



Windows
Mobile[®]

**Windows Mobile Devices and Security:
Protecting Sensitive Business
Information**

March 2006

For the latest information, please see www.microsoft.com/windowsmobile/

The companies and products featured in this white paper are for information purposes only and form a guide to a subset of the products available today. Microsoft does not recommend or endorse any product or company mentioned in this paper above another.

Contents

INTRODUCTION	1
THE RISKS	3
“It’s Just My Calendar!”	3
Theft/Loss.....	3
Personal Device Ownership	3
Malicious Software	4
Cracking/Hacking	5
SECURITY PRACTICES.....	6
Start with a Risk Analysis.....	6
Establish Key Security Policies	6
Automate Enforcement	7
AUTHENTICATION.....	9
ENCRYPTED DATA.....	12
ENCRYPTED CONNECTIVITY	13
Application-Level Encryption	13
Information Service Encryption	14
Network-Level Encryption	14
SECURITY MANAGEMENT	16
Replacing a Device	16
Configuration Management	16
Virus Protection	18
Lock-Down Functionality	18
Digital Signatures for Trusted Systems	18
Thin Client Connectivity.....	18
CONCLUSION	20
APPENDIX A: THIRD-PARTY SECURITY ADD-ON PRODUCTS.....	21
Authentication.....	21
Encryption	24

Security Management.....26

Introduction

Today's mobile devices offer many benefits to enterprises. By converting paper-based processes to form-based applications and extending desktop computing systems to mobile devices, products such as the Microsoft® Windows Mobile®-based Pocket PC and Smartphone can help improve the productivity of mobile professionals while also reducing operational costs.

As organizations consider mobile enterprise solutions, a key evaluation point is security. Mobile solutions need to be safe and reliable, whether they involve personal information or confidential transactions at work. Personal digital assistants (PDAs) and Smartphones can store large amounts of data and connect to a broad spectrum of networks, making them as important and sensitive computing platforms as laptop PCs when it comes to an organization's security plan. But even if a mobile device stores only an individual's calendar and contacts, losing control over this data can pose a serious threat to an organization.

When choosing a mobile computing platform on which to standardize, organizations should keep in mind that not all PDAs and Smartphones were designed with enterprise-class security in mind. The Windows Mobile software platform, however, was designed for enterprise solutions and has incorporated security options and documented programming interfaces for security applications in every generation of Windows Mobile-based devices.

To provide the highest level of security, mobile devices must be secured at six points:

- **Access to the device.** Because the small size of mobile devices makes them susceptible to being lost or stolen, devices need to be able to verify that the person attempting to access them is a legitimate user. This can be done by using a password, a biometric such as a fingerprint reader, or a physical token like a smartcard or a SecurID token.
- **Access to data at rest (stored data).** The storage cards that fit into the expansion slot of a Pocket PC or Smartphone can store anything from a few hundred megabytes up to five gigabytes or more. While this data storage capacity is a key enabler for data-intensive enterprise applications, it also heightens concern about all this data falling into the wrong hands.
- **Access to data in motion (over the networks).** Wireless connectivity achieved through expansion cards, external jackets, or integrated wireless chips provides access to sensitive business information stored on personal, local, and wide area networks. Security is needed at this point to help prevent unauthorized access to information stored on these networks.
- **Access to the corporate network (stored credentials).** While mobile devices used to access corporate resources may not directly expose any interesting data to attackers, they can still provide a valuable cache of credentials that can be used in other attacks. These credentials must be securely stored and made resistant to recovery attempts.
- **Viruses, spyware, and malware.** As mobile devices incorporate increasingly sophisticated network stacks and protocol suites, they must be prepared to handle incoming traffic as well as outbound connections. These devices must have proper firewall, anti-virus, and anti-spyware defenses.
- **Access to mobile applications.** Corporate IT departments need to be able to exert the same degree of control over mobile applications that they do over desktop and laptop applications. This level of control requires the ability to designate trusted and non-trusted applications and specify how they may interact with the mobile device.

This paper looks at the typical security risks related to mobile devices and shows how they fit into one of the six categories above. It provides an overview of security policies and

procedures for mobile devices, and then presents the different technologies and applications that enable Windows Mobile-based devices to help counter the security risks detailed above.

The Risks

This section examines the various types of risks that can threaten the security of mobile devices and relates them to the six security points presented in the previous section.

“It’s Just My Calendar!”

(access to data at rest)

Many mobile devices enter the enterprise through the back door: employees purchase these devices at retail stores and bring them into their workplace. Often the initial need is simply to easily access their calendar and contacts information. Some organizations consider mobile devices a security risk only if they have a business application installed. However, this type of incident represents a threat to stored data.

It’s worth considering what would happen if an employee’s calendar fell into the hands of a competitor or became public knowledge. For example, the notes in an executive’s calendar can describe the background of different meetings, which could range from fixing internal problems to addressing customer issues—or even to merger and acquisition discussions. At best, it could be embarrassing if this information were to become public. Contact information can also be valuable to an organization and cause problems if it falls into the wrong hands. That’s why organizations should give serious consideration to security protection for *all* their employees’ mobile devices, regardless of whether they are running business applications or “just” calendar and contacts information – important data that can have great value.

Theft/Loss

(access to the device; access to data at rest)

Industry estimates indicate that hundreds of thousands of cell phones and handheld devices are left behind or lost every year. And as the number of Smartphones and PDAs increases, the potential for information to fall into the wrong hands also increases. This type of incident represents both access to the device and to the data stored on it.

The problem with a stolen or lost device is twofold. First, the user may no longer be able to work efficiently until a new device can be supplied and set up. Second, the data stored on the device may be of value to competitors and criminals.

Organizations also need to consider the legal aspect of a stolen device. In many countries, if a device used to store confidential information (such as medical records) is stolen, the owner of the data could be liable for its loss and misuse under data protection laws.

Personal Device Ownership

(access to data at rest; access to data in motion; access to the corporate network; viruses, spyware, and malware)

Personal ownership of mobile devices moves control away from the IT manager and firmly into the hands of the employee. When data belonging to the corporation resides on a device owned personally by an employee, a clear conflict of interest can arise—one that can have adverse effects on corporate data security. Consider, for example, cases such as the following:

- When the device is privately owned and a disgruntled employee is suspected of stealing sensitive data or acting maliciously, the company could have to resort to expensive legal action to confirm this suspicion. While this issue is related to all personal computing devices, the amount of data that can be stored on mobile devices—especially those with removable data storage cards—is substantial.

- If the device has a number of connectivity options installed, the user is free to connect with a variety of public networks. This could lead to system damage—for example, from the propagation of malicious code—the next time the user connects to the corporate network. Also, if the user's connection to the organization's network uses clear text transmissions rather than end-to-end encryption and authentication, the organization's data as well as sensitive corporate credentials (such as network or file-sharing passwords) could easily be compromised.

Because different types of network connections require different security setups, mobile devices need multiple types of connectivity protections. For example, mobile devices connecting to virtual private networks (VPNs) over wide area networks (WANs) need to be able to encrypt transmissions using Secure Sockets Layer (SSL) technology; those connecting over local area networks (LANs) using the 802.11b/g protocols need either Wi-Fi Protected Access (WPA) or Wired Equivalent Privacy (WEP) security, preferably in conjunction with the 802.1x authentication protocol. Those connecting through a Personal Area Bluetooth connection need Bluetooth security technology.

One way to address this issue is for IT managers to bring handheld computing within the corporate fold—that is, to insist that every device connecting to or exchanging data with the organization's network follow clear security policies. [Hewlett Packard](#), for example, offers a [security add-on](#) for Pocket PC that can prevent partnering and syncing with non-approved computers. Symbol Technologies also offers add-on security software for their Pocket PC.

Note that system security is not just about implementing technology. It is about raising employee awareness of the threat from lost devices, lost business data, and lost personal data and about putting organizational processes and procedures in place to protect against this threat. It is about finding safe ways to allow users to access the applications and data they need so that they work with security measures instead of against them. (See section on [Security Practices](#), below.)

Malicious Software

(viruses, spyware, and malware; access to the corporate network; access to mobile applications)

Although Microsoft Windows Mobile-based devices have yet to become a significant target for malicious code, one may argue that it is only a matter of time before such threats occur. Also, even if the devices themselves are not affected by such code, when they connect to a network they can serve as transport mechanisms for passing destructive software on to other computing systems.

Malicious software can take a number of forms, including viruses, Trojan horses, and worms. Viruses are usually propagated through some kind of user-initiated action, such as opening an attachment or running a script or application. They attempt to spread undetected through the system by attaching themselves to other files. Trojan horses are programs that masquerade as genuine applications in order to perform some unauthorized activity once they gain access to a user's system, such as install spyware or allow remote attackers to control the device. Worms actively work their way through a system and look for other systems to infect, often causing denial-of-service (DoS) attacks.

It is important to note that while not all malicious software is deliberately designed to take destructive actions such as deleting data, they are often poorly designed and coded and cause unintended damage to infected systems. Another form of collateral damage, unauthorized data disclosure, has the potential to cause serious legal liability under regulatory compliance scenarios.

Cracking/Hacking

(access to the device; access to data at rest; access to data in motion; access to the corporate network; access to mobile applications)

In addition to being vulnerable to unauthorized access on their own, mobile devices also provide a route into the systems with which they connect. By using a mobile device to appear to these systems as a registered user, a would-be cracker is then able to steal data or compromise corporate systems in other ways.

Another threat comes from the practice of port scanning. First crackers use a DNS server to locate the IP address of a connected computer (either the mobile device itself or a gateway server to which it connects). Then they scan the ports on this known IP address, working their way through its TCP/UDP stack to see what communication ports are unprotected by firewalls. For instance, File Transfer Protocol (FTP) transmissions are typically assigned to port 21. If this port is left unprotected, it can be misused by attackers.

Protecting against port scanning requires software that traps unauthorized incoming data packets, thereby preventing a mobile device from revealing its existence and identity. A personal firewall on a Pocket PC or Smartphone device can be an effective protective screen against this form of attack for users connecting through a direct Internet or Remote Access Server (RAS) connection. For situations where all connections to the corporate network pass through a gateway, placing the personal firewall on the gateway itself is the simplest solution, as it avoids the need to place a personal firewall on each mobile device. In either case, deploying secure access methods that implement strong authentication keys will provide additional protection. These methods are discussed further below, in the section on [Authentication](#).

Security Practices

Organizations using mobile devices should establish security practices at a level appropriate to their needs, subject to legal and other external constraints. Some organizations will implement security procedures and tools extensively, while others will place more value on cost and convenience.

Whichever approach an organization chooses, it's important that the effort start with a CEO, president, or director, who takes security seriously and communicates that throughout an organization. The best security technology features are worthless if there is no organization policy or automated enforcement to ensure that they are actually used. In some cases, for example, senior executives have been given special access rights to the corporate network which can circumvent standard security procedures.

Start with a Risk Analysis

Risk analysis, perhaps undertaken in cooperation with a specialist consultant, will help organizations identify the appropriate levels of security for each potential risk area. Once the risk analysis has been completed, the technical design work can start. This step will identify and implement the policies, procedures, products, and technologies that will establish the desired level of security. In performing your security assessment, design, deployment, and ongoing management, you may want to follow one of the established standards-based approaches, such as [ISO 17799](#) or the [British Standard 7799](#).

As you identify each risk, determine what type of threat it represents. This allows you to correctly identify what countermeasures to take to mitigate the risk.

Establish Key Security Policies

Once you have established your risks, you need to take the appropriate steps to neutralize or mitigate those risks. Although many of your solutions will involve the application of technological countermeasures, you should first establish key security policies that govern your security efforts. These policies provide a foundation that helps ensure you are addressing your risks thoroughly, addressing the highest-priority threats first before moving on to lower-priority risks.

Microsoft recommends that organizations concerned about the security of their data set mobile device security policies. The following examples represent a typical set of policies and the areas you should ensure they address:

- **Passwords.** All mobile devices should have power-on passwords enabled, similar to an organization's standards for laptop computers. Any devices that do not have a power-on password activated should be blocked from accessing a private network. Systems management products can automate this password check and blocking function, as well as help to enforce other corporate security policies. More rigorous authentication can be achieved with SecurID cards, biometric fingerprint systems, signature authentication systems, pictograph passwords, or smart cards. If the organization chooses not to require authentication to access the device itself, it should at least prohibit mobile device users from storing their enterprise network access passwords on the mobile device (including passwords for a dial-up connection to a Remote Access Server and for accessing e-mail servers). It's also a good idea to encourage users to have the device display their owner information when powered on, to speed the return of lost devices. New capabilities within Windows Mobile 5.0 allow the creation and enforcement of password policies, including the ability to remotely or locally wipe stored data if an unauthorized user attempts to access the device. Windows Mobile 5.0 also provides the option to use secure digital certificates for synchronization with the

corporate Exchange account, removing the need for network credentials to be used for e-mail.

- **Antivirus software.** Mobile devices should have antivirus software installed to help prevent viruses from being vectored into the corporation—either as e-mail attachments or through file transfers. See a list of third-party anti-virus offerings in Appendix A.
- **Encryption.** Organizations should evaluate encryption options for protecting data—on the device itself, on external storage cards, and over networking links, including Point-to-Point Tunneling Protocol (PPTP) and IPsec/Layer 2 Tunneling Protocol (L2TP) VPN connections over a wireless link through the Internet. Worldwide organizations should use Cryptographic Application Program Interface (CryptoAPI)-enabled encryption technology to help achieve a consistent security level across international boundaries. Windows Mobile 5.0 provides expanded support for cryptographic standards (including support for AES-256 and PFX/PKCS12, and it has achieved FIPS (Federal Information Processing Standard) 140-2 certification.

Note that the static WEP key is not an effective form of encryption for users connecting over a wireless LAN, as it can easily be circumvented. Microsoft recommends the combined use of more rigorous wireless LAN authentication and encryption technologies such as 802.1x and WPA. Other protocols, such as HTTP, should be protected through the use of SSL.

- **Need-to-know data storage.** Rather than putting all of an organization's data on every mobile employee's device, it may be possible to put only a small subset on each individual's device, based on the information their job role requires. For example, Microsoft SQL Server™ 2005 Mobile Edition (SQL Mobile) enables a small portion of a partitioned SQL Server database to be synchronized with a Pocket PC and stored in an encrypted format. This approach can be beneficial in a number of ways: it keeps unnecessary data from getting in the way of employees accomplishing their tasks quickly; it helps reduce synchronization time; and, from a security perspective, it exposes less data.
- **Application installation and execution model.** Permitting users to install and execute any applications is a risk. Using the new security policy features of Windows Mobile 5.0, devices can be configured to help enforce application trust and privilege levels by use of code signing. These policies can require applications to be signed by trusted certificates and, on devices that support the two-tier functionality, can distinguish between privileged and unprivileged actions, including desktop computers that attempt to synchronize with the device.

Although you might only have a single policy, or break up your policies in a fashion different from that described, your policies should cover all of the points presented above.

Automate Enforcement

In addition to establishing security policies, it's also necessary to automate enforcement. There are many mechanisms and solutions to help administrators create, deploy, and enforce their policies, in addition to the built-in code signing and privilege features mentioned previously.

Windows Mobile 5.0 can be combined with Microsoft Systems Management Server 2003 (SMS) to provide a centralized mobile device provisioning, management, and policy enforcement solution. In addition, there are numerous third-party systems management solutions. These solutions enable a centralized IT organization to maintain an asset inventory of the devices that connect to the corporate network and to automatically fix configuration settings and distribute software updates as they become available. For a sample list of systems management solutions for Windows Mobile-based devices, please

visit the [Windows Mobile Solutions Provider](#) Web site and search the Software Solutions section under the Systems Management category. The IT Management category in the Vertical Market Solutions section may also be of interest.

Windows Mobile 5.0 devices with the Messaging and Security Feature Pack (MSFP), combine with the advanced mobility features in Microsoft Exchange Server 2003 Service Pack 2 (SP2) to provide support for both local and remote data wipe in the event that managed devices are lost or compromised, as well as to automatically enforce compliance with password and automatic device locking policies.

One more technique for automating enforcement of an organization's security policy is to provide a critical internal utility, such as an employee directory, which checks that the device settings are in compliance. If they are not, this utility can help do any of the following:

- Automatically change the settings to be in compliance.
- Prevent the device from functioning until its settings are in compliance.
- Send a message using e-mail or Short Message Service (SMS) to IT, highlighting the policy violations.
- Wipe all sensitive data from the device.

The advantage of this approach is that devices that do not connect to the corporate network on a regular basis can continue to be checked for policy compliance.

Finally, low-deductible insurance coverage is available for mobile devices. The Signal, a large wireless phone insurance provider, offers underwritten by the Insurance Company of North America (INA); other insurance companies offer similar coverage.

Authentication

The first step in securing information on a handheld device is to protect the device against unauthorized access. Various mechanisms are available to identify and authenticate users. To achieve a high level of security, Microsoft recommends that you use two out of the following three approaches (an approach that is often referred to as two-factor authentication):

- 1) Something the user knows (for example, a password).
- 2) Something the user has (for example, a security certificate in a smartcard or a SecurID token).
- 3) Something that is part of the user (for example, a fingerprint).

In certain cases, additional authentication may be required. These include:

- Applications that require user authentication before they will run. This requirement may apply if the application hasn't been used for a certain amount of time, or it may occur on a repeating basis (for example, every 15 minutes).
- A data storage card that has its own authentication mechanism to decrypt its data.
- Additional authentication for accessing an organization's private network. For example, the Microsoft Exchange Server 2003 uses Windows® Active Directory® authentication to provide access to corporate e-mail, calendar, and contacts from mobile devices. In Exchange Server 2003 Service Pack 2 (SP2), devices can instead use a digital certificate for authentication to remove the need for the user to provide their network credentials. This reduces the risk that the user's credentials will be compromised. See the section on [Information Service Encryption](#), below, for more information about Exchange 2003 security.
- An additional log-on step for accessing a protected shared file server.
- Additional sign-on credentials to access certain Web sites.

Authentication options available in Windows Mobile 5.0 software include:

- **Perimeter security.** Other protections against unauthorized access to the devices available in Windows Mobile software include several forms of physical device security technology:
 - **Power-on passwords.** Pocket PC 2003 and Smartphone 2002 both support four-digit power-on passwords for helping protect access to the device, and the Pocket PC 2003 also supports strong alphanumeric power-on passwords—that is, passwords requiring at least seven characters, including a combination of uppercase and lowercase letters, numerals, and punctuation. A four-digit password can also be associated with the phone card (Subscriber Identity Module) for GSM devices. For greater protection, all passwords are hashed (converted into a different form, making them harder to break) before being stored. Even if an attacker copies the hashed form of the password, it is infeasible to work backwards and get the original password. When a user attempts to access the device with an incorrect password, the system imposes a time delay before allowing access again—a delay that increases exponentially with each attempt. In addition, the Pocket PC File Explorer software requires user authentication for accessing shared Windows-based file servers. For further protection, an organization can set up automatic enforcement of its authentication policies using centralized management software, as discussed below in the section on [Configuration Management](#).

- **Cabinet (.cab) file signing.** This uses third-party software to digitally sign a file using an X.509 digital certificate. This provides a way to determine the origin of the file and whether the file has been altered after it was signed.
- **Secure device management technology.** This enables over-the-air changes to be made in a way that helps protect against hackers. Most Windows Mobile devices that include wireless data functionality include some degree of secure device management to help prevent arbitrary applications from being downloaded and executed over the air.
- **Application-level security** (for example, for such applications as Microsoft Internet Explorer Mobile, ActiveSync®, e-mail attachments, and infrared beaming). This type of security can use any of a number of approaches, ranging from requiring users to enter their password in order to gain access to an application, to authentication mechanisms such as biometrics or smartcards. The requirement could be set up to apply to each access attempt, to apply only when the application hasn't been used within a certain time period, or to require reauthorization every so many minutes.
- **Network/Internet access.** Pocket PC and Smartphone software also includes built-in authentication capabilities for accessing corporate networks and restricted Internet sites. These protection features, together with other security options, are designed to prevent the most likely security issues related to Pocket PC and Smartphone use, including spoofing, tampering, information disclosure, and denial of service. They include:
 - **Kerberos support** for connections to corporate resources in a Windows Active Directory domain.
 - **Dial-up authentication** using Windows NT® LanManager Challenge/Response (NTLM) support for legacy application compatibility.
 - **Support for multiple networking and authentication protocols for accessing secure Web sites**, including SSL 3.1 and Private Communications Technology (PCT) as well as Wireless Transport Layer Security (WTLS) class 2 for accessing secure Wireless Access Protocol (WAP) sites.
 - **Authentication for Virtual Private Networking**, using PPTP or IPSec/L2TP, as well as integration of the Challenge Handshake Authentication Protocol (CHAP and MS-CHAP versions 1 and 2) and Password Authentication Protocol (PAP), over network connections using Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP).
- **Certificates.** Windows Mobile 5.0 software supports X.509 certificates, which provide a means for authenticating applications, users, operators, and servers. The certificates may be securely stored, managed, and deleted on the mobile device.

Table 1 summarizes the native authentication functionality available in the Pocket PC and Smartphone software.

Table 1: Microsoft Authentication Functionality

Feature	Pocket PC	Smart-phone
Automatic 4-digit device password option, with passwords hashed before being stored	X	X
Automatic strong password option (with 7 or more alphanumeric and punctuation characters)	X	
SIM lock for GSM devices	X	X
SSL 2.0, TLS, and PCT secure Web site authentication	X	X
Windows NT LAN Manager (NTLM) Challenge/Response dial-up network authentication	X	X
Kerberos support for authentication with Active Directory domain resources	X	X
Network file-share password authentication in File Manager	X	
PEAP and EAP-TLS authentication for 802.1x	X	X
CHAP, MS-CHAP version 1 & 2, and PAP Virtual Private Networking authentication	X	X
WTLS class 2 support for Pocket Internet Explorer, enabling the browser to view secure WAP sites	X	X
.CAB file signing	X	X

See Appendix A for a list of third-party authentication add-on products.

Encrypted Data

Pocket PC and Smartphone data can be stored both in the device's Random Access Memory (RAM) and in external [storage cards](#), such as Secure Digital/Multimedia cards (SD/MMC), CF cards, and PC storage cards. These storage cards can handle from hundreds of megabytes up to five gigabytes of data; some external storage options can even hold up to [60 gigabytes](#). Either way, there are a number of ways to encrypt the stored data in order to help protect it from unauthorized access.

For Pocket PCs, Microsoft offers a mechanism for storing encrypted data in a relational database. This data, stored in [SQL Server 2005 Mobile Edition](#), is protected with both 128-bit encryption and password support. SQL Mobile is a compact database for rapidly developing applications that extend enterprise data management capabilities to mobile devices.

See Appendix A for a list of third-party data encryption add-on products.

Encrypted Connectivity

Encryption is sometimes desired not only for data stored on a mobile device, but also to protect data and communications that pass through networks. This encryption can be done by an application, by an information service, or by the network itself.

Application-Level Encryption

To help protect data from unauthorized access, mobile devices must support industry-standard 40-bit, or better, 128-bit encryption or be able to use other encryption techniques accessible to developers through the industry-standard CryptoAPI.

Microsoft is developing tools and technologies to support encrypted applications using the .NET Compact Framework—a development platform that brings managed code and XML Web services to smart devices and enables them to execute secure, downloadable applications. One such tool is the High Encryption Pack for Pocket PC, which can be used with applications that support 128-bit cryptography with CryptoAPI. The .NET Compact Framework also includes support for [encryption classes](#) to help protect application data during sensitive operations such as e-commerce.

The Windows Mobile platform provides a range of encryption algorithms for different types of application and networking needs. These include:

- Stream-based encryption algorithms, including RC2 and RC4 (both 128-bit key strength).
- Block cipher encryption algorithms, including AES-256 (256-bit key strength), 3DES (112- and 168-bit key strength), and DES (56-bit key strength).
- One-way hashing algorithms, including MD2, MD4, and MD5 (all 128-bit key strength), SHA-1 (160-bit key strength), MAC (128-bit key strength), and HMAC (128-bit key strength).
- Digital signature encryption using the RSA public-key algorithm (1024-bit key strength).

In addition, Windows Mobile 5.0 software supports 128-bit encryption strength for the CryptoAPI, which developers use to integrate encryption into their applications and communications. Now that the U.S. government has relaxed export restrictions for the strength of encryption technology from 40-bit to 128-bit encryption, Microsoft has incorporated this technology into the Windows Mobile platform. This functionality is also available as an add-on to earlier Pocket PCs using the [High Encryption Pack](#).

Table 2 lists the application-level encryption functionality available from Microsoft. See Appendix A for a list of third-party application-level encryption add-on products.

Table 2. Microsoft Application-Level Encryption Functionality

Feature	Pocket PC	Smart-phone
128-bit encryption strength for applications that take advantage of 128-bit cryptography and the CryptoAPI (built into Windows Mobile, Pocket PC 2003, and Smartphone 2002 software; available through the High Encryption Pack for older Pocket PCs)	X	X
NET Compact Framework encryption classes for application data	X	X
Various encryption algorithms, including stream-based 128-bit algorithms (RCE 2, RC4); block cipher algorithms (AES-256 at 256 bits, 3DES at 112 and 168 bits, and DES at 56 bits); one-way hashing algorithms (MD2, MD4, MD5, MAC, and HMAC at 128 bits and SHA-1 at 160 bits); and the RSA public-key algorithm at 1024 bits	X	X

Information Service Encryption

[Microsoft Exchange 2003](#), with integrated Exchange ActiveSync (EAS), provides technology for encrypting e-mail, calendar, and contacts data and for synchronizing this data between the server and a Windows Mobile-based device, as well as enabling mobile devices to browse the Internet over an encrypted link. Exchange Server 2003 SP2 broadens this support to allow greater management of Windows Mobile 5.0 devices that have the MSFP installed, including push synchronization, certificate-based authentication, and remote wipe functionality. In previous versions of Exchange, mobility functionality was provided by Mobile Information Server 2002.

As a best practice alternative to locating your front-end Exchange 2003 servers in the perimeter network, deploy Microsoft Internet Security and Acceleration (ISA) Server. ISA Server acts as an advanced firewall that controls Internet traffic entering your network. When you use this configuration, you put all of your Exchange 2003 servers within your corporate network and use ISA Server as the advanced firewall server exposed to Internet traffic in your perimeter network. To help protect outbound and inbound mail, deploy SSL to encrypt messaging traffic. Details about deployment architectures and setting up SSL are provided in the [Exchange 2003 Deployment Guide](#).

Due to the range of encryption technologies available in today's mobile devices, Exchange 2003 uses a combination of encryption technologies to achieve an end-to-end encrypted connection. These include:

- **128-bit, end-to-end SSL encryption** when synchronizing calendar, contacts, and e-mail to a Windows Mobile-based device.
- **WTLS encryption** when using a WAP-enabled browser to connect to Outlook Mobile Access (OMA), or 128-bit SSL encryption when using a conventional web browser to directly access the OMA application.

Network-Level Encryption

To help protect data transmitted over the Internet and wireless networks, mobile devices need not only application-level and information service encryption, but also network-level encryption. This level of encryption includes:

- **VPN protocol support.** Devices using a VPN protocol, such as PPTP or IPSec/L2TP, to connect to the Internet through a corporate server need to

encrypt the data before transferring it. Support for PPTP and IPSec/L2TP connections is built into Connection Manager in Windows Mobile-based devices. Additional VPN protocol support is available from third parties, as well as through an integrated personal firewall (see Appendix A).

- **Encryption for accessing secured Web sites.** The Internet Explorer Mobile Web browser included in Pocket PC and Smartphone software uses 128-bit SSL (https) and PCT encryption technologies to access secured Web sites. In earlier versions, the High Encryption Pack may be required to upgrade from the native 40-bit encryption to 128-bit encryption. In addition, Windows Mobile-based devices offer WTLS class 2 support for accessing secure WAP sites.
- **Encryption for wireless LAN connectivity.** The static shared-key WEP algorithm has been easily defeated by researchers at the University of California, Berkeley. This means alternative approaches are necessary to securely connect mobile devices over 802.11b/g wireless LANs. Three alternatives are available:
 - **VPN.** This approach enables mobile devices using 802.11b/g to connect to an organization's network over the Internet, with VPN security software providing user authentication and a strongly encrypted connection.
 - **802.1x.** Windows Mobile 5.0 software supports 802.1x technology for wireless LANs, including the Extensible Application Protocol-Transport Layer Security (EAP-TLS) algorithm for certificate-based authentication and the PEAP (Protected Extensible Authentication Protocol) algorithm.
 - **WPA.** Windows Mobile 5.0 includes built-in support for WPA.

Table 3 shows the network-level encryption available from Microsoft.

Table 3. Microsoft Network-Level Encryption Functionality

Feature	Pocket PC	Smart-phone
PPTP VPN protocol support enables Windows Mobile-based devices to connect to private networks through the Internet.	X	X
128-bit SSL (https) and PCT encryption is built into the Pocket Internet Explorer Web browser.	X	X
128-bit SSL encryption is available by using the Crypto API.	X	X
SSL support is built into the Inbox on Windows Mobile-based devices, encrypting communications to IMAP, POP3, and SMTP servers.	X	X
802.1x technology for wireless LANs supports EAP-TLS and PEAP authentication algorithms.	X	X
IPSec/L2TP VPN support enables Windows Mobile-based devices to connect to private networks through the Internet.	X	X
WTLS class 2 support enables Internet Explorer Mobile to view WAP sites that use this technology.	X	X

See Appendix A for a list of third-party network-level encryption add-on products.

Security Management

Until an organization sets a mobile computing standard, it is difficult to enforce security policies. Once a mobile device standard is in place, tools are available to assist organizations in centrally managing corporate-wide deployments. This section identifies products that enable IT organizations to efficiently support their mobile professional customers.

Replacing a Device

Microsoft recommends setting your organization's mobile devices to display owner information upon power-up. That gives them the best chance of being returned if they are lost.

From the mobile user's perspective, the main goal when a mobile device is lost or stolen is to get up and running quickly. If security policies for authentication and encryption are in place and enforced, there should be little concern about the missing device beyond the replacement cost.

Here are some techniques for getting a new device set up quickly to the last backed-up state of the missing device:

- **Backup file.** A number of products are available to perform a complete backup of a mobile device (see Appendix A). If a full restore from a backup is not needed, the AutoRun capability on storage cards enables applications to be automatically installed on a mobile device when the storage card is inserted into the device (subject to application and execution policy controls).
- **Data on the user's PC.** The [ActiveSync](#) software that comes with Windows Mobile-based devices can restore data from the old mobile device that is still retained on a PC to the new device.
- **Data on network servers.** The new device can use the pass-through feature in [ActiveSync](#) to connect to network servers and synchronize data with them.
- **Restore process on secure organization Web page.** Organizations can provide a secure Web page with instructions for setting up a new device. The new device can download a standard device image file (made using a product like [Sprite Clone](#)) to automatically set up the core configurations and install any business or administrative applications. The user can then synchronize the device with corporate servers to restore data.

See Appendix A for a list of third-party backup/restore products.

Configuration Management

Windows Mobile-based devices include a Configuration Manager facility for easily transferring security settings to mobile devices. This management component offers several benefits:

- Enterprises can use it to configure devices to connect through the appropriate protocol—for example, GPRS (General Packet Radio Service), WAP, or CSD (Circuit Switched Data)—thereby saving users the time and trouble of trying to configure their own devices.
- Mobile operators can use it (with the appropriate security permissions) to configure connectivity settings over the air.

- Independent software vendors can use it to programmatically configure connectivity settings on mobile devices.

One method for transferring security settings to mobile devices is **.CAB provisioning**. .CAB (Cabinet) files are often used in conjunction with installing new software. Pocket PCs and Smartphones can have their settings configured through .CAB files, which can either be located on removable media cards (such as CF or Secure Digital cards) or downloaded from a Web site. The Pocket PC and Smartphone [Software Development Kits](#) (SDKs) provide details on how to do this.

Using Configuration Manager, Pocket PC and Smartphone software can enforce the following security settings for installation and execution privileges:

- **Privileged trust.** The application has full access to the system resources and APIs.
- **Unprivileged trust.** The application has limited access to the system resources and APIs.
- **Untrusted.** The application is not permitted to load and execute on the system and has no access to system resources or APIs.

Windows Mobile-based devices can also help enforce:

- **Security policies.** Security policies give organizations the flexibility to control how secure the device is, from no security to high security. The policies are defined globally and enforced locally, on each device. Security policies are used to help enforce security settings, such as authentication, through security role assignments and certificates (see next two bullets below). Smartphones come with a default, built-in security policy document. Organizations can also create their own security document using a signed XML file. Once loaded onto the device, security policies are enforced at critical points across the architecture of the device, often interacting with Configuration Manager and device security settings.
- **Security roles.** Security roles provide a means of specifying the levels of access a user has to device resources, such as registry keys, files, settings, and APIs. Examples of roles include:

Manager—the highest level of authority.

OEM—for the device manufacturer.

Operator—for the mobile operator.

See the [Windows Mobile SDK](#) for more details.

- **X.509 Certificates.** These certificates provide a means to authenticate applications, users, operators, and servers. Windows Mobile-based devices store, manage, and delete the authorities for X.509 certificates.

Third-party systems management products are also available. Some provide inventory-management functions for mobile devices, including tracking device settings and software version levels. This information can be used to automate updates or changes to a device the next time it connects to the organization's network. Others provide centralized security systems that enforce how, when, and what a mobile device can access on an organization's network. These tools can enforce such security policies as how many wrong passwords can be entered before a device is locked down—or, in some cases, has all its data erased.

See Appendix A for a list of third-party systems management products.

Virus Protection

The biggest virus threat that mobile devices pose today is passing viruses into a corporate network. This can take place through files that are attached to e-mail messages or copied and pasted onto network file servers.

Microsoft has worked closely with the anti-virus software community to provide programming interfaces that enable their products to more easily detect and remove known viruses. Look for anti-virus solutions that run natively on the mobile device.

See Appendix A for a list of third-party anti-virus products.

Lock-Down Functionality

Some organizations wish to restrict or turn off some of the functionality on mobile devices in order to meet their security requirements. As indicated in Table 4, Smartphone comes with a Prevent Memory Card Auto-Run function that can prevent applications on memory cards from automatically running or installing.

The Windows Mobile 5.0 Local Authentication Subsystem (LASS) provides a comprehensive and expandable device lock platform that can be triggered from within applications instead of just during device power-on. LASS helps protect the device from brute force attacks by providing an exponential back-off delay in response to repeated failed authentication attempts. Additionally, OEMs, ISVs, and developers can develop additional Local Authentication Plug-ins (LAPs) that extend the LASS and provide additional authentication functionality. The built-in Password LAP provides the same password functionality that was present on pre-Windows Mobile 5.0 devices.

Table 4. Microsoft Lock-Down Functionality

Feature	Pocket PC	Smart-phone
Prevent Memory Card Auto-Run can prevent applications on memory cards from automatically running or installing.		X
Exponential back-off protection against brute-force authentication attacks.	X	X
Programmatic and extendable authentication through LAP modules.	X	X

See Appendix A for a list of third-party lock-down products.

Digital Signatures for Trusted Systems

Enterprises are adopting trust-based security systems to conduct electronic business as well as to help protect software and files that are distributed to remote mobile devices. Public Key Infrastructure (PKI) enables organizations to deploy digital certificates, which can be used in a variety of ways—for example, for digital-signature-based user login, or to digitally sign files and software distributed to mobile devices. See Appendix A for a list of third-party PKI toolsets.

Thin Client Connectivity

In some cases, an organization might need a way for mobile users to access software or data without placing it on a mobile device. This is particularly true in vertical industries with sensitive data, such as healthcare, government, financial services, and manufacturing. In other cases, organizations may prefer to avoid the overhead of maintaining current versions of software on

intermittently connected mobile devices. A thin client architecture is the solution in both cases. The built-in Terminal Services client in the Pocket PC software offers this option, giving mobile device access to applications running on a Windows server. See Appendix A for a list of third-party thin client products.

Conclusion

Mobile devices, which can offer the benefits of improved employee productivity and reduced operational costs, also potentially represent security risks. These devices can store large amounts of sensitive data, which could cause harm if accessed by unauthorized users. Mobile devices also have the potential to provide unauthorized users with access to corporate networks and to introduce viruses and other harmful software into these networks. For these reasons, it's important for organizations to create a set of clear security policies and automate their implementation to the highest degree possible, to ensure their consistent and vigilant application. It's also important to select a mobile platform that supports strong security.

Windows Mobile-based Pocket PCs and Smartphones, designed from the ground up for enterprise use, offer a wide range of security options, enabling organizations to protect both their sensitive data and their networks. The rich Windows Mobile platform, which includes a multi-tasking operating system, extraordinary processing power, fast clock speeds, larger data storage capacity, and broad connectivity options, also offers strong security protection. In addition, a wide range of third-party security software and peripheral products are available. Together, these built-in security features and third-party options give Windows Mobile-based devices a high level of security protection, while at the same time providing a platform on which enterprises can standardize their mobile business applications.

Appendix A: Third-Party Security Add-on Products

Authentication

Add-on products available from a number of security vendors provide additional authentication functionality, including:

- Signature authentication.
- Picture-based passwords.
- Fingerprint authentication.
- Smart card security certificate authentication.
- SecurID card authentication.
- Certificate authentication on a storage card.
- Legacy host access.

The following tables list some of the companies that offer authentication products for the Pocket PC and Smartphone. Microsoft lists these products for informational purposes only and does not in any way endorse them.

Table 5: Third-Party Signature Authentication Products

Company	Product
Certicom Corporation	Security Builder provides a complete suite of algorithms, making it easy for developers to integrate encryption, digital signatures, and key exchange mechanisms into applications.
CIC-PenOp	iSign Suite is a software development kit for implementing systems using electronic ink or handwritten signatures.
PGP Corporation	CryptoEx Pocket supports encryption and digital signatures on mobile devices, including e-mail as well as encrypting and signing sensitive files.
Romsey Associates Ltd.	PDALok uses Dynamic Signature Recognition to enable only the rightful owner to access a Pocket PC.
Transaction Security, Inc.	Crypto-Sign uses biometric pattern recognition technology to enable a user to enter a secret sign (with no display or inking) that provides access to the device.
VASCO	Digipass offers strong authentication and digital signatures for Pocket PCs.

Table 6. Third-Party Products for Enhanced Password Protection

Company	Product
Asynchrony.com	PDA Defense for the Pocket PC provides auto-lock functionality and erases the data on the device if too many incorrect passwords are attempted—or if the synchronization process is not run within the required window of time.
Bluefire Security Technologies	Bluefire Mobile Security Suite provides centrally managed password enforcement and block-on-tampering features like "device wipe" and "device quarantine".
Hewlett Packard	Security enhancements for the Pocket PC provide support for alphanumeric passwords that are hashed before being stored. If an incorrect password is entered a predetermined number of times, the system memory is erased. This product can also help prevent partnering and synching with non-approved PCs.

Table 7. Third-Party Pictograph Authentication Products

Company	Product
Pointsec Mobile Technologies	Pointsec's picture-based authentication software enables users to select a password consisting of a combination of icons. Upon power-on, icons are displayed in random order. After a preset number of bad passwords are attempted, the device will be locked down, requiring assistance from an IT administrator to re-enable it.

Table 8. Third-Party Fingerprint Authentication Products

Company	Product
Hewlett-Packard Company	The HP iPAQ h5550 Pocket PC includes a biometric fingerprint reader that can be used by itself or in conjunction with a PIN to provide a choice of authentication approaches.

Table 9. Third-Party Products for Card-Based Authentication

Company	Product
Axalto (formerly Schlumberger)	The Reflex 20 PCMCIA Smart Card Reader provides smartcard access for Windows Mobile devices that support PCMCIA cards.
Access Mobile Communications	Blue Jacket is a line of HP iPAQ Pocket PC jackets that incorporate combinations of a Smart Card reader, Type II CF card slot, Bluetooth module, and digital camera.
ProActive	SpringCard-CF is a Compact Flash Smart Card reader for Pocket PCs.

Table 10. Third-Party Products for Storage-Card-Based Certificate Authentication

Company	Product
JGUI	AccessRights can lock or unlock access to a Pocket PC by a special key on any memory card.

Table 11. Third-Party Products for Legacy Host Access

Company	Product
Antenna Software	A3 Mobile Foundation is an XML-based infrastructure for enterprise field-service solutions. Working with Siebel, Clarify, and other CRM systems, it handles the underlying performance, transactional, security, and administrative functions.
mov Software	sshCE is a SSH (secure shell) client with VT100/VT52 support for connecting to a remote host. It uses strong authentication and Blowfish and Triple-DES encryption.

The most current list of add-on software and hardware options for Windows Mobile-based devices can be found in the [Enterprise Solutions](#) section of the Microsoft Web site.

Encryption

Table 12 lists some of the data encryption products available for the Pocket PC and Smartphone from other companies.

Table 12. Third-Party Products for Software Storage Encryption

Company	Product
Asynchrony.com	PDA Defense for the Pocket PC encrypts databases, files, and memory cards.
Bluefire Security Technologies	Bluefire Mobile Security Suite encrypts database (PIM) files, and provides user defined folder encryption on the device and removable storage media.
Cranite Systems	WirelessWall provides AES data encryption for Pocket PCs.
Developer One, Inc.	CodeWallet Pro provides a way to store and access important information on your Pocket PC or Smartphone .
Handango, Inc.	Handango Security Suite for Pocket PC provides file and data encryption.
Pointsec Mobile Technologies	Pointsec for Pocket PC encrypts all data stored in the device, whether in RAM or on external storage cards.
SoftWinter	seNtry 2020 encrypts data on external storage cards.
Trust Digital LLC	Trust Digital 2005 Mobile Edition includes access control and data encryption for Pocket PC devices. It also prevents unauthorized infrared beaming of data.
Ultimaco Safeware AG	SafeGuard PDA Enterprise Edition provides a number of security functions for Pocket PCs including data encryption.

Table 13 lists some application-level encryption products available for the Pocket PC and Smartphone from other companies.

Table 13. Third-Party Application-Level Encryption Products

Company	Product
Certicom Corporation	Security Builder provides a suite of algorithms that enable developers to easily integrate encryption, digital signatures, and key exchange mechanisms into applications.
PGP Corporation	CryptoEx Pocket supports encryption and digital signatures on mobile devices, including e-mail as well as encrypting and signing sensitive files.
Ntru Cryptosystems, Inc.	Ntru Neo is a security toolkit that includes public-key cryptography functions, symmetric-key cryptography functions based on the Rijndael AES, hashing tools, and tools for hashing and message digest creation.

Table 14 lists some of the companies that offer VPN products for Windows Mobile-based devices.

Table 14. Third-Party Products for Virtual Private Networking

Company	Product
Certicom Corporation	The MovianVPN client for Pocket PCs is interoperable with VPN gateways from Check Point, Cisco, and Nortel.
Check Point Software Technologies Ltd.	VPN-1 SecureClient enables users to set up an encrypted connection through the Internet and provides a personal firewall on Windows Mobile-based devices.
Columbitech	Columbitech makes a wireless VPN client for the Pocket PC that uses WTLS encryption.
Ecutel Inc.	Viatores Mobile IP VPN is a mobile VPN solution that uses IPsec technology.
Entrust, Inc.	Entrust Entelligence Mobile Security offers security policy enforcement, VPN access, and data encryption for Pocket PC devices.
Symbol Technologies, Inc.	AirBEAM Safe is a wireless VPN that provides end-to-end security for mobile applications running on Symbol Pocket PCs.
AEP Networks	SmartGate for Pocket PC provides an encrypted VPN connection.

Table 15 lists some of the companies that offer networking encryption products for Windows Mobile-based devices.

Table 15. Third-Party Wireless Network Infrastructure Products

Company	Product
Action Engine Corporation	Mobile Services Platform provides a smart client/smart server architecture for developing and deploying applications for wireless Pocket PCs and Smartphones.
Birdstep	Birdstep Intelligent Mobile IP provides seamless handover, with no user intervention, between infrastructures such as Ethernet, GSM/HSCSD/GPRS or CDMA/IS-95A/B, WLAN (IEEE 802.11b or HiperLAN2), Bluetooth, and HomeRF. It depends only on terminal support for the necessary network interfaces.
Broadbeam	Broadbeam provides development tools and consulting services to assist enterprises in creating wireless enterprise solutions.
Ekahau, Inc.	Ekahau Positioning Engine provides positioning information about a Pocket PC user in a building or campus with a wireless local area network. It offers positioning accuracy up to 1 meter.
Funk Software	Radius/AAA Odyssey is an 802.1x client for communication between Pocket PCs and enterprises using wireless 802.11b LANs. It works with any 802.1x-compatible adapter card and supports EAP-TTLS, EAP-PEAP, EAP-TLS, Cisco's LEAP, and EAP-MD5 802.1x protocols, along with the WPA and WEP encryption methods.
NAVARA	Navara offers a broad range of mobile workflow solutions that provide workflow capabilities to wireless and mobile devices.

Novarra	Deployed behind a corporate firewall, Novarra's mobile web solutions provides a single point of access for integrating mobile device services with a corporation's management and security infrastructure.
NetMotion Wireless, Inc.	NetMotion networking infrastructure software maintains a logical connection when the physical network connection is dropped and re-established.
Odyssey Software	ViaXML enables developers to create client/server and Web services applications for intermittently connected mobile devices.
Sylogist	Sylobridge and Syloway are software infrastructure products for managing connections and data transfer between mobile devices and Enterprise Resource Planning (ERP) applications, using SAP, Oracle, DB2, Access, and other back end storage systems. Sylvia is business event software that brokers complex inter-application workflows.
Symbol Technologies, Inc.	AirBEAM Connect provides a persistent application connection for Symbol Pocket PCs.
weComm Ltd.	The WAVE platform is a gateway that aggregates any content type and delivers it over any wireless network to a wide range of mobile devices in a real-time, fully interactive, and transactional manner.

Security Management

Table 16 lists third-party software solutions that provide additional device backup and restore functionality.

Table 16. Third-Party Backup/Restore Products

Company	Product
Developer One, Inc.	FlashBack Database Edition enables database files to be backed up to memory or CF storage cards.
Satsuma Solutions Ltd.	The DataSafe software package and memory card provide an automated backup and data restore solution for Pocket PCs.
Sprite Software Limited	Pocket Backup saves a complete image of a Pocket PC's files, databases, and registry settings to a storage card or local file system. It can restore the entire image or selectively recover individual files or directories from the image.
Sprite Software Limited	Sprite Clone enables an enterprise to capture a complete image of a Pocket PC (file system, databases and registry settings) and deploy this image to target Pocket PCs.
Nokia	The Intellisync Data Sync toolkit helps companies provide enterprise information to employees, on the go.
iAnywhere	Afaria automates installing and maintaining software on Windows Mobile-based devices. It delivers up-to-date content, captures asset information, monitors system performance, and provides backup of Windows Mobile-based devices.

Table 17 lists third-party products that provide security management functions to automate the enforcement of an organization's security policies.

Table 17. Third-Party Systems Management Products

Company	Product
Wavelink Mobile Manager	Wavelink Mobile Manager provides device control and data security for wirelessly connected Pocket PCs, including the ability to remotely lock or unlock a device, purge specified files, and encrypt/decrypt data on the device.
Computer Associates	Unicenter TNG provides event management, asset management, software delivery, and storage management.
CREDANT Technologies	CREDANT Mobile Guardian (CMG) Shield enforces security policies on Pocket PCs by consistently authenticating mobile users, validating application and privilege rights, and helping protect corporate information on the mobile device. Its functionality includes enforcing on-device mandatory access control and data encryption security policies.
IBM Corporation	Tivoli Smart Handheld Device Manager automates change management and device provisioning processes. It supports software distribution, wireless WAN and LAN connectivity, device discovery, device configuration, and dynamic device groups.
Mobile Automation, Inc.	Mobile System Manager, works with Microsoft System Management Server, enables IT to manage remote and mobile devices.
Odyssey Software	ViaXML ManageFX provides mobile software services for software distribution, remote administration, and device management.
PhatWare Corporation	HPC NetProfile is a network utility program that enables users to create multiple TCP/IP network profiles for each installed network adapter on a Pocket PC. This product also enables users to quickly switch between subnet domains in a corporate network.
Symbol Technologies, Inc.	AirBEAM Smart provides systems and application software synchronization for Symbol Pocket PCs.
Symbol Technologies, Inc.	AppCenter prevents Pocket PC users from running unauthorized programs. It simulates the functionality of a custom vertical market device typically used in sectors such as manufacturing, warehousing, utilities, and field service. Details about AppCenter can be found in Symbol's Developer Zone (visitors must register to access this zone).
Nokia	Intellisync Mobile Systems Management provides inventory capabilities for managing hardware and software assets, together with remote software installation functionality.
TCOsoft	TCOSoft Remote Director management software for Pocket PCs and Smartphones helps simplify device administration, software updates, configuration, remote screen control, customer support, inventory management, security, and centralized control in both wireless and wired environments.
Trust Digital	Mobile Discovery Monitor discovers, monitors, controls, and manages mobile asset usage—that is, who is syncing, on what device, where, when, and with what apps. It is centrally managed by the Small Business, Workgroup, and Enterprise versions of the Trusted Mobility Suite.

iAnywhere	Afaria automates software installation and maintenance, delivers up-to-date content, captures asset information, monitors system performance, and provides reliable backup of Windows Mobile-based devices.
---------------------------	---

Table 18 lists third-party products that provide centralized security management functions to automate the enforcement of an organization's security policies.

Table 18. Third-Party Products for Centralized Security Management

Company	Product
Asynchrony.com	PDA Defense can limit the number of attempts to unlock a device. When the maximum number of attempts is exceeded, PDA Defense bit-wipes all RAM databases. The Enterprise version enables administrators to customize or preset security features, including minimum password length, alphanumeric passwords, and time-based password change.
Bluefire Security Technologies	Bluefire Mobile Security Suite provides central-site management software that configures and distributes security policies to Windows Mobile-based devices.
Pointsec Mobile Technologies	Pointsec's mobile security software will lock down the device, requiring assistance from an IT administrator, after a preset number of incorrect passwords are entered.
Trust Digital LLC	PDASecure Policy Editor provides centralized management for pushing security policies to Pocket PCs and Smartphones.
Utimaco Safeware AG	SafeGuard PDA Enterprise Edition provides a number of security functions for Pocket PCs including central administration of password and user rights.

Table 19 lists some of the anti-virus products available for Windows Mobile devices.

Table 19. Third-Party Antivirus Products

Company	Product
Computer Associates	eTrust Antivirus protection for Pocket PCs (formerly called InoculateIT) provides virus pass-through protection.
F-Secure	F-Secure Mobile Anti-Virus provides on-device background virus checking with automatic virus database updates, both in corporate environments and over wireless connections.
Handango, Inc.	Handango Security Suite for Pocket PC provides file and data encryption along with virus protection.
McAfee	McAfee Mobile Security for Enterprise provides virus protection for mobile devices.
SOFTWIN	BitDefender is an anti-virus solution designed to run on Pocket PCs.
Symantec	Symantec AntiVirus for Handhelds provides real-time defense against viruses on a Pocket PC.

Table 20 lists third-party products that enable IT organizations to turn off certain functionality on a Pocket PC.

Table 20 Third-Party Lock-Down Products

Company	Product
Symbol Technologies, Inc.	AppCenter helps prevent Pocket PC users from running unauthorized programs. It simulates the functionality of a custom vertical market device typically used in sectors such as manufacturing, warehousing, utilities, and field service. Details about AppCenter can be found in Symbol's Developer Zone (visitors must register to access this zone).
Trust Digital LLC	PDASecure Policy Editor provides centralized management for pushing security policies to all of an organization's PDA users.

Table 21 shows third-party PKI toolsets available for Pocket PCs.

Table 21. Third-Party PKI Toolsets

Company	Product
Certicom Corporation	Security Builder PKI is a set of software components, products, and tools for building and deploying trust management solutions using the public-key infrastructure (PKI).
Diversinet Corp.	Diversinet's MobiSecure products provide strong PKI-based authentication on a variety of mobile platforms.
PGP Corporation	CryptoEx Pocket supports encryption and digital signatures on mobile devices, including e-mail as well as encrypting and signing sensitive files.

Additional thin client offerings are available from the companies listed in Table 22.

Table 22. Third-Party Thin Client Products

Company	Product
Citrix	ICA is a thin client for Pocket PCs.
FinTech Solutions Ltd.	Varadero Wireless Framework is an ultra-thin client. Designed for server-based applications such as Visual Basic®, it uses common development tools.

#####

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2006, Microsoft Corporation. All rights reserved.

Microsoft, ActiveSync, Windows, the Windows logo, Windows Mobile, Windows NT, Microsoft Windows Server, Microsoft Office Outlook, and Visual Basic are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.