) to handle user authentication. To help corporations migrate from legacy authentication to PKI, they can use Nokia Security Service Manager to handle the migration. Mobile users can authenticate to it using a SecurID card, for example, and get a digital certificate from a CA (internal to Nokia SSM or from an external CA). Once users have digital certificates, they can start using them for VPN connection authentication.

### **Deploying Mobile VPNs**

Nokia provides a single point of management for mobile VPN infrastructure. In the future, it will be possible to integrate this function as a part of the phone security enforcement to create a flexible management and deployment solution, which is protected by a corporate level security solution. By providing this level of integration, Nokia truly enables enterprises to mobilize their business critical applications and services while maintaining the same level of security or improving it. Nokia Security Service Manager can handle the initial deployment and automate the future updates to mobile VPN client configurations. Automated policy deployment is essential for large-scale deployment where all the users need to be updated with the latest security settings.

### **Internal Addressing and NAT**

Internal addressing is a technique where the mobile phone is granted a corporate LAN internal address and access to DNS services. Without internal addressing, phones could not utilize the corporate internal DNS naming convention (intranet) and corporate firewalls might deny the access to some corporate servers. With internal addressing, mobile users are virtually part of the corporate network. Nokia has also implemented support for Network Address Translation (NAT) so that the existence of public network NAT services can be automatically detected and IP packets can be encapsulated in UDP packets to bypass the NAT service.

### **Reliable, Scalable VPN Connections to Enterprise Networks**

Extending an enterprise network to mobile phones requires an infrastructure (network, gateways, management, tools) that can handle the management and support of massive numbers of new devices. Nokia provides a mobile VPN infrastructure on which enterprises can base their core services.

The Nokia Mobile VPN solution includes patented IP clustering technology to ensure unprecedented reliability, scalability, and availability. It allows several devices to act as a single network entity, sharing a single external IP address and a single internal IP address. This single entity is called a gateway. A gateway can be made up of a single node or multiple nodes, often referred to as a cluster of nodes. To handle an increasing number of mobile concurrent users, new nodes can be added to the gateway cluster. As additional nodes are added to the gateway, the load is automatically balanced to include the new nodes with no impact on current nodes. To ensure VPN service in the case of node failure, all session state information, including IPSec information, is maintained and flow processing is seamlessly migrated to other nodes. Thus, IPSec security associations can actually move from one node to another node in a manner completely transparent to the other endpoint of the session. The result is no disruption in service for the end user, which is especially important for mobile users.

## **Mobile User Experience**

The ultimate success of deploying mobile solutions depends on how end users adopt and accept mobile phones and security on them. Mobile phones present a special challenge in usability since the screen size and input methods are limited by the size of the phones. Nokia provides an intuitive user interface for its mobile phones by providing minimal need for user intervention and tight integration to the operating system. Continuing in this vein, Nokia hid the complex technology involved in mobile VPNs. Few steps are required to use the mobile VPN application on Symbian devices, thus supporting a seamless security experience with access to corporate resources. One key area in hiding the complexity is to make sure that end users do not need to create complex configurations and that mobile phones can be administered over the air.

## Future Issues

### **Multiple Identity**

Mobile phones especially differ from other mobile devices (PC's and laptops) with respect to personal usage. At the same time as a mobile worker is accessing corporate data securely, the phone is also their personal communication device. This means that personal and corporate data are accessed at the same time (VPN connection and phone call to a friend) which presents yet another challenge for security. Phone, operating system and applications must have support for this kind of multi-identity scenario and still support the level of security that enterprises require from mobile phones. Addressing this issue will decide how fluently mobile phones support end user behavior and are accepted as both personal and corporate business tools.

### **Complete Security Package**

Mobile VPN is only one part in a corporate security package. Personal firewall, anti-virus, and local data encryption are must-have components so that enterprises can be sure that data is secured. Management will play an important role in ensuring that all mobile users have up to date configurations. In addition, mobile phones mean that all configurations must be delivered securely over wireless networks. To provide the best possible user experience all these configurations should be provided automatically through similar if not identical user interface. At the same time, a single security interface will help save phone resources.

### **Always Connected**

Future mobile phones will support multiple network interfaces depending on user location or preferences (GSM, GPRS, UMTS, WLAN). An example of this would be a mobile worker using GPRS outside the office and a WLAN inside the office. A mobile VPN solution must be able to adapt to network changes and maintain a secure connection even if the underlying network changes. This will provide users a true mobile environment and an always connected experience.

## Nokia Internet Communications

Nokia Internet Communications, headquartered in Mountain View, California, provides world-class Network Security, Virtual Private Network and Internet Traffic and Content Management solutions that ensure the security and reliability of corporate enterprise and managed service provider networks. Nokia is committed to enhancing the end user experience by bringing a new level of security and reliability to the network, enabling an Internet transaction that is personal and trusted-each and every time.

For more information, please visit [www.nokia.com](http://www.nokia.com) and click on Secure Network Solutions. Nokia Internet security and virtual private network appliances span the spectrum of price/performance points, and secure the widest range of network environments-from the smallest branch office to the largest Internet data center. The expansive product line, backed by world-class global support and services, provides customers the ability to deploy multiple solutions from a single product to secure all elements of a distributed enterprise.

## Nokia

Nokia is the world leader in mobile communications. Backed by its experience, innovation, user-friendliness and secure solutions, the company has become the leading supplier of mobile phones and a leading supplier of mobile, fixed broadband and IP networks. By adding mobility to the Internet Nokia creates new opportunities for companies and further enriches the daily lives of people. Nokia is a broadly held company with listings on six major exchanges.

### **Nokia Internet Communications Americas**

313 Fairchild Drive, Mountain View, CA 94043

Tel: 1 877 997 9199

E-mail: [ipsecurity.na@nokia.com](mailto:ipsecurity.na@nokia.com)

### **Europe, Middle East and Africa**

Nokia House, Summit Avenue

Southwood, Hampshire, GU14 ONG, UK

Tel UK: +44 161 601 8908

Tel France: +33 170 708 166

Email: [ipsecurity.emea@nokia.com](mailto:ipsecurity.emea@nokia.com)

### **Asia Pacific**

438B Alexandra Road

#07-00 Alexandra Technopark, Singapore 119968

Tel: +65 6588 3364

E-mail: [ipsecurity.apac@nokia.com](mailto:ipsecurity.apac@nokia.com)

[www.nokia.com](http://www.nokia.com)



Copyright © 2003 Nokia. All rights reserved. Nokia and Nokia Connecting People are registered trademarks of Nokia Corporation. Other trademarks mentioned are the property of their respective owners. Nokia operates a policy of continuous development. Therefore we reserve 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 direct, special, incidental, consequential or indirect damages howsoever caused.