

Security and device management – Nokia Eseries



NOKIA
Connecting People

Security and device management – Nokia Eseries

This White Paper describes the fundamentals of security and device management, with a focus on the features of the most advanced Nokia business devices: Nokia Eseries. Aimed at IT professionals and decision-makers who need to provide secure mobile access to corporate data systems, the document also contains information that may benefit business end-users.

Contents

Security enabling business mobility	3	Security applications	8
Secure mobility considerations for today and tomorrow	3	Device management	8
Security and device management: the essential components	4	Trust administration model (Terminal Administration Rights Model – TARM)	8
Device security	4	Compatible OMA device management solutions.....	8
Device lock.....	4	Managing policies for Mail for Exchange users.....	8
Remote locking.....	5	Managing policies for IBM Lotus Notes Traveler users.....	9
Memory card security.....	5	Nokia Configuration Tool	9
Call barring.....	5	Conclusion	10
Certificates.....	5		
Connection security	6		
Bluetooth® security.....	6		
Wireless LAN security.....	6		
Secure browsing.....	6		
Secure intranet access.....	6		
Content and application security	7		
Device memory and memory card encryption.....	7		
Data backup.....	7		
Application signing.....	7		
Device Platform API controls.....	7		

Security enabling business mobility

Companies are increasingly finding that both time and money can be saved when mobile employees have easy access to enterprise information and IT services. At the same time, the security of that information, as well as the ability to manage access to it, has never been more important.

As more mobile workers access more confidential information within an organisation's IT infrastructure, administrators are faced with real security concerns. What happens if a mobile device is lost or stolen? Can data on the device be encrypted so company-sensitive information is protected? And is it possible to protect mobile devices and the connection to the corporate network from outside threats such as hackers and viruses?

Mobile security is not simply a type of software or solution; it is a combination of solutions that together best meet the varied security needs of an organisation. For organisations, it is essential to be able to control access to corporate resources effectively. Only authorised and authenticated users and devices should be allowed to access company IT services. Access technologies also need to provide confidentiality to prevent unauthorised parties from eavesdropping or altering communications. Nokia has collaborated with leading IT vendors to ensure that their solutions extend to Nokia mobile devices. In many cases, administrators can use the same, well-known solutions to manage fixed and mobile solutions simultaneously.

Secure mobility considerations for today and tomorrow

The amount of computing power available on smartphones has increased dramatically in recent years. Being more like a computer implies increased exposure to security threats typical on personal computers. Malicious programs such as viruses, worms and Trojan horses will likely become more prevalent on mobile devices in the years ahead. One major difference between the PC and mobile devices is that mobile devices are typically carried with the user at all times, whether in the office, out of town, at home, or all points in between. This increases the risk of the mobile device being lost or stolen, thereby exposing the data, calendar information, key contacts, and email stored on the device being compromised. Nokia recognises these potential threats so Nokia Eseries devices incorporate underlying technologies that enable IT departments to extend their security policies into mobile devices. These security features are built on top of Symbian, a secure operating system built with trusted computing concepts.

These security policies can be managed via Microsoft Exchange policies or standards based Open Mobile Alliance (OMA) Device Management (DM) technology. Aside from enforcing security, having the ability to configure devices, manage applications and settings remotely helps organisations to save costs related to support and maintenance functions. The rest of this paper elaborates how Nokia products are built with an eye toward mobile security.

Security and device management: the essential components

Mobile security involves several different areas. The most tangible element of mobile security for the typical business user is the mobile device and its user interface. Mobile security can be divided into three key areas: device security, connection security, and content security.

Mobile security area	Key function
Device security	Out-of-the-box hardware and platform security
Connection security	Protecting data in transit
Content security	Protecting both business and personal data from unauthorised use in case of theft or loss

Security within a mobile device entails both hardware and platform security. Hardware security enables the storing and execution of sensitive information, and helps ensure that the device will only run valid software. Platform security involves the management of services like the authorisation and authentication of software, which helps ensure that only verified applications can access protected resources. The platform also typically provides security services for the user and upper level applications, such as application programming interfaces (APIs) that applications use to process encrypted data or to access hardware-based security services. It can also address usability issues related to security, such as how the user is prompted and what kinds of prompts are shown.

Should an additional level of security be required than a device originally supports, then it is possible to deploy applications that can be used to further improve the security of the device. For instance, add-on firewall, data encryption and antivirus applications can be used to address specific security concerns. Additionally, device management can be used to help ensure that a device has the correct settings, and that the device software is current.

Connection security refers to how the device connects to secured services like company intranets. VPN connectivity can be used to help ensure smooth and reliable access to IT resources and services. Additionally, Bluetooth® and Wireless LAN connectivity methods include their own security functions.

Nokia Eseries are business-optimised devices offering built-in features as well as add-on applications to meet the security needs of an organisation. Features including

built-in encryption functionality for both the device memory and for the memory card, integrated mobile VPN support, and device lock and wipe all support enterprise-specific deployments.

Device security

As users increasingly install software from different sources on their advanced mobile devices, the importance of security features becomes clear. The design objective for security-related features is to work to ensure that whatever decisions and interactions the user has to make, they are not too difficult to perform or understand. Security mechanisms that are too difficult to use or too complicated to carry out mean that the user becomes frustrated, possibly leading to the disregard of security related issues or abandonment of the service.

To achieve this high level of security and simplicity, Nokia married trusted computing concepts from the defence industry with user centric experiences from our consumer heritage of Connecting People. Security professionals are always pleasantly surprised that Symbian is a trusted operating system with application compartmentalisation and a Trusted Computing Base (TCB) capability model.

Feature	Key function
Device security	Prevent unauthorised usage
Device locking	Protects the device in case of theft or loss
Memory card security	Protect data with password and optionally with encryption
Call barring	Restrict incoming or outgoing calls
Certificates	Secure transfer of confidential data and user authentication

Device lock

Users have the option of activating a security key guard to lock the keypad on the device when it is not in use. This is an important feature for protecting device data, and the code can be changed by the user at any time. The user can attempt to enter the device lock code any number of times, but after every fifth false code attempt, the device will time-out for five minutes before allowing any further attempts. During this period, the device will remain locked, even if the correct device lock code is typed in. Any attempts to type in a code during this time

will reset the timer and a new five-minute period will start. The user can also set the device to ask for the lock code when the SIM card is changed.

Remote locking

Remote locking allows device lock to be activated remotely by the user or by the IT administrator. Device lock can be activated by sending a text message that includes a user predefined remote locking code. The user receives a confirmation text message that the device is locked and that the remote lock code is also enabled for the memory card. Remote locking codes can be from five to twenty characters. If the device is locked and the attacker changes the SIM card, he/she will find that the device cannot be used.

Remote locking and lock policy can be controlled over-the-air using a compatible OMA device management solution. The individual user is able to choose their own lock code, though within the parameters of the company's lock policy. Parameters such as minimum lock code length, require alphanumeric lock code, maximum inactivity time and local wipe of the device after maximum number of attempts are supported. In case the device is lost or stolen, the user can also call the help desk administrator to initiate remote lock and wipe over-the-air via the company's device management system.

Memory card security (for devices with memory card support)

The memory card can be protected with a password that is required before it can be used and accessed with another device or computer. Additional security in the

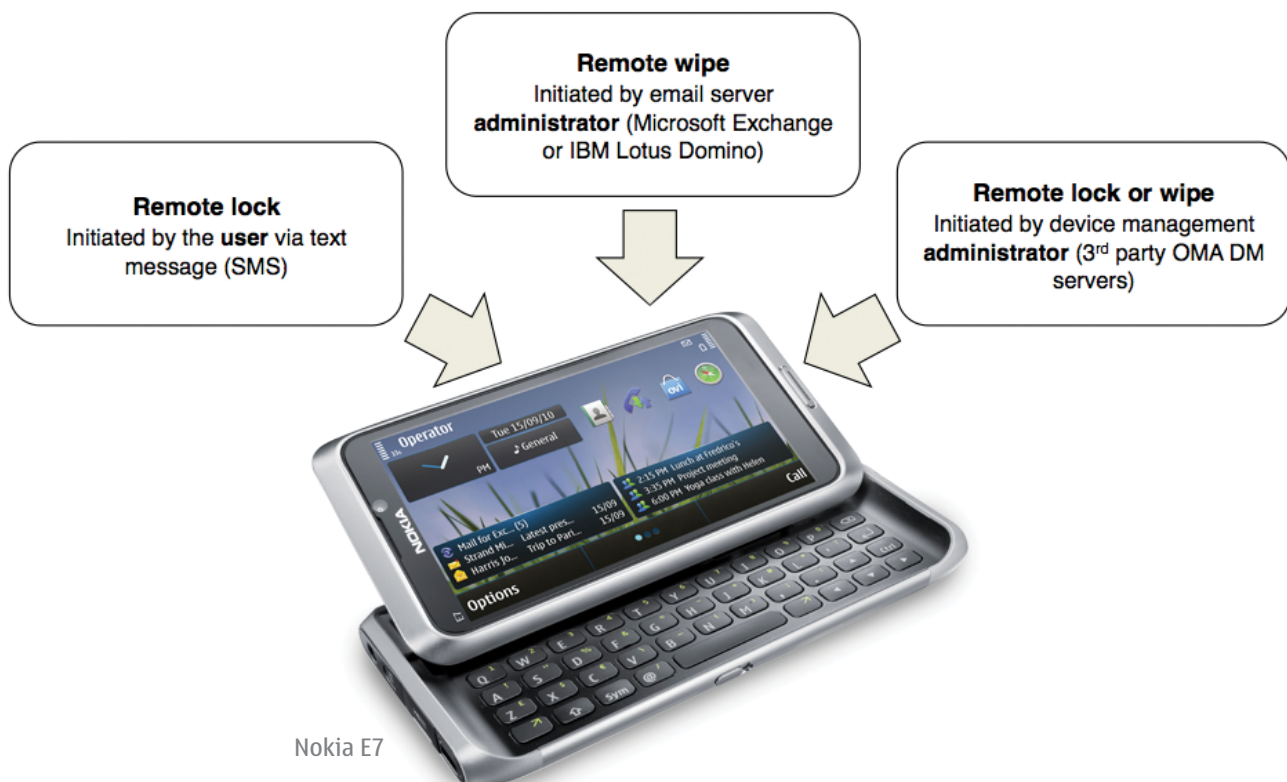
form of hardware accelerated memory card encryption is also available on compatible devices including all Eseries devices.

Call barring

This feature allows the user to restrict incoming or outgoing calls, as well as access to international calls. Call barring and call diverting cannot be active simultaneously. Calls to specific official emergency numbers are still possible when other calls are barred. To use the call barring service, users need the call barring password supplied by the service provider.

Certificates

Digital certificates are used to connect to a site in order to transfer confidential information, such as with an online banking service. They can also be used to check the authenticity of software that the user wants to download, reducing the risk of viruses and malware. Symbian stores certificates in four certificate stores – personal certificates, phone certificates, trusted site certificates and authority certificates. Certificates in the personal store can only be used after the user enters the correct PIN code; this is in contrast to the phone certificate store. User certificates for Mail for Exchange should be stored in the latter store so that users are not repeatedly prompted to provide a PIN. The trusted site store is used for SSL certificates that are signed by an unknown CA and that the user has elected to trust. The authority certificate store is used to store CA certificates that are used to check the validity of other certificates, for example those presented by an e-commerce



web site. The certificate stores are located in a secure area of the platform and their contents are secure and encrypted.

Connection security

Connecting securely to vital information while away from the office has never been easier. Users are in touch and in control, with secure access to the corporate network for email, applications and the intranet. However, communicating via any network carries the risk that the mobile device is attacked electronically. Guarding against electronic penetration is therefore a security issue.

Mobile workers need to be sure that they can connect to their enterprise networks safely, meaning that both ends of the communication are authenticated, and the communication is encrypted for privacy and integrity.

Nokia Eseries devices can access Internet and corporate data using different network connection types such as WLAN (wireless local area network) and GPRS (general packet radio service) interfaces, to enable network access under various conditions. Bluetooth® is available for local connectivity – for example from device to PC – to transfer files, images and other content. For security purposes, each Symbian application uses internet access points to connect to the network. Symbian platform security prevents applications from listening to each other while sending and receiving data.

Bluetooth® security

Nokia provides options for users to manage the Bluetooth® visibility of their device. For additional protection, and also to prevent unwanted connection requests, users can set the device's discoverability to 'hidden' mode. This does not impact the use of personal devices like headsets and car kits. Alternatively it is possible to blacklist arbitrary devices by adding them to the 'blocked devices' list. Bluetooth® can also be completely switched-off without affecting other functions of the device.

Wireless LAN security

Wireless LAN is challenging to protect, because the coverage area cannot be confined within walls and protected with locks and security guards. Attackers can attempt to associate with access points from neighbouring buildings or even cars in car parks or eavesdrop on all kinds of digital traffic including email, web and voice. To help ensure security from mobile devices to the access point, various WLAN authentication and encryption features can be used. Nokia Eseries devices support WEP,

WPA, TKIP, WPA2, 802.1x, Advanced Encryption Standard (AES), CCX3 and a wide variety of EAP schemes including SIM, AKA, TLS, PEAP, TTLS, LEAP and FAST.

Secure browsing

Nokia Eseries devices include a comprehensive S60 mobile internet browser. The browser uses standard HTTP protocol over TCP/IP to connect to the web. The browser supports SSL/TSL protocols for security.

For privacy, the user can choose from a number of auto-cleaning options to clear cache data, cookies, history, auto-bookmarks and stored form data including passwords entered into web forms.

Secure intranet access

Nokia Mobile VPN is an IPSec virtual private network (VPN) application developed by Nokia for S60 platform-based mobile devices. An IPSec VPN allows a user to use the mobile network and the Internet to safely connect from the mobile device to the company network. Once authentication to the company VPN is successful, all data transmitted between the mobile device and the company network occurs through an encrypted tunnel. This tunnel provides confidentiality and integrity.

Nokia Mobile VPN allows users to browse intranet pages, access links to an intranet web page embedded in an email and make VoIP calls over secure connection.

IPSec-based VPN gateways compatible with Nokia Mobile VPN include Alcatel-Lucent, Check Point, Cisco, Nokia IP VPN and Nokia Siemens Networks.

Nokia Mobile VPN supports, for example, digital certificates, username/password authentication infrastructures, RSA SecurID token or Active Directory/LDAP-based schemes for authentication. For setup instructions, please visit nokia.com/business where you can find links to the Nokia Configuration Tool used for set up, as well as instructions for different VPN headends.

Content and application security

Protecting both business and personal data stored on a mobile device is equally important. Encrypting the device and using a device lock code is a powerful way to protect against device theft or loss since an attacker will be prevented from gaining access to data via the user interface or sophisticated low level attacks at the memory storage level. Nokia uses a special application signing process to verify the origin of the application and to ensure that applications do not cause any harm to other functions on the device.

Device memory and memory card encryption

Nokia E71 and Nokia E66 introduced hardware-accelerated device and memory card encryption to the Nokia Eseries range of devices. All user-accessible files on the device memory or on the memory card can be encrypted. This includes, for example, email messages and attachments, office documents, calendar entries, and contacts. Hardware acceleration offers unprecedented speed and responsiveness of Nokia Eseries devices, despite encryption. In most daily-use cases, differences to a non-encrypted device can hardly be noticed.



Nokia E5

Advanced encryption key sharing enables teams to collaborate and share encrypted memory cards, and users to switch between devices and continue using the same memory card. Separately available OMA device management solutions allow remote management and security enforcement of device and memory card encryption.

Summary of specifications for device memory and memory card encryption:

- Encryption cipher: Advanced Encryption Standard (AES) in the XTS mode, P1619 Standard Architecture for Encrypted Shared Storage Media
- AES operations do not slow the application processor, as they are performed by a dedicated crypto co-processor
- The solution works below the file system and is therefore transparent to applications
- Cryptographic operations are performed and keys are stored on protected hardware area

- A hardware-based random number generator is used in key generation
- Encryption key length: 128 bits; Initialisation vector: 128 bits
- Key backup file format: PKCS#5 pass-phrase protected file

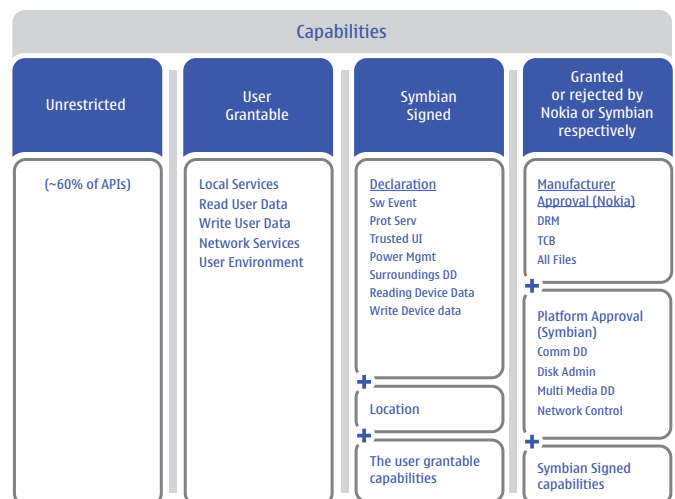
Data backup

For backing up user data from the device, users can employ Ovi Suite, which can be downloaded free of charge from www.nokia.com/ovisuite. With this convenient application, users will also be able to install maps, move music to their device and update their phone software.

Application signing

Nokia supports the Java Verified Program and the Symbian Signed application signing process. Digital signing is based on the standard Public Key Infrastructure (PKI) model. When an application is being installed on a Nokia S60 device, the application installer checks the certificate and compares it to the certificates in the device that are used in the application installation. If none of the certificates trusts the signature, the application is installed but a warning message is displayed to the user. In cases where the application has a signature that is trusted by one of the certificates used by the application installer, no warning message is displayed and the application is installed. The signature protects the integrity of the signed file. If a signed file is changed, the signature is broken and the file is no longer trusted.

Device Platform API controls



Security applications

Nokia collaborates with third party vendors to meet the specific security needs of its customers. Security applications complement the native security offering of Nokia S60 devices. Solutions such as anti-virus, personal firewall, data security and authentication are available for Nokia Eseries devices. Application developers include Cisco, F-Secure, Juniper, Kaspersky, RSA and Trend Micro. For further information about security applications and other third party business solutions, please see www.nokia.com/business.

Device management

Device management typically refers to the ability of IT departments to remotely manage, configure and update a mobile device. With device management, businesses can help users to take new services and applications in use, as well as modify the configuration of existing ones with minimal effort. It also enables the IT department to track the enterprise's inventory of devices. Device management also provides a tool to deploy and manage mobile security for all users.

Applications such as personal information synchronisation, network access and email all need separate configuration settings, making them time-consuming for end-users to configure manually. By allowing IT to automate configuration, device management offers benefits for virtually all members of the mobile value chain. It is a critical enabler for enterprises that have a large number of mobile devices, allowing efficient usage and cost-effective management.

Nokia uses Open Mobile Alliance (OMA) device management technology and has been active in OMA standardisation work. OMA device management is designed to work in the wireless environment and makes it possible to add, modify and remove parameters, to provide new services and applications, and to perform troubleshooting by identifying configuration issues. The following examples show what can be achieved with a full device management solution:

- 'Out-of-the-box' provisioning – For a new device, services and applications can be deployed and configured using device management systems
- Reactive or proactive provisioning of new service settings – Mobile users may request new settings for a service, or they can be automatically prompted to do so, for example, in the case of upgrades
- Troubleshooting – If incorrect settings cause problems for mobile users, the help desk can check the settings, determine what caused the problem, and fix it by sending the correct settings to the device

- Mass configuration – Administrators can configure services and applications across their entire fleet of mobile devices

Trust administration model (Terminal Administration Rights Model – TARM)

Symbian's trust administration model allows trust to be established between the device and the device management server, and ensures that only the authentic server is able to make changes, enforce policies or perform lock/wipe on the device. A typical example is to enforce password use and related password complexity and ageing policies.

Compatible OMA device management solutions

Nokia collaborates with OMA device management vendors who develop and market solutions that are compatible with Nokia devices. Solutions are available for both network operator and enterprise IT environments. Device management vendors include Fromdistance, InnoPath, Mformation, Nokia Siemens Networks, Perlego, Smith Micro and Sybase. For more information about device management solutions and other third party business solutions, please see www.nokia.com/business.

Managing policies for Mail for Exchange users

Mail for Exchange is the Nokia implementation of Microsoft® Exchange ActiveSync® protocol for Nokia devices. Mail for Exchange provides business users with direct access to Microsoft Exchange Server for push email and synchronisation of calendar, contacts and to-do notes. Nokia devices offer rich support for Microsoft Exchange policies and this has been a very popular and accepted way to manage mobile devices. One of the most common policies is the enforcement of device lock to ensure users cannot disable the device lock password and thus keeps sensitive corporate email data protected from unauthorised users. This Microsoft Exchange policy implementation is based on the same trust administration model described above. Supported Microsoft Exchange policies include the following:

Device lock policies:

- Require a password for device lock
- Require alphanumeric password
- Minimum password length
- Require complex passwords
- Track password history
- Password expiration days

- Maximum inactivity timeout
- Maximum password attempts
- Local wipe after maximum attempts

Device encryption policies:

- Device encryption enabled
- Require device encryption
- Require storage card encryption

Device wipe policies:

- Remotely wipe device memory and memory card (NS.confirmation email)

Other policies:

- Allow non-provisionable devices
- Allow attachment download
Set maximum attachment size that can be downloaded
- Allow synchronisation while roaming
- Allow HTML email viewing
- Allow Bluetooth®
- Allow camera
- Allow storage card
- Allow Wi-Fi

For further information about Mail for Exchange solution, please see www.nokia.com/mailforexchange.

Managing policies for IBM Lotus Notes Traveler users

IBM Lotus Notes Traveler provides a built-in set of default device preferences and security settings that an administrator can modify for use when a device initially registers with Lotus Notes Traveler.

Device lock policies:

- Configurable password strength rules
- Minimum password length
- Password requires upper and lower case
- Password requires alphanumeric characters
- Password maximum repeated characters
- No consecutive numbers allowed in password
- Password history count (0-20)

- Password expires after specified number of days (0-365)
- Inactivity time-out (minutes until the screen lock engages)
- Wrong number of passwords before the device is wiped

Storage card encryption:

Administer multi-level remote device wipe

Remote policy compliance monitoring:

- Lotus Notes Traveler client reads the server policy and compares it to the current device settings
- If violations are detected, violation action is performed
 - Enforce
 - Disable Sync
 - Report
- Device user is notified of the problem in any case, and can take corrective action

Other supported policies:

- Attachment sizes
- Mail filtering on days of email, size and importance
- Calendar filtering on past and future events
- Journal and To-do filtering on dates and status
- Selective data synchronisation

For more information about IBM Lotus Notes Traveler security functions please visit <http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp>, see Lotus Notes Traveler 8.5.1.

Nokia Configuration Tool

Nokia Configuration Tool is a PC application to locally manage settings for Nokia Eseries and other compatible Nokia devices. IT professionals and other advanced users can edit and store settings on a compatible PC and transfer them to compatible Nokia devices using Bluetooth® connectivity or a Universal Serial Bus (USB) cable.

With Nokia Configuration Tool, you can configure various settings, such as wireless LAN (if available), email, VoIP and internet access points. You can also transfer files, contact cards and applications, if available. Settings can be grouped into multiple profiles for different purposes and different types of devices.

Settings that can be managed with Nokia Configuration Tool include internet access points, email, SIP and VoIP, SyncML, add and delete applications, device encryption, Nokia Mobile VPN, Mail for Exchange, Nokia Call Connect, F-Secure and more.

Nokia Configuration Tool requires a PC running Windows 7, Windows XP or Windows 2000. Nokia Configuration Tool and Nokia Ovi Suite can be downloaded free of charge from the Nokia website. See detailed features and requirements in the Nokia Configuration Tool User Guide.

Conclusion

If mobility is to become fully adopted within the enterprise, device security and life-cycle management will need to be aligned with existing corporate policies. There is certainly no shortage of solutions for various types of wireless security threats. But to be effective, corporate IT managers must first understand precisely what threats their particular systems face and, second, identify the best solution. With years of experience in the area of security, Nokia delivers a variety of offerings with its devices to flexibly accommodate a wide range of user and network requirements.