White Paper

The Evolution of Mobile VPN and its Implications for Security

June 2005

NOKIA
CONNECTING PEOPLE

Table of Contents

1 Introduction

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

2 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 and IPSec gateway and a remote user who has an IPSec VPN client installed.

A Mobile VPN extends the VPN concept to mobile workers 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 e-mail, word processing, and presentations. Mobile workers establish an IPSec VPN tunnel from their handheld device (smart phone or PDA) 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 allows mobile users to access their enterprise intranet along with applications such as e-mail securely.

3 Drivers for Mobile VPN

Mobile VPN technology enables mobile users to create secure, transparent connections to secured services. Today, the need for Mobile VPN comes mainly from the enterprise world where the number of mobile workers is constantly increasing. Businesses are taking steps to ensure that employees have access to enterprise data via handheld devices while out of office range. It is becoming less and less acceptable to be unable to access enterprise resources while traveling away from the office. Anytime, anywhere connections continue to grow in concept and practice, which is changing the workforce landscape. Ultimately, the availability of handheld devices that are data-enabled coupled with development of 2.5, 3G and WLAN networks will drive requirements for secure connections back to enterprise networks.

Two of the most common applications are a mobile worker accessing their enterprise network to retrieve their e-mail and getting information from the intranet. This type of access gives any employee a tool to respond in a timelier manner to either urgent or routine business. Additionally, there are a growing number of mobile employees, especially sales people, data collectors, and field service workers, who need access to applications away from the office. For example, if data is entered electronically in the field, it can be fed back to central databases. One of the results is better tracking of worldwide operations, which is an important gauge in determining how different regions are performing. In addition, sending data, whether it is instructions or orders, allows companies to fulfill customer requirements more readily. Finally, mobile workers used to record data on paper and later entered it in the office or on a laptop from a remote location. Now, they can enter it once in the field and send it to a database, which avoids re-entry of information thereby decreasing both workload and errors.

3.1 Mobile Handheld Market

The evolution of technology is responding to user demand for having a handheld wireless device that can operate as both a mobile phone and computer. The demand for smart phones is increasing, thus giving way to increased shipments around the world. With the exception of Palm OS and Windows CE based smart phones, most shipping models are built around Symbian OS. Symbian OS is a driving force behind the smart phone momentum, which will grow stronger as 2.5-generation (2.5G) and third-generation (3G) wireless networks and services begin to emerge. There are currently 41 different Symbian based mobile devices from 8 different manufacturers on the market. According to Symbian (www.symbian.com) 14.4 million Symbian OS based phones were sold in 2004.

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 devices 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 e-mail and data applications, will increase.

3.2 Wireless Connectivity

The latest developments in wireless network technology have enabled wireless handheld devices to have fast connections (>100kbps) to the Internet. The deployment of third generation (3G and WLAN) 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. The third and fourth generation of mobile networks and WLAN allow mobile users to benefit from ever increasing service opportunities which are enabled by evolving networking technologies and increased bandwidth (Figure 1).

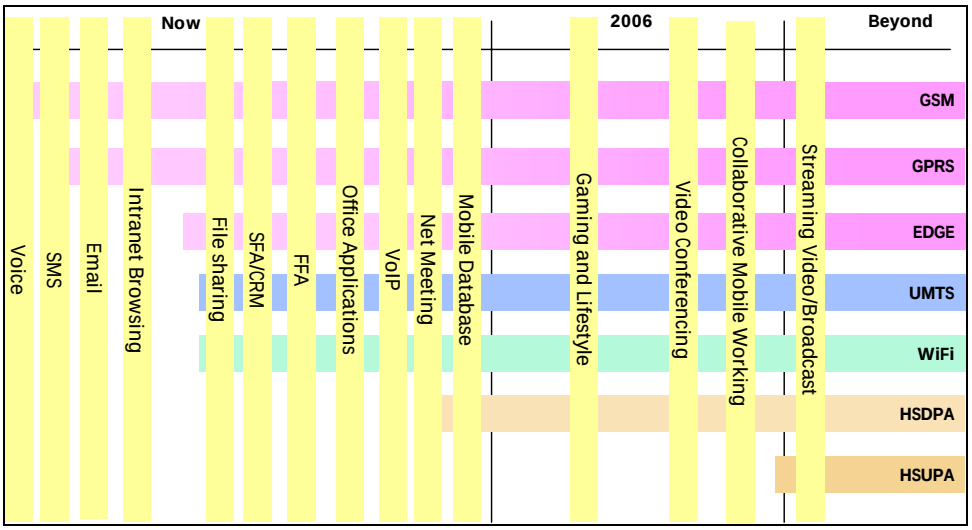

Figure 1: Service offerings increase as network technologies evolve

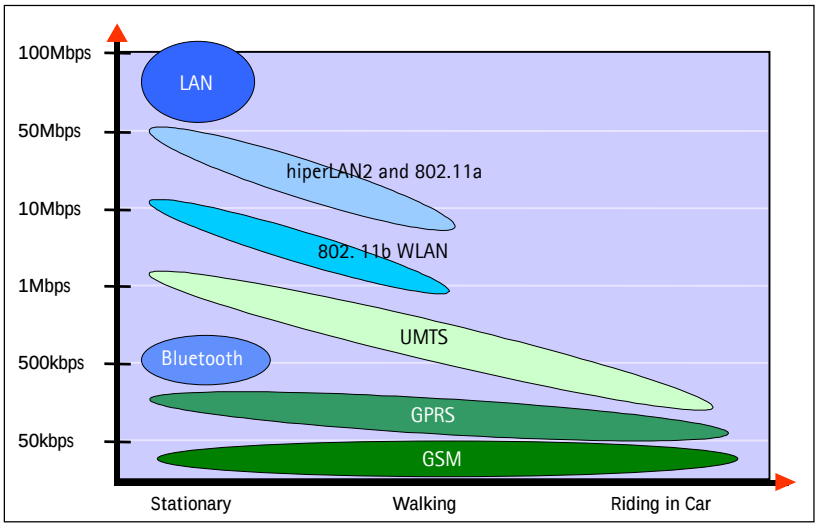

Figure 2: Transmission speeds changes for mobile user

Figure 2 depicts wireless technologies and their respective bandwidths. It also illustrates how transmission speed depends on the rate at which a mobile user is traveling—a common issue in mobile communications. The connection speed decreases as the mobile user's speed increases because of timing issues between the moving user and the base station. The higher the connection speed, the more sensitive it is to timing. Many wireless protocols can detect these timing errors and decrease the transmission speed in order to maintain the connection.

3.3 Mobilizing Enterprise Employees

Mobile handheld devices are fast becoming a centerpiece of business. Enterprise e-mail systems have become the foremost communication system 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 the enterprise end user's 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 and wireless communications with some additional protocol support, traffic and service awareness, and security vulnerability preparedness.

Extending the enterprise networks to cover wireless networks creates an obvious security risk: A wireless network is considered a hostile network. It should be treated as the Internet—anybody can access it. When a corporation decides to use the Internet over private lines and implement fixed VPNs to protect connections, the connections from the wireless world to the protected enterprise network must be protected too. 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 enterprises can build and extend their mobile applications and services.

4 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 device. 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 enterprises.

4.1 Site-to-Site VPNs

Site-to-site VPNs often replace leased lines connecting enterprise office networks. These VPNs provide the same or better level of security, but are usually faster to set up and 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, 3DES or AES). 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 enterprise 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 enterprise 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 enterprise headquarters.

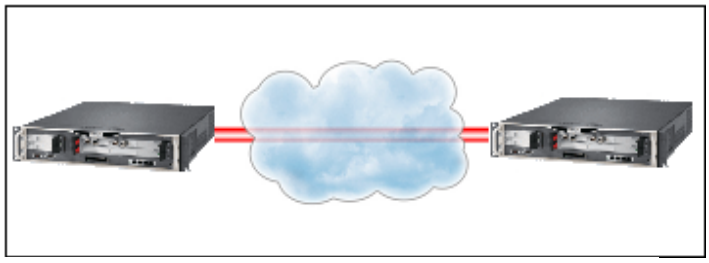

Figure 3 illustrates how a corporation can connect a remote office (Boston) located anywhere in the world with an Internet access to their headquarters (Helsinki). The Internet is used as transport media and an IPSec VPN solution (two VPN gateways) is applied to provide the necessary security solution over the public network.

Figure 3: Site to site VPN

4.2 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 or XDSL 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, SSL and L2TP with IPSec.

Managing remote access with pure IPSec requires that each remote client has 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 4.)

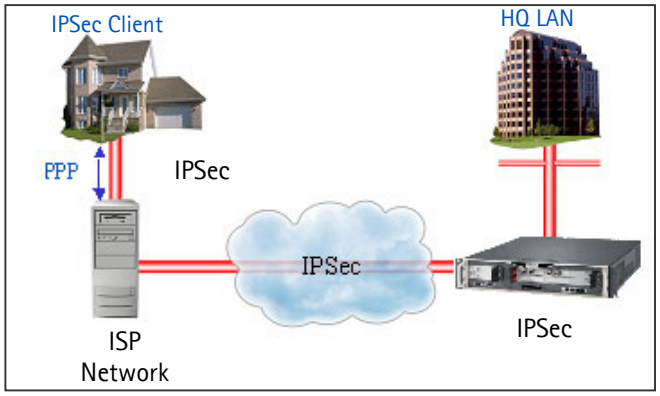

Figure 4: Remote Access VPN

4.3 Mobile VPNs

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

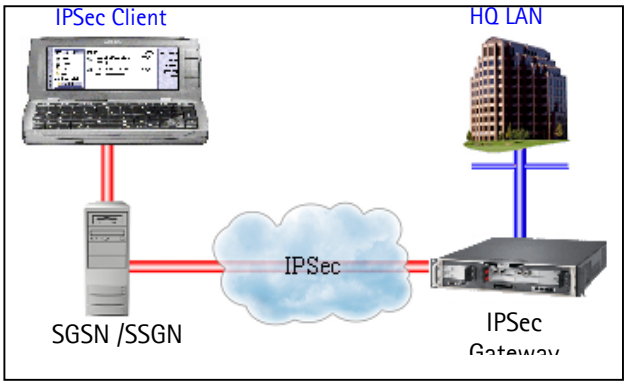

Figure 5: Mobile VPN

In both Mobile and Remote Access VPNs, users are allowed virtual connections to the enterprise network. Mobile users access the same enterprise network as they would if they were on-site connecting to the enterprise 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 enterprise gateway. After successful authentication, the mobile user is granted access to the enterprise network and provided security in the same way as the laptop user of a Remote Access VPN.

4.4 Other Security Protocols: SSL versus IPSec

If properly implemented, Secure Sockets Layer (SSL) and IPSec both offer robust security solutions. The main difference between these two protocols is that SSL operates at the application level whereas IPSec operates at the network level.

Unlike IPSec, SSL requires modifying individual applications on both the client and server end. For instance, in order for a mobile client to use e-mail, the Web browser interface provided by the server would need to be changed. Typically, this requires changes to existing applications or a special SSL UI (for example, a Web browser UI) needs to be built. In most SSL solutions, only the server is authenticated using certificates and clients are authenticated by applications using legacy authentication. This opens up a possible security risk as the clients can create a tunnel into secured network before they are authenticated.

An IPSec VPN offers a transparent solution where the applications do not know about the underlying security solution. In fact, the applications do not need to know whether there is a security solution to protect the traffic. Usually, VPNs are more complex to set up, but they authenticate clients at the network edge so attackers cannot access the network. All remote users are authenticated to gateways using digital certificates, legacy authentication mechanisms such as a SecurID card, or pre-shared secrets. Additionally, gateways must authenticate to remote users. Here, clients cannot get access to the secure network until they are authenticated. For enterprise access, an IPSec VPN is an ideal solution when the corporation does not want to change the existing applications to support SSL.

The advantage of SSL is that it offers more detailed filtering options to create very granulate access control options. SSL is good choice if applications need the knowledge about underlying security and authentication information. At the same time SSL solutions typically require more processing power that IPSec based solutions because they are implemented closer to the applications.

5 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.

5.1 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 (no IP address known) of the handheld connections makes the security management of the devices challenging. When the mobile user is establishing the secure connection to the enterprise intranet, 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.

5.2 Inherent Properties of Mobile Handheld Devices

5.2.1 Limited Memory and Resources

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

5.2.2 Processing Power

Typical handheld devices are powered by a CPU, which provides only a fraction of the computing power compared to a typical desktop PC (206Mhz ARM vs. 3Ghz Pentium IV). This means that the computation intensive tasks like key material generation and encryption take more time on a handheld device than on a desktop computer. With slow connection speeds (below 100kbps), encryption is not so much of an issue. However, generating long keys (>2048bit) from equally strong key material can take several seconds.

Although mobile device are less powerful they can offer same level of security as desktop PC's so that mobile devices won't be the "weak link" in a complete security solution.

5.2.3 Limited Battery Power

Mobile devices 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 device's CPU busy and hence require more power. Push email and similar solutions, which require continuous connection (always on connectivity)to the network may require that the device battery needs to be charged every day compared to once or twice a week.

5.2.4 Device Security

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

5.3 Number of Mobile Users

In the wireless world, the sheer number of clients can create problems for the existing infrastructure. The number of clients sets 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. Mobile user work patter is also different from a desktop user (connecting and disconnecting several times a day), which further emphasizes the gateway ability to authenticate and establish tunnels over pure throughput capacity.

5.4 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.

5.5 Seamless Roaming

Newest mobile devices (e.g. Nokia 9500) are equipped with WiFi (IEEE 802.11) capability, which means that they can be used to connect to wireless hot spots or to internally deployed WiFi infrastructures. While roaming between different GPRS networks (or network cells) is handled by the network provided (operator), roaming between different network technologies (or operators) must be handled by the device. Different techniques have been developed to address this issue (Mobile IP, MobIKE, application level roaming). Security solutions must either adapt to these technologies (Mobile IP, application level roaming) or integrate roaming capability to the security solution itself (MobIKE).

While roaming itself is an important feature, the management of roaming is equally so. Managing which networks user can and should connect to can be a tedious task for the end users so administrator should be able to provision these mobility settings to devices over the air. Ideally, security and mobility management could be done from a same management server.

6 Nokia's Mobile VPN Technology

Nokia provides end-to-end mobile security solutions for the wireless world. Nokia's Mobile VPN 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 wireless services on top of a secure platform infrastructure. The sections below describe how Nokia is implementing Mobile VPN technology. For more information, see www.nokia.com/mobilevpn.

6.1 Mobile Devices: The Operating System

Nokia Mobile VPN is designed for Series 60 smartphones running the Symbian Operating System (Symbian OS, http://www.symbian.com). 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 latest edition of Series 60 Platform (http://www.series60.com) supports all the features and functions of the second Edition and even more - especially in the enterprise and multimedia areas. In addition, the Series 60 Platform third Edition introduces a new level of flexibility and security into the platform, enabling manufacturers more easily to create devices targeted to mass markets.

The Nokia Mobile VPN Client is tightly integrated with the platform system itself using as much of the available OS components as possible thus helping to reduce the overall overhead and enhance the user experience. Nokia Mobile VPN Client comes preinstalled with some phone models and is available as an installable component for other models.

6.2 VPN Policy: Encryption and Authentication Support

Nokia Mobile VPN supports multiple encryption and public key algorithms as well as several key-management protocols including the support for industry standard IKE (Internet Key Exchange, also referred to as ISAKMP/Oakley) protocols. Nokia VPN solutions can automatically negotiate the strongest possible encryption and data authentication algorithms available between the communicating parties. This includes DES, Triple DES (3DES) and Advanced Encryption Standard (AES) 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 device itself and have the public key certified by a CA. This way the private key never leaves the device, 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 Certificate Authority (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, enterprises can utilize the existing infrastructure (for instance, SecurID cards and RADIUS servers) to handle user authentication. To help enterprises to 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 NSSM or from an external CA). Once users have digital certificates, they can start using them for VPN connection authentication. With NSSM enterprises can

6.3 Managing provisioning

Nokia has developed a Nokia Security Service Manager (Nokia SSM) product to address the needs of secure deployment. With Nokia SSM the administrators can do the initial provisioning wirelessly (maintaining strong security) and automating the updates to client polices and settings. Furthermore, Nokia SSM is able to provision additional mobility settings for the clients so that administrators can make sure that clients can adapt to the specific network environment.

Nokia SSM is a single point of management for mobile VPN infrastructure. It is the management and interoperability point for Mobile VPN Clients and different VPN gateways. In the future, it will be possible to integrate this function as a part of the device security enforcement to create a flexible management and deployment solution, which is protected by a enterprise 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.

6.4 Internal Addressing and NAT

Internal addressing is a technique where the mobile device is granted a enterprise LAN internal address and access to DNS services. Without internal addressing, remote devices could not utilize the enterprise internal DNS naming convention (intranet) and enterprise firewalls might deny the access to some enterprise servers. With internal addressing, mobile users are virtually part of the enterprise 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.

6.5 Reliable, Scalable VPN Connections to Enterprise Networks

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

The Nokia 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.

6.6 Interoperability

From the beginning, the Mobile VPN Client has been developed to be standards based IPSec client that is interoperable with number of VPN gateway vendors. From device point of view, interoperability is key feature in a multi gateway environment so that only one client is needed for all devices. Interoperability enables enterprises and especially service providers to offer a single client for end users, which they can use to connect to different VPN gateways.

6.7 Seamless roaming

Newest mobile devices are equipped with WiFi (IEEE 802.11) capability, which means that they can be used to connect to wireless hot spots or to internally deployed WiFi infrastructure. Roaming between different GPRS networks (or network cells) is handled by the network provided (operator) but roaming between different network technologies (or operators) must be handled by the device. Different techniques have been developed to address this issue (Mobile IP, MobIKE, application level roaming).

6.8 Mobile User Experience

The ultimate success of deploying mobile solutions depends on how end users adopt and accept wireless devices and security on them. Mobile devices present a special challenge in usability since the screen size and input methods is limited by the size of the devices. Nokia provides an intuitive user interface for its mobile devices 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 enterprise 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 devices can be administered wirelessly.

7 Future issues

7.1 Multiple identity

Mobile devices and smart phones especially differ from standard enterprise devices (PC's and laptops) with respect to personal usage. At the same time as mobile worker is accessing enterprise data securely the device is also his personal communication device. This means that personal data and enterprise data are accessed at the same time (VPN connection and phone call to a friend) which presents yet another challenge for security. Device, 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 devices. Addressing this issue will decide how fluently mobile devices support end user behavior and are accepted as both personal and enterprise business tools.

7.2 Complete security package

Mobile VPN is only one part in a enterprise security package. Personal firewall, anti-virus and local data encryption are must-have components so that enterprises can be sure that enterprise data is secured. Management will play an important role in ensuring that all mobile users have up to date configurations. In addition, mobile devices mean that all configurations must be delivered securely over wireless networks. To provide 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 device resources.

7.3 Voice services

Enterprises are deploying more and more WLAN access points, which makes it possible to route voice calls through enterprise own infrastructure. Voice over WLAN (or VoIP) is not secured by any encryption protocol and IPSec would be an ideal technology to have secure calls over WLAN networks. Voice packets can be authenticated by IKE encrypted by IPSec. Voice data is very sensitive to delays and other network problems, so quality of service (QoS) is very important VoIP is being implemented.

7.4 Always connected

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

About Nokia Enterprise Solutions

Enterprise Solutions is dedicated to helping businesses and institutions improve their performance by extending their use of mobility from mobile devices for voice and basic data to secure mobile access and use of their content and applications.

Our solutions range from business-optimized mobile devices for end users to a broad portfolio of IP network perimeter security gateways and mobile connectivity offerings. These solutions include mobile email and Internet, virtual private networks, or VPNs, and firewalls. Our solutions are designed to help companies mobilize their workforces while ensuring the security and reliability of their networks. Enterprise Solutions works with other technology companies to create solutions for customers.

www.nokiaforbusiness.com

About 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.

www.nokia.com