

Nokia Mobile VPN Solution Extending Your Enterprise by Mobilizing Business

Nokia for Business



management of them. Nokia SSM can manage the PKI (Public Key Infrastructure) related requirements in mobile environments.

Using VPN for Mobile Phones

The Nokia Mobile VPN solution extends enterprise networks to mobile devices that are optimized for business use, offers secure access to business applications, and provides a single point of security management for an increasing number of mobile employees and devices. Key components of Nokia Mobile VPN include Nokia Mobile VPN Client and Nokia Security Service Manager (Nokia SSM).

Nokia Mobile VPN Client

Nokia Mobile VPN Client is an Internet protocol security (IPSec) virtual private network (VPN) application developed by Nokia for Symbian OS-based mobile devices. An IPSec VPN allows you to use the mobile network and the Internet to safely connect from the mobile phone to the enterprise network. Once you authenticate to the enterprise VPN successfully, all data travels to and from the mobile phone encrypted and is received exactly as the sender sends it. IPSec also protects against electronic data theft because attackers cannot capture data when you send or receive it and retransmit it later.

Key features of the Nokia Mobile VPN Client:

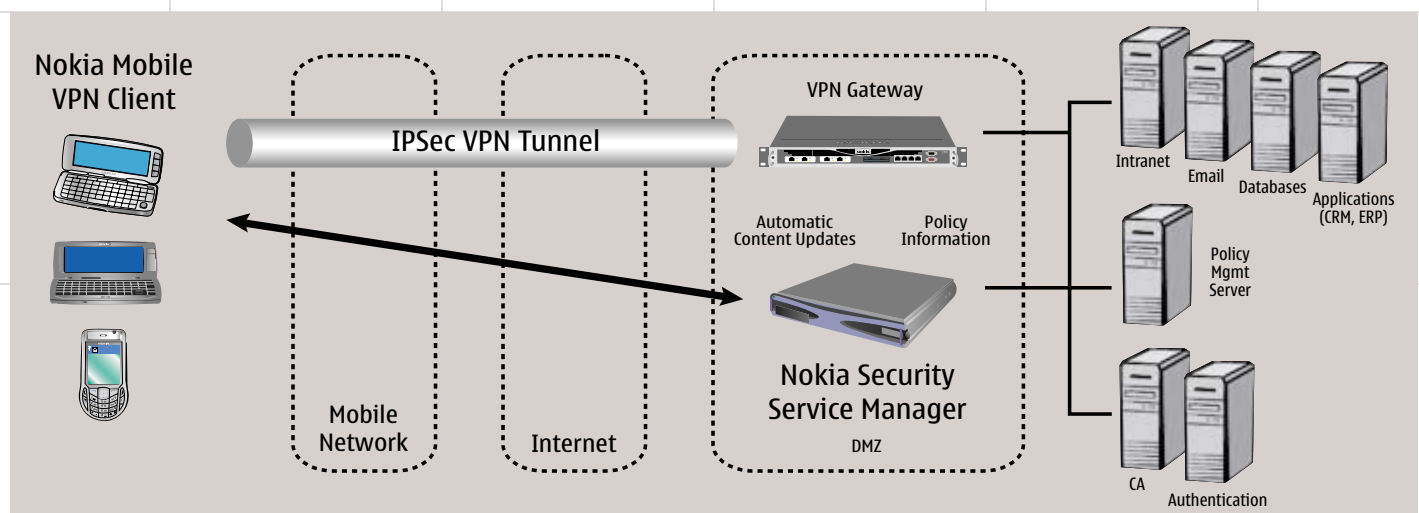
- Empowers a mobile worker to securely access any network services from emails to mobile client-server applications like CRM and ERP as well as database applications
- Supports Nokia Series 60 and Series 80 business range devices based on Symbian OS including Nokia 9500, Nokia 9300, Nokia 6670, Nokia 6630, Nokia 6600, Nokia 6620, Nokia 6260, Nokia 7610, Nokia 3660, Nokia 3650, Nokia 7650, Nokia 9200 Communicators and more
- Supports legacy and PKI based authentication
- DES, 3DES and AES for encryption
- SHA-1 and MD5 for data integrity
- Uses Nokia SSM for automatic provisioning of VPN settings, policy updates and certificate enrollment
- Integrates with Nokia IP VPN, compatible with Cisco and Check Point VPN gateways

Nokia Security Service Manager

Nokia Security Service Manager is the centerpiece of a scalable Mobile VPN solution. It enables VPN to be extended to the mobile domain using the Nokia Mobile VPN Clients and supported VPN gateways. Nokia SSM is designed specifically to address the initial deployment of Nokia Mobile VPN Client software and policies and subsequent

Nokia Mobile VPN Solution

- Secures mobile connections for business use
- Provides easily-managed security
- Connects mobile workers reliably to their work



NOKIA
Connecting People

Key features of Nokia Security Service Manager:

- Key for rapid, large scale Mobile VPN deployments
- Integrates with VPN policy management systems and external authentication servers
- Enables the creation of trust between the user and the corporate infrastructure
- Provides automatic over-the-air provisioning of VPN configuration securely to mobile devices
- Provides mobile devices with PKI services

Deploying and Managing Mobile VPN

Initial deployment of the Nokia Mobile VPN Client software and configuration information must take place securely without compromising the overall security of the VPN system.

For initial installation, Nokia SSM provides a way to reliably and mutually authenticate mobile devices. Authentication can take place against the Nokia SSM local database or external authentication server (RADIUS, LDAP). After initial authentication, the client is issued a user certificate by Nokia SSM internal certification authority (CA), which is then used for authentication when policy or any other content updates are required.

Nokia Security Service Manager provides automatic policy updates to Nokia Mobile VPN Clients. When a VPN connection has been initiated, the mobile device automatically connects to Nokia SSM to check for updates. If an update is available, it is installed on the mobile device with a notification to the user that the update will take place.

Migrating to PKI

Nokia Security Service Manager has powerful PKI features that provide enterprises an easy migration path from legacy authentication to certificate-based authentication. Nokia SSM can act as a registration authority (RA) towards external CA's providing an automatic certificate enrollment process for end users. The supported protocols are SCEP (Simple Certificate Enrollment Protocol) and CRS (Certificate Request Syntax).

Nokia Security Service Manager includes an internal CA that can 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 can also result in substantial cost savings compared to using certificates issued by an external CA. The certificates issued by the Nokia SSM internal CA adhere to the X.509v3 standard. Certificate Revocation List's (CRL) are supported for checking certificate revocation information issued by internal or external CAs.

Nokia IP VPN Solution

Nokia IP VPN is a secure connectivity solution which connects people and locations to business applications and data from corporate-issued devices. The solution is ideally suited for IT Managers of growing companies who need to scale their connectivity infrastructure easily to support their fixed and mobile environments. Unlike competitors, Nokia provides easy scaling of IP VPN networks for dynamic networks, extreme reliability, superior price performance, mobility and a seamless end-user experience. Nokia Mobile VPN is integrated with Nokia IP VPN solution providing complete end-to-end connectivity solution for enterprises.

Requirements

Nokia Mobile VPN Client is supported on Nokia 9500 Communicator, Nokia 9300, Nokia 6670, Nokia 6630, Nokia 6260, Nokia 7610, Nokia 6600, Nokia 6620, Nokia 9200 Communicators, Nokia 3660, Nokia 3650, Nokia 7650 and N-Gage. See the latest list of supported models at www.nokia.com/mobilevpn. Nokia Security Service Manager is supported on Sun Solaris 8 or 9 and Red Hat Enterprise Linux 3.

Compatible VPN gateways include:

- Nokia IP VPN Gateways (Nokia 500i, Nokia 100i, Nokia 50i and Nokia 10i) with Nokia VPN Manager
- Check Point VPN-1 running on Nokia IP Security Platform with Check Point SmartCenter NG AI or higher
- Cisco 3000 Concentrator running software release 4.7 or higher. Note: Software release 4.7 planned to be available from Cisco in April 2005.

Supported Industry Standards

Encryption algorithms

- DES (56 bit), 3DES (168 bit), AES (128, 192, 256 bit)
- SHA1, MD5 Hash algorithms

User authentication

- X.509v3 Digital Certificates
- CRACK for Legacy Authentication
- Username/Password (RADIUS)
- Tokens (SecurID)
- IKE Pre-shared secret
- DSA Certificates
- RSA Public Key encryption, RSA revised encryption

Public key algorithms

- Diffie-Hellman 768-1536 bit (Groups 1, 2 & 5)

Key management

- IKE (ISAKMP/Oakley) (Main, Aggressive)
- PKCS#8 for private key format, PKCS#5 v2 for private key encryption
- PFS for IPSec associations

Americas

Tel: 1 877 997 9199

Email: mobile.business.americas@nokia.com

www.nokiaforbusiness.com