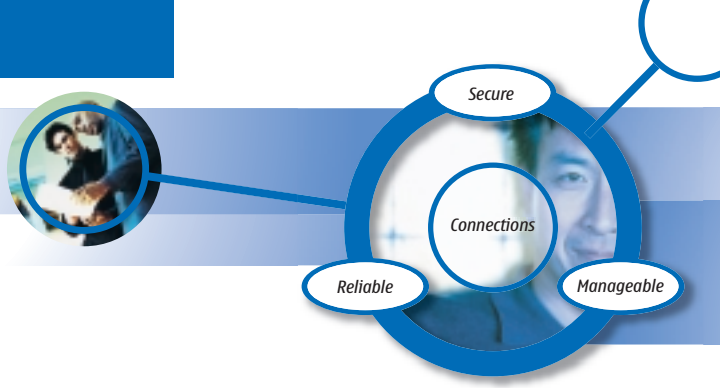


Nokia Mobile VPN Solution

Extending Your Enterprise by Mobilizing Business

Using VPN for Mobile Phones

The Nokia Mobile VPN solution extends enterprise networks to mobile phones 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 phones. The solution consists of Nokia Security Service Manager (Nokia SSM) and Nokia Mobile VPN Client that interoperates with Check Point VPN-1 software running on Nokia IP security platforms.

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

Key benefits of Nokia Security Service Manager:

- Manages security lifecycle on Symbian OS-based mobile phones
- Manages security on mobile phones from a single point to reduce administration complexity and costs
- Provisions and manages security applications and policies over-the-air
- Provides automatic policy and other security content updates enabling uninterrupted service for mobile workers
- Utilizes existing legacy authentication services already in place to allow easy integration of mobile security as part of existing IT infrastructure
- Enables rapid and seamless migration from legacy to certificates-based VPN authentication

Nokia Mobile VPN Client

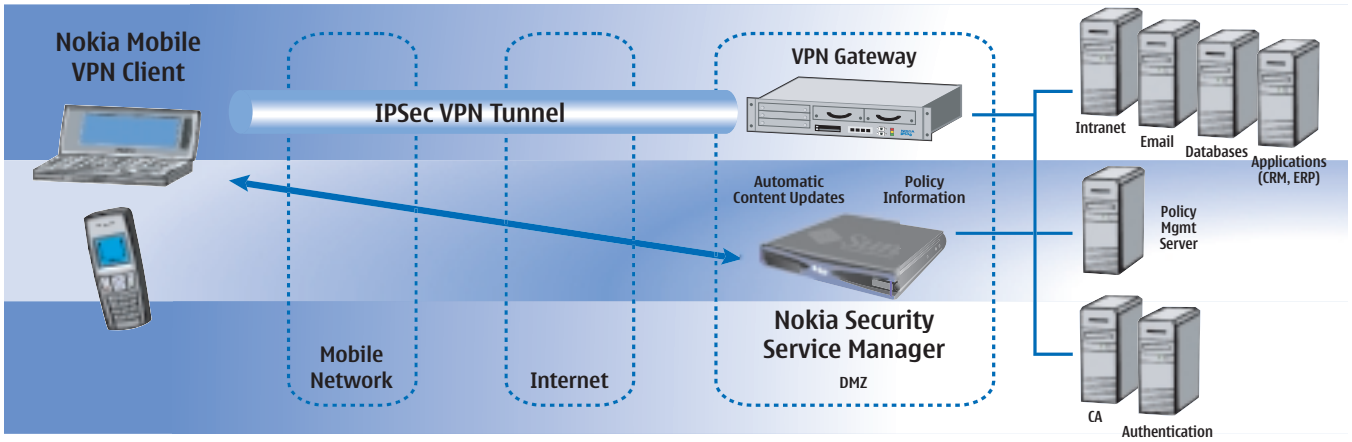
Nokia Mobile VPN Client is an Internet protocol security (IPSec) virtual private network (VPN) application developed by Nokia for Symbian OS-based mobile phones. An IPSec VPN allows you to use the mobile network and the Internet to safely connect from the mobile phone to the enterprise network. Once 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.

Nokia Mobile VPN Benefits

- Secures mobile phones for business use
- Provides easily-managed security
- Connects mobile workers reliably to their network

Key benefits of the Nokia Mobile VPN Client:

- Is a network layer security solution – no application specific security required
- Empowers mobile workers to securely access any network services from Email, calendar and contacts and is tailored to mobile client-server applications like CRM and ERP as well as database applications



NOKIA

CONNECTING PEOPLE

- Supports Nokia 9200 Series Communicators and Nokia 7650/3650 mobile phones
- Supports legacy and PKI based authentication
- Uses DES and 3DES encryption
- Uses SHA-1 and MD5 for data integrity
- Uses Nokia Security Service Manager for automatic policy updates
- Supports automatic certificate enrollment via Nokia SSM
- Interoperates with Check Point VPN-1 NG software from Nokia global partner, Check Point Software Technologies

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 phones. Authentication can take place against the Nokia SSM local database or external authentication server (RADIUS). 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 phone automatically connects to Nokia SSM to check for updates. If an update is available, it is installed on the mobile phone 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.

Requirements

The Nokia Mobile VPN solution environment consists of these components:

- Nokia Security Service Manager 2.0
- Nokia Mobile VPN Client 2.0
- Check Point SmartCenter running Check Point NG
- Nokia IP security platform running Check Point VPN-1/Firewall-1 NG

The supported platform for Nokia Security Service Manager 2.0 is Sun SPARC/Solaris 8. The Nokia Mobile VPN Client 2.0 is supported on Nokia 9200 Series Communicators (9210, 9210i and 9290), and on Nokia 7650/3650 mobile phones. The Check Point SmartCenter can be run on Nokia IP security platform, Microsoft Windows 2000, NT, Sun Solaris, or Linux.

Supported Industry Standards

Encryption algorithms

- DES (56 bit), 3DES (168 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 (Group 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: ipsecurity.na@nokia.com

Asia Pacific
Tel: +65 6588 3364
Email: ipsecurity.apac@nokia.com

Europe, Middle East and Africa
France +33 170 708 166
UK +44 161 601 8908
Email: ipsecurity.emea@nokia.com

NOKIA
CONNECTING PEOPLE

N15 000 040
Copyright © Nokia Inc. 2003. All rights reserved. Nokia and Nokia Connecting People are registered trademarks of Nokia Corporation. Check Point, the Check Point logo, FireWall-1, and VPN-1 are trademarks or registered trademarks of Check Point Software Technologies, Ltd or its affiliates. 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.