White Paper:

Managing Security on Mobile Networks

October 2002

NOKIA

CONNECTING PEOPLE

ABSTRACT

This white paper discusses the challenges of provisioning and managing security in mobile terminal environments and explains how a well-designed deployment system can alleviate these challenges. Furthermore, this white paper highlights the new technology that Nokia is developing for addressing the challenges of transparently managing security on mobile terminals, with Mobile VPN as the example.

NOTE: The term "mobile terminal" refers in this paper to handheld devices such as smart phones (for example, Nokia 9200 Series Communicators) and PDAs. Deployment and provisioning refer to delivering of software, for example Nokia Mobile VPN Client, and the initial configuration as well as subsequent updates to this software to the terminal.

EXECUTIVE SUMMARY

Mobile offices are becoming a centerpiece of business as technology savvy enterprises look for ways to improve their overall operating efficiency. Delivering faster while maintaining accuracy to both internal and external customers brings up a company's overall value. In the end, this contributes significantly to a corporation' s bottom line.

Enterprises are increasing operating efficiency by strengthening productivity. In large part, this is being achieved by extending network infrastructure to mobile terminals such as the Nokia 9200 Communicator series so that work can be done from anywhere at anytime. With mobile offices, employees are empowered to check and respond to email, send and receive faxes, hold conference calls, play video and audio content, and access corporate database applications such as SAP, People Soft, and Lotus Notes to view and edit everything from sales reports to service orders away from their desks.

A key component of setting up and maintaining mobile offices is securing information transactions from employees' mobile terminals to their corporate networks. Nokia is enabling these transactions by developing technology for transparently managing and providing security to mobile offices so that they may be used routinely without worry.

It is important to understand the specific requirements that mobility and mobile networks have on security and managing it on mobile terminals. From initial deployment to continuous management of security software on the terminal, these specific challenges can be addressed by a management system. The key requirements for a successful deployment system are centralized and automated management of mobile employees.

THE IMPORTANCE OF MANAGING SECURITY ON MOBILE TERMINALS

The number of handheld devices with connectivity to the Internet is expected to grow rapidly over the next few years. As these devices become more "business enabled," they will be used by an increasing number of employees to access corporate resources when on the move. A management challenge arises when an enterprise has a large number of mobile users whose security software and configuration on the terminals must be kept up to date. A well-designed deployment system can significantly alleviate the administration burden and contribute to providing the end users with a secure, uninterrupted service. Typically, the cost of such a system can be easily justified by looking at the dramatically reduced administration costs.

When securing mobile devices, enterprises often choose to deploy IPSec based Virtual Private Networks (VPN) in the early stages since VPNs have become an attractive way for enterprises to provide their employees with secure connections to the corporate network in a cost effective manner. Remote access VPN usage is growing quickly, starting first in laptops and now extending to mobile terminals. This can largely be attributed to the growing number of handheld devices that provide functionality and features that make them useful for actually working when on the move. Today with Mobile VPNs, employees are able to work efficiently with mobile terminals without compromising the company's security policies from basically any where they have mobile connectivity. In this white paper, Mobile VPNs are used as an example of a security application that is currently used on mobile terminals.

DEPLOYMENT CHALLENGES IN A MOBILE ENVIRONMENT

The special characteristics of mobile terminals and networks must be taken into account by a deployment system. The nature of mobile terminals and mobile access impose specific requirements on managing deployment to terminals. For a variety of reasons, mobile terminals are more challenging to manage than familiar remote access devices such as PC laptops.

Unlike laptops, mobile terminals are rarely connected directly to the corporate intranet. This means that the connections from mobile terminals are almost always from non-trusted, public networks and are shorter in duration. The location of terminals changes often in mobile networks. In fact, the location of mobile terminals can change from one type of mobile network to another.

Compared to fixed networks, mobile networks are more diverse in terms of bandwidth, reliability, and accessibility. For example, GSM HSCSD (Global System for Mobile Communications using High Speed Circuit Switched Data) provides dial-up type data connectivity with speeds ranging from 14.4 kbit/s up to 43.2 kbit/s whereas GPRS (General Packet Radio Service) provides always-on type connectivity with roughly similar data speeds. While the mobile networks provide reasonable data speeds and reliability, they are currently slower than fixed networks speeds.

Mobile terminals have less memory, storage, and processing power capacity than laptops. Smart phones, for instance, typically come with 4-16MB of available memory for applications and have considerably less powerful processors than standard desktop PCs (e.g. 206Mhz ARM vs. 2Ghz Pentium IV).

VPNs: AN EXAMPLE OF SECURITY ON MOBILE TERMINALS

VPN usage can be roughly divided in two areas: site-to-site and remote access. Site-to-site VPN refers to two separate network entities connected together over an insecure network where

communications from one network to the other is secured (encrypted) transparently without the parties engaged in the communication being aware of it. On the other hand, remote access VPN refers to individual end users accessing a private network over insecure public networks forming connections from their terminal to the private network. Corporate employees requiring secure access to the corporate network over the Internet use remote access VPNs.

Mobile VPN is a specific type of remote access VPN where the end user VPN connections are established from mobile terminals instead of laptops. The nature of mobile terminals and mobile networks adds to the complexity of the VPN solution. Mobile VPNs require management software to administer the client environment. In addition to the VPN client software, specific configuration information (often referred to as VPN policy) is required in the client end so that the VPN client can determine the following:

- The gateway the client should connect to.
- The circumstances under which the client should connect to the gateway,
- The security parameters the client should use when connecting to the gateway.
- The protected networks the client is allowed to access.
- The PKI data configuration if it is to be used in VPN authentication.

Managing the above-listed information requires a robust deployment system that can securely deliver the client software and configuration as well as secure, transparent updates to mobile terminals.

REQUIREMENTS OF A SECURE DEPLOYMENT SYSTEM

The problem of managing security applications and configuration of them on mobile terminals can be divided into two separate areas that share similar characteristics. They are: 1) the initial deployment phase; and 2) the subsequent automatic, transparent updates.

The initial deployment stage is where the software, for example Mobile VPN, and the initial configuration information need to be delivered to mobile terminals. There are several ways of accomplishing this. The initial installation may be carried out centrally by the corporate IT-services. In this case, the end user gets a terminal with the VPN Client software installed and configured. Here, it can be assumed that the personnel carrying out the installation are trusted and authorized to do the work. Therefore, there is no problem related in establishing initial trust in the terminal.

In another case, end users may be required to carry out the initial installation of the Mobile VPN Client software. In this scenario, it is critical to establish initial trust in terminals without compromising the overall security of the VPN system. Establishing the initial trust is the first stage since it will be used for providing automatic configuration updates to terminals. This makes the initial deployment stage especially challenging since terminals have nothing either VPN gateways or the deployment system can trust.

The initial trust between a terminal and the deployment system can be achieved by utilizing the existing user authentication systems of an enterprise. In addition to authenticating the user to the deployment system, the deployment system must authenticate to the user. Once both parties have authenticated each other, a certificate can be issued to the terminal can be used for future authentication. Similarly, the deployment system will use certificates to authenticate itself to the terminal.

The second stage covers all the subsequent updates to the client software and its configuration. The delivery of content must take place securely. Trust in the form of certificates created between the terminal and the deployment system s used to securely authenticate both parties and deliver the required updates to the terminal. In mobile networks, certificates provide an ideal method of authentication. Using certificates for content updates saves mobile users time and effort since they do not have to spend valuable airtime using manual authentication methods to get their updates.

The initial deployment and update phases described above set the unique set of requirements for a secure, transparent, powerful deployment system.

AUTHENTICATING MOBILE TERMINALS TO A DEPLOYMENT SYSTEM

Before any kind of configuration information is sent to the terminal, the deployment system as well as the client must authenticate each other to ensure that the parties engaged in communications can be trusted. Unless this trust can be reliably established, there is a danger that intruders portray themselves as a trusted part. The deployment system could then provide a trusting party with false information or gather information provided by the trusting party. For example, if the user cannot reliably authenticate the deployment server, an intruder could provide the user with false configuration information and then render the Mobile VPN Client inoperable or direct the client to a false service.

There are number of ways to authenticate parties. In large mobile client environments, only PKI based authentication methods provide a scalable and manageable solution. A deployment system should be able to utilize an enterprise's existing PKI solution or provide the required PKI functionality or both.

DELIVERING OF SECURE CONTENT

After both parties have been successfully authenticated, the delivery of the content from the deployment system's management server must take place in a secure way. This can mean either encrypting the actual connection between the terminal and the deployment system or encrypting the content that is being delivered. No matter what the approach, the terminal must be able to verify that content delivered is indeed from the intended originator and that it has not been modified during delivery.

AUTOMATICALLY UPDATING SECURITY ON MOBILE TERMINALS

Updates to policy or any other configuration information in terminal must take place automatically and transparently without any end user intervention. Consider the care of VPN. Configuration changes in the VPN infrastructure affect large numbers of users and any new configuration must be available immediately.

The frequency of changes in the VPN configuration vary from case to case, but when a change takes place it tends to affect the majority of the remote users. Carrying out the deployment of these new configurations manually can be either impossible or take so long that it has serious impacts on the VPN service to the users. An automatic update mechanism enables either new or updated configurations to be available for mobile employees as soon as changes take place.

The security infrastructure should be as transparent as possible to mobile users. When the mobile user is not required to deal with updates, there is less chance for errors occurring. Furthermore, if

the updates are done automatically, potential security compromises during the updates are avoided. An automatic system guarantees that the most up-to-date configuration is always in use, thus guaranteeing uninterrupted, secure access to corporate resources.

ADMINISTERING LARGE NUMBERS OF MOBILE TERMINALS

In large deployment environments, administration tasks are commonly distributed among many people. One or many system administrators may be responsible for the overall configuration and operational aspects of the system. User management may be distributed to dedicated user administrators who in turn may have management rights to specific user groups. To support this kind of distributed administration model, the deployment system must support multiple levels of administrator roles and strictly control access to the system accordingly.

BENEFITS OF A SECURE DEPLOYMENT SYSTEM

The benefits of a deployment system can be viewed from various points of view. The maintenance and management costs involved with mobile devices are high. The cost of the devices themselves, when compared to the total cost of ownership over the devices' lifetime, forms a minor share of the total cost of ownership whereas management and maintenance costs can be significant. Financial models, such as various TCO models, provide means to estimate the financial impact of mobile devices and give justification for investing in a management and deployment system. [1]

Ultimately, a sound, business case will determine how much enterprises are willing to invest in a provisioning and management system. Making this decision requires careful consideration of the technology as well as the business drivers for implementing a management system for mobile devices.

ADOPTING AND DEPLOYING SECURITY RAPIDLY

Enterprises that expand their VPNs to mobile devices must guarantee that new services and security for them is deployed rapidly. The larger the number of mobile users, the more important it is to make sure the client software and initial configuration are made available to users as soon as the VPN system is up and running.

Deployment of a mobile VPN service is also a matter of cost. The longer the initial deployment phase, the higher the overall costs of the mobile VPN project. Productivity of the mobile workers increases considerably when the corporate resources can be accessed securely from anywhere at any time. Therefore, offering mobile VPN to all mobile users as soon as it is possible will increase their productivity.

CENTRALLY MANAGING MOBILE TERMINALS

Key features of a good deployment system are centralized management of mobile users and their corresponding configurations. When the amount of terminals grows to hundreds or thousands, management of software like Mobile VPN Clients becomes almost impossible without a deployment system. In large enterprises with offices all over the world, mobile users can connect to the corporate resources through a variety of VPN gateways. These enterprises require a centralized

[1] Mobile and Wireless Security: Worst and Best Practices, Research Note, 20 September 2001, Gartner

distribution system. This system guarantees that the mobile user is always provided with the most current policies.

An automated system for delivering configuration updates to thousands of mobile terminals reduces the time required to send configuration information to mobile employees. Timely delivery of the required configuration information is essential to ensure that end user access to the corporate network is not disrupted. An automated system also reduces the number of people needed to carry out manual deployment, which can be time consuming. Finally, support overhead is reduced since potential errors caused by end users manually updating configurations are totally eliminated.

ENHANCING SECURITY THROUGH MANAGEMENT

Any security system is as vulnerable as its weakest link. Therefore, it is essential that no shortcuts be taken when deploying security. Having a deployment system that does initial provisioning and future updates automatically enhances and enforces and enterprise's security policy. A well-designed deployment system handles various updates to the terminal automatically requiring very little intervention from the end user. Thus, an automatic deployment system saves significant amount of end user time when the updates to the terminal take place automatically. Perhaps even more importantly, an automatic deployment system removes the requirement of having mobile employees update their security. They don't have to know how to implement security—it is just there for them.

Additionally, a deployment system can act as a centralized provider of PKI services for enterprises. By adopting PKI as part of the security infrastructure, enterprises can enhance the overall security of its systems. Authentication is one of many areas where PKI can simplify and enhance security. Moving from legacy authentication to PKI based authentication is a major change for any organization. A well-designed deployment system can provide functionality to ease this transition.

NOKIA SECURITY SERVICE MANAGER (NSSM)

Nokia Security Service Manager (NSSM) is a deployment and provisioning system designed specifically to address the initial deployment, subsequent configuration management, and PKI related requirements in mobile environments. To start, NSSM provides a scalable Mobile VPN solution that enterprises can use to extend their VPN to the mobile domain using the Nokia Mobile VPN Client for Symbian OS and supported Check Point VPN gateways. Mobile VPN is independent of the VPN system and can be run with any VPN system that is capable of delivering its client policy information to NSSM. This section explains how NSSM expedites deployment of security within an enterprise using Nokia's Mobile VPN Client as an example.

DEPLOYING SECURITY TO MOBILE TERMINALS

The initial deployment of the Nokia Mobile VPN Client software and policy must take place securely. The key step in achieving this security is establishing a trust between a mobile terminal and the deployment system, NSSM. NSSM provides a means of reliably and mutually authenticating mobile terminals and NSSM with each other. The authentication mechanism allows rapid initial deployment of large numbers of mobile terminals.

NSSM has a web-interface that can be accessed by any TLS/SSL enabled browser with high encryption capabilities (such as 3DES with 168-bit keys). This HTTPS interface is used to authenticate mobile users the first time they access NSSM. Authentication can take place against a

RADIUS server, for example. In addition to providing their user credential, users are also required to enter an identification code produced by NSSM. This code is delivered by some out-of-band mechanism and verifies the authenticity of NSSM to them.

UPDATING SECURITY POLICIES

NSSM provides automatic policy and configuration updates to the Nokia Mobile VPN Clients. The first time mobile employees connect to NSSM, they are required to authenticate using a username and password. After initial authentication, the client is issued a device certificate by NSSM's internal certification authority (CA) that is then used for authentication when policy or any other content updates are required. The mobile device automatically connects to NSSM to check for updates when a VPN connection is being initiated. If an update is available, it is installed on the mobile user's terminal and they are notified that the update took place. The user can also manually initiate an update request to NSSM.

CONVERTING SECURITY POLICIES

NSSM provides automatic conversion of the VPN policy to a format required by the Nokia Mobile VPN Client for Symbian OS. NSSM has an open content delivery interface that defines the format and method of delivering VPN policy information from any vendors' VPN policy management system to NSSM. This open Content Update Interface is based on SSL protected HTTP requests that contain XML-formatted messages.

MANAGING MOBILE USERS

NSSM provides flexible tools for managing the mobile employee user base. User information can be retrieved using various methods from the existing user databases. Hierarchical user groups enable users to be organized to best reflect the planned deployment model. The content delivered to the terminals is associated with the user groups allowing content delivery to be managed at a granular level.

Grouping can be based on any number of things such as geographical location or departments within a company. Users can be members of multiple groups. When a user logs into NSSM, their group memberships are automatically checked. The content presented to them is based on all the groups the user is a member of or has inherited from other groups through group hierarchies.

AUTHENTICATING TO THE DEPLOYMENT SYSTEM

NSSM supports user authentication using certificates, normal and one-time passwords generated with token cards such as SecurID against RADIUS servers, and usernames and passwords against NSSM's local database. Ability to utilize the existing legacy authentication services that the enterprises already have in place allows NSSM to be easily integrated as part of existing IT infrastructure.

MIGRATING TO PKI INFRASTRUCTURE

NSSM has powerful PKI features that provide enterprises an easy migration path from legacy authentication to certificate-based authentication. NSSM can act as a registration authority (RA) towards external CAs providing an automatic certificate enrollment process for end users. Depending on the external CA used to issue the certificates, NSSM can communicate with the protocol required by the CA to enable automatic certificate issuance. Currently, the supported protocols are SCEP (Simple Certificate Enrollment Protocol) and CRS (Certificate Request Syntax).

NSSM also adds to the security of the enrollment process since it can be configured to require users to authenticate to NSSM when this process is initiated. In addition to authenticating the mobile employee, NSSM also checks that they are entitled to carry out the enrollment request. The enrollment gateway functionality provides a central point where the administrator can see the status of the enrollment requests and certificates in use.

NSSM also includes an internal CA. It is used in providing PKI based authentication services to the automatic policy update functionality. It can also be used to issue dedicated certificates for VPN authentication usage. If the certificates are used in a closed VPN environment only, then this approach is not only more flexible from the administration point of view but it can also result in substantial cost savings compared to using certificates issued by an external CA. The certificates issued by the NSSM internal CA adhere to the X.509v3 standard. CRLs (Certificate Revocation List) and OCSP (Online Certificate Status Protocol) are supported for checking certificate revocation information issued by the internal CA or external CAs.

FUTURE ISSUES IN MANAGING MOBILE TERMINAL SECURITY

Mobile terminals and smart phones differ from standard corporate terminals (PCs and laptops) with respect to the capabilities of the terminals and the mobile environment they operate in. They are also often utilized for both business and personal use, which presents challenges for managing multiple identities and security domains on terminals. The requirements for security applications on mobile terminals and management of them are specific and complex.

NSSM is a step towards providing a single point of security management for all security related applications on mobile terminals. It is a vendor and application independent, self-sufficient security provisioning and management system. The provisioning functionality can be utilized for rapidly deploying security applications such as anti-virus software and personal firewalls and providing them with automatic configuration updates when required. NSSM has open interfaces for configuration provisioning that any vendor can utilize. The standards based PKI functionality in NSSM can also be utilized by various applications to enhance their security and use-ability on mobile terminals. NSSM will continue to address the specific needs of mobile security and provide 3rd party vendors with open interfaces to utilize its services.

CONCLUSION

In mobile terminal environments, an easy-to-manage, secure deployment and provisioning system adds to the overall value of a company's security system. A well-designed deployment system addresses various requirements in the area of authentication and content delivery to mobile terminals. PKI plays an important role in making the deployment system capable of scaling to support large numbers of mobile users. The criteria for choosing a deployment system must ultimately be based on a solid, justifiable business case, not solely on the deployment technology itself.

NSSM has been designed to support rapid deployment of security applications such as Nokia Mobile VPN Clients on mobile terminals and provide means to automatically update configuration and other content when required. The guiding principles have been administration cost reduction, ease of mobile client management, and enhanced end user experience without compromising security at any stage of the provisioning process.

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 and Internet transaction that is personal and trusted-each and every time.

For more information, please visit 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

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

Asia Pacific
438B Alexandra Road
#07-00 Alexandra Technopark, Singapore 119968
Tel: +65 6588 3364
E-mail: ipsecurity.apac@nokia.com

www.nokia.com

NOKIA
CONNECTING PEOPLE