Mobile Messaging and Business Application Solutions with Windows Mobile: Addressing Key Questions

White Paper

Published: July 2006

Microsoft

Contents

Executive Summary

Microsoft® Windows Mobile® software powers advanced, easy-to-use mobile devices that allow users to send and receive e-mail messages, browse the Internet, and use mobile versions of familiar Microsoft Office programs. Designed to provide mobile devices to companies both small and large, Windows Mobile combines with the Microsoft Exchange Server 2003 communication and collaboration server so organizations can make use of existing technology investments in hardware, software, and training and can mobilize workforces quickly and easily.

This paper addresses specific questions we have heard from customers following the release of Windows Mobile 5.0 with the Messaging and Security Feature Pack and Service Pack 2 for Exchange Server 2003.

For more information on mobile messaging, please visit:
http://www.microsoft.com/windowsmobile/business/email.mspx

.

Introduction

From increased customer responsiveness and reduced cycle times to improved collaboration and faster decision-making, many companies have experienced the benefits of providing users with mobile access to e-mail. As a result, organizations are now looking for ways to deliver mobile access to a much larger employee population rather than a select few. In addition, they are looking for ways to expand mobile access beyond e-mail to include line-of-business (LOB) applications.

In the past, there have been many barriers to large-scale deployments, including cost, security, the ability to scale, and limited device choices. But as mobility products have matured, there are now new solutions that help overcome these barriers, presenting organizations with the opportunity to deploy mobile devices throughout the enterprise. With the range of options in the marketplace, choosing the right mobile technology to meet current and future needs is more important than ever.

How can Microsoft Windows Mobile 5.0 help enterprises?

By implementing a solution based on Microsoft® Windows Mobile® 5.0, the newest version of the Microsoft platform for mobile devices, organizations can offer their employees an entirely new generation of connected Pocket PCs (PPCs) and Smartphones. Windows Mobile 5.0 helps companies improve business performance by extending to mobile workers mobile versions of core desktop applications, such as Microsoft Office, which includes the Microsoft Outlook® messaging and collaboration client, and LOB applications.

As the software for Windows Mobile powered devices, Windows Mobile is just one part of the Microsoft mobile solution. Windows Mobile works with Exchange Server 2003 to help provide businesses with secure mobile messaging and personal information management (PIM) that is mobile operator-independent and does not depend on either third-party middleware servers or third-party network operations centers (NOCs). With Windows Mobile, Exchange administrators can now manage each deployed mobile device user like just another Exchange client using the same Exchange System Manager tools they use every day. With the introduction of the Messaging and Security Feature Pack (MSFP) for Windows Mobile 5.0, organizations gain Direct Push e-mail and new levels of security and control delivered by the Exchange Service Pack 2 (SP2) mobile services policy and device management interface.

Third Party Relay vs. Direct Push Technology

A number of mobile messaging solutions now offer “push e-mail,” which is the ability for e-mail to be “pushed” directly from a mail server to a mobile device, without requiring that the device continually polls the server mailbox to check if there are new messages.

Other push e-mail solutions require that customers invest in a third-party solution to integrate with their existing e-mail server. This requirement may generate additional cost and complexity. Furthermore, the mail server is continuously polled by a middleware server; e-mail messages are pulled from the mail server to the middleware product—and only then pushed either to the device or to a third-party service center or NOC where it is stored until it can be routed to the mobile device.

In contrast, Exchange Server 2003 with SP2 includes native support for push e-mail, known as Direct Push, without involving middleware. With Direct Push, customers can get near real time access to their e-mail without requiring any additional software or third-party services. The Exchange Server synchronizes e-mail messages with a Direct Push mobile device as soon as they are received. With Direct Push, users gain immediate access to messages because the mobile device becomes a dynamically-updated copy of the user’s mailbox.

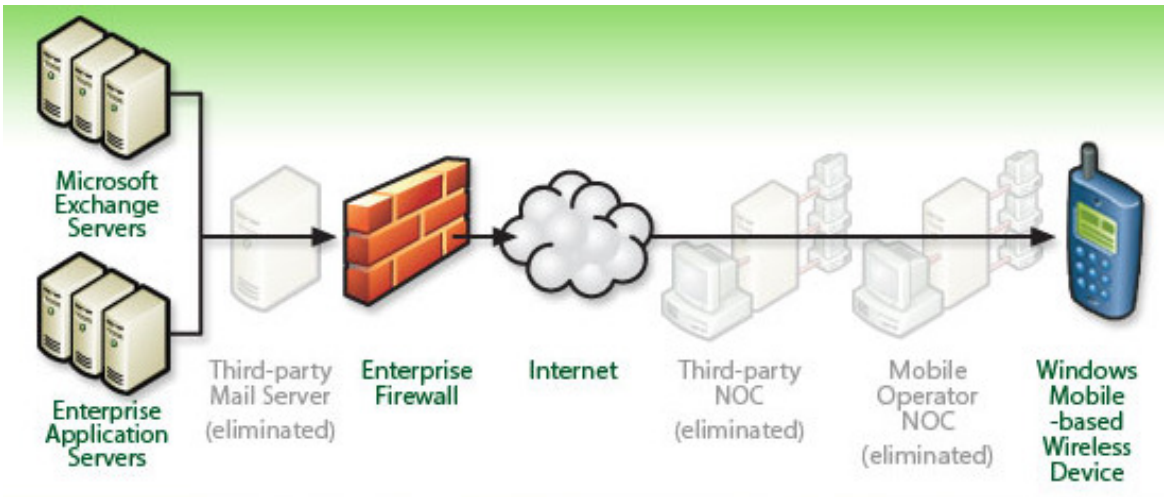

Figure 1: Direct Push eliminates the need for middleware.

What is Direct Push Technology and how does it work?

Direct Push is the Microsoft implementation of push e-mail. With Direct Push Technology, Exchange Server sends e-mail and PIM updates directly to a mobile device over HTTPS (a secure Internet transfer protocol), which is the same way customers already access Exchange via Outlook Web Access (OWA).

Unlike prior implementations of Windows Mobile, Direct Push does not rely on Short Messaging Service (SMS), but instead uses a persistent, long-lived HTTPS connection. When a mobile device comes on to the network and receives an IP address, it establishes a secure socket layer (SSL) RC4 or 3DES connection with the Exchange Server and reports that it is ready to receive. The device then enters an idle state—known as the “heartbeat” interval—waiting for new e-mail or any other Exchange folder changes. As new mail arrives, Exchange Server pushes a Microsoft Exchange ActiveSync® notification to the mobile device. Exchange ActiveSync is a built-in component of Exchange Server and is the engine behind

Direct Push technology. If no new mail arrives or has been sent on the device within a certain amount of time the mobile device reconfirms the connection with the Exchange Server and reenters the heartbeat interval, waiting for new mail.

The amount of data transmitted during the mobile device's initial connection with the Exchange Server is small, well under one kilobyte, and the heartbeat interval is dynamically configured to optimize network performance, mail delivery, and battery life.

What is Scheduled Sync and what benefits does it provide?

In addition to Direct Push, Microsoft Exchange and Windows Mobile offer the freedom of Scheduled Synchronization on both Windows Mobile 5.0 and Windows Mobile 2003 powered devices. Scheduled Sync allows users to control when and how often mail is delivered to their mobile device—and can range every four hours to upon arrival. Users can also configure Scheduled Sync to perform only when the user initiates it. For instance, many users choose to have e-mail pushed to them during business hours, less frequently during the evening, and not at all on weekends.

Why doesn't the Windows Mobile solution use a Network Operations Center?

Windows Mobile doesn't require a NOC because Direct Push enables e-mail to be delivered directly from the server to the mobile device, without being intercepted and relayed by a third party. Direct Push connects the server directly to the mobile device, whether over a mobile operator network, a public Wi-Fi network, or a private LAN.

NOCs may limit flexibility because each NOC-managed device is mapped to a particular mobile operator and a particular user—and can only work with that mapped operator and user. In addition, because the NOC is outside corporate IT control, and sometimes even located in a different country, it is a point of failure that can have a negative impact on productivity if an outage occurs.*

Rather than managing by the device, as found in the NOC model, Exchange manages by the user. In other words, it allows any user provisioned by Exchange User Manager to use any mobile operator anywhere in the world with any Windows Mobile device supported by that operator. With Windows Mobile, businesses get enterprise-grade security without the point of failure and the third-party mail servers and software required to poll Exchange and push to the NOC. The enterprise stays in control of their messaging environment and can allocate—and re-allocate—devices to users as they see fit. This ability helps the enterprise to change, activate, and deactivate devices.

Why is Direct Push a viable alternative to third-party relay systems?

Direct Push offers many performance and design features, including the following:

1. For Exchange 2003 SP2 users, Direct Push does not require the purchase, installation, administration, and support of additional middleware servers.
2. Direct Push places minimal load on the back-end Exchange environment because it does not have to continually poll those servers for new content. In contrast, many third-party solutions place a large load on these servers, often requiring additional mail servers and new middleware servers. In fact, some middleware solutions can increase

* Outages are not uncommon with the NOC model: Blackberry users experienced outages in March 2006 (http://www.wirelessweek.com/article/CA6316609.html); T-Mobile BlackBerry users were affected in February 2006 (http://news.com.com/2061-10801_3-6044449.html); and the BBC was forced to stop using BlackBerries after a software glitch became apparent (http://networks.silicon.com/mobile/0,39024665,39153677,00.htm?r=1).

load anywhere from 3 to 8 times.[†] To put this figure into perspective, consider the following: deploying 100 mobile users can add the load of 300 to 800 additional users to the mail environment.

3. Direct Push is integrated into the Microsoft Active Directory® service so administrators do not need to administer another directory and grant "super user" mailbox access to a middleware server.
4. Direct Push uses the native Exchange ActiveSync server interface rather than the Messaging API (MAPI) desktop interface to deliver e-mail. MAPI is not designed for continuous high volume polling and has a fixed limit of 500 mailbox connections per middleware server. In contrast, Exchange ActiveSync is designed specifically for mobile email delivery and supports thousands of mailbox connections.

Is a third-party relay NOC required for enterprise-grade security?

No. Routing data through a middleware server or a third party network operations center does not enhance the security of the data being transmitted between the mail server and the device. Instead, the security of data being transmitted depends on the encryption method between the mail server and the mobile device.

Windows Mobile uses SSL with either RC4 or 3DES ciphers to encrypt data between the mail server and the mobile device. SSL connections are widely used in e-commerce and on-line banking, and are also used by Microsoft Exchange Server to support OWA and Outlook Anywhere, formerly Remote Procedure Call (RPC) over HTTPS. In addition, the underlying cryptographic application programming interfaces (APIs) and cryptographic service providers have been certified to meet U.S. Government Federal Information Processing Standard 140-2 (FIPS 140-2). Finally, because data is not stored at a NOC, it is not outside enterprise IT control.

Can Windows Mobile 5.0 devices be upgraded so they can run Direct Push?

Yes. The operators may choose to upgrade devices. Operators who have announced that they will support Direct Push represent more than half of the world's subscriber base.[‡] Direct Push is already available for more than 25 devices.

Does Direct Push increase data usage more than previous versions of the Windows Mobile e-mail solution?

Comparison testing between Direct Push and Scheduled Sync shows that in cases where users process fewer than 75 e-mail messages per day, Direct Push is more efficient. This is due to the fact that Scheduled Sync has high fixed bandwidth costs (a fixed number of syncs everyday) but it does not increase with the number of e-mails sent or received.

Direct Push also uses GZIP compression which reduces data usage by 40-50% over Windows Mobile 2003.

[†] RIM white paper: Performance Characteristics: BlackBerry Enterprise Server version 3.6 for Microsoft Exchange

[‡] http://www.microsoft.com/windowsmobile/business/5/default.mspx

Release	Test Mobile Schedule	25th percentile	75th percentile
Windows Mobile 2003 Sch Sync (no GZIP compression)	10 mins peak + 10 mins offpeak	400KB (10MB/month)	600KB (15MB/month)
Windows Mobile 5.0 Sch Sync (with GZIP compression)	10 mins peak + 10 mins offpeak	240KB (6MB/month)	360KB (7.5MB/month)
Windows Mobile 5.0 + MSFP (with GZIP compression)	AUTD (always up to date)	150KB (3.75MB/month)	430KB (10.75MB/month)

Figure 2: Direct Push is more efficient than Scheduled Sync.

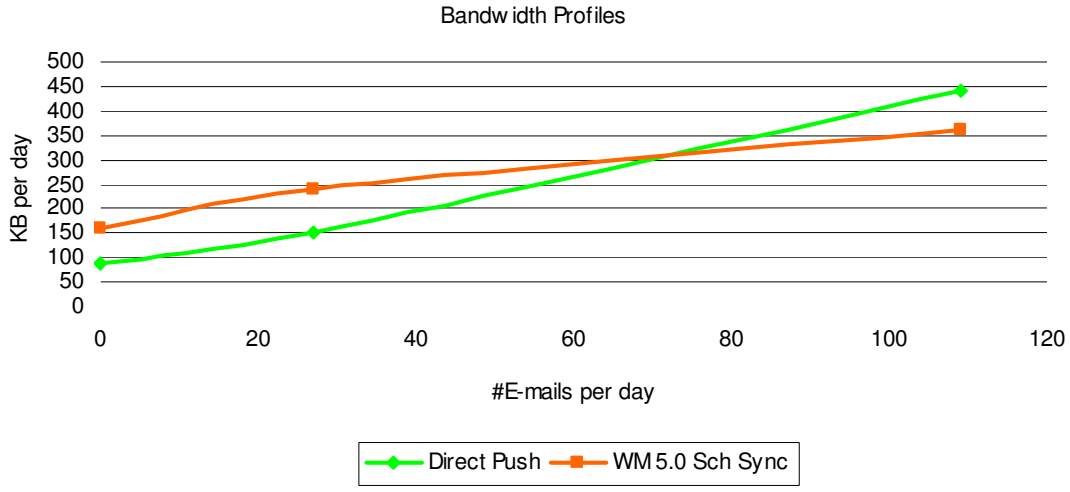

Figure 3: For the majority of users, Direct Push uses less bandwidth than Scheduled Sync.

Addressing Security Needs

As enterprises consider large-scale deployments of mobile devices, they are becoming increasingly concerned about confidential corporate data being compromised by falling into the wrong hands. Windows Mobile helps organizations extend business information to their mobile users while providing a way to help manage and control access to their devices.

How can Windows Mobile and Direct Push help my company meet its security requirements?

Windows Mobile is designed with enterprise-grade security support right out of the box. The combination of Windows Mobile, Exchange Server, and Exchange ActiveSync helps to give enterprises flexible, single-point control over their mobile messaging. First, the communication channel between the device and Exchange Server is encrypted end-to-end using SSL. Second, the direct HTTPS connection between Exchange Server and a Windows Mobile powered device eliminates the need to route data through additional servers or a third-party NOC. Third, the security policies and device management portfolio built into SP2 and MSFP helps the enterprise to control device access, and by extension, the data on those devices.

What are the primary security benefits of MSFP?

When combined with Exchange Server 2003 with SP2, MSFP provides security policies that enable enterprises to help protect the Windows Mobile 5.0 powered devices their mobile workforces use. MSFP provides the following benefits:

- Allows system administrators to remotely manage and enforce select corporate IT policies over-the-air
- Enables local device wipe (hard reset) when the password is entered incorrectly a set number of times, protecting the device from unauthorized use.
- Configures device timeout which locks access to the device.
- Helps administrators to better protect device data with the ability to remotely wipe a device by using the Exchange Mobile Administration Web tool.
- Allows increased access security to Exchange Server using certificate-based authentication to the server
- Helps protect e-mail content while in transit and at rest on the device with native S/MIME support

What security features are built into Windows Mobile 5.0 and MSFP?

Windows Mobile offers security features that enterprises require. These include the following:

- **Encrypted Protection of the Data Transport Layer.** Native support for SSL helps Windows Mobile users gain a security-enhanced, end-to-end channel of communication between Exchange Server and each authenticated mobile device. As a default setting, Windows Mobile uses SSL with RC4 cipher (128-bit encryption), the standard for online banking. 3DES can also be used when FIPS 140-2 is enabled on the front-end server. In addition, SSl is configured so that only inbound data from an authenticated device or client is allowed through the Web-listening port. This is the same port used for other Exchange HTTPS connections such as OWA, RPC over HTTP, and OMA.
- **Encrypted Protection of the E-mail Data Payload.** Secure Multipurpose Internet Mail Extensions (S/MIME) is a standard protocol that uses content encryption and

digital signature features to help protect messages as they are transferred and at rest on the device. Windows Mobile provides native support for S/MIME that involves S/MIME certification via peripheral smartcard reader to help ensure that only the intended recipient can access the contents of the message. (This feature requires a hardware card reader.)

- **Encrypted Access to Corporate Network Data.** Windows Mobile powered devices can connect to corporate networks with native support for virtual private networks (VPNs), including traditional Point-to-Point Tunneling Protocol (PPTP) as well as Layer 2 Tunneling Protocol (L2TP) with IP Security Protocol (IPSec).
- **Policy Provisioning and Enforcement.** The Exchange system administrator can help control access to the device because Exchange 2003 SP2 PIN/password and timeout policies are pushed to the device when a sync is first initiated by the device after policy initiation. The user then sets the PIN or password on the device; this becomes the key to unlocking the device after a timeout. The user may change the PIN/password at any time, depending on the constraints on the policy that has been established.
- **Remote Device Wipe.** In case a mobile device is reported lost or stolen, it is possible to "wipe" the device back to factory default settings—a hard reset—to help prevent data and applications from falling into the wrong hands. Using the browser-based Mobile Admin Web tool, an IT administrator searches synced devices for a particular username/alias and then initiates the wipe command. The device receives the wipe command as part of the normal Exchange update and executes the command. The wipe command status is then relayed back to the Mobile Admin Web tool as a logged transaction to show the IT administrator that it has been completed.
- **Local Device Wipe**. IT staff can configure the number of allowed attempts to access the device when they establish the PIN/password policy using the Exchange Server Console. If this number is exceeded a hard reset occurs: all e-mail, PIM data, configurations, applications, and media are deleted from the device's resident memory. External memory remains intact. This data remains in the Exchange Server folders and can be re-synced to the device if it is recovered, or, of course, synced with a new device.
- **Two-Factor Identification.** Windows Mobile supports third-party smart cards and biometrics. In addition, RSA's SecurID, which is widely used in Europe and by companies in the financial industry, is also fully supported.
- **Cryptographic APIs and Native Encryption in Microsoft SQL Server™ Mobile.** Microsoft makes cryptographic APIs available so that custom applications can be written to encrypt data. In addition, native encryption support in SQL Server Mobile helps ensure that data remains secure.

Reducing Total Cost of Ownership

More than ever, enterprises are seeing the productivity and operational benefits of mobilizing more of their workforce—yet at the same time are under pressure to rationalize these improvements against the costs of their mobile solution investments. The Windows Mobile platform can help by enabling organizations to use their existing infrastructure to expand mobile messaging throughout the workforce, often at lower TCO than competing mobile solutions.

What does my company need to get started with Windows Mobile and Direct Push?

Organizations that have Exchange Server 2003 with SP2 already have Direct Push Technology and don't need any additional server hardware or software. In addition to eliminating third-party hardware or software fees, companies with Microsoft Premier support contracts also reduce product support costs because they already have support for Exchange and Windows Mobile as part of that support package. And finally, IT departments have the simplicity of a single platform to manage with all the key device provisioning and management services available as part of the Exchange System Manager toolset. Exchange Server 2003 with SP2 is only required on front end servers to support Direct Push, so IT administrators need not wait to upgrade all servers before deploying Windows Mobile devices to users. (Microsoft recommends that the backend servers eventually be upgraded to improve overall system efficiency).

How does the scalability of Windows Mobile impact TCO?

The scalability of Windows Mobile is linked to the native scalability of Exchange. A single Exchange 2003 server can support thousands of users. Therefore, mobilizing existing Exchange users with Windows Mobile does not require as many additional Exchange Servers as would be required with middleware solutions. In addition, there are no additional Windows Mobile licensing fees for existing Exchange 2003 installations. Enterprises that already use OWA or Outlook Anywhere already have HTTPS connectivity between clients outside the corporate firewall and Exchange via the Internet. As a result, adding Windows Mobile powered device connectivity as another external client doesn't require additional infrastructure cost. Simply stated, Direct Push can scale with a company's Exchange system because it uses the same underlying infrastructure as other clients, which helps reduce TCO for the entire mobile solution.

What evidence is available to support these TCO reduction arguments?

According to a Microsoft-sponsored study recently conducted by Wipro, a consulting firm with a focus on new and emerging technologies and more than 10 years experience researching, analyzing, and documenting the business value of technology solutions, choosing a mobile solution based on Windows Mobile offers many TCO benefits for companies already using Exchange Server 2003 with SP2, including the following:

- The TCO of the Windows Mobile platform is 15-24% lower than that of a comparable third-party relay solution from RIM using BlackBerry devices. TCO savings vary by the number of users deployed.
- There is a significant difference in fixed and variable costs between Windows Mobile 5.0 and RIM's solution due to the additional infrastructure and support required by the RIM solution: BES (BlackBerry Enterprise Server) software licensing, hardware,

installation, maintenance (includes software updates), and data center operations, RIM NOC gateway fees, RIM TSupport technical support, and SQL Server hardware and software.

- Windows Mobile avoids the additional load placed on Exchange by BES polling via MAPI and thus avoids the added cost of additional Exchange Servers required to support large RIM deployments (over 500 users).[§]

As another example, Lifetime reports lowered annual costs of U.S.$2,000 per user, and has not seen an increase in data costs. Read more at: http://members.microsoft.com/CustomerEvidence/Search/EvidenceDetails.aspx?EvidenceID=3958&LanguageID=1

[§] Wipro, "Mobile Device Platforms," October 2005

Taking Advantage of the Already Familiar Microsoft Windows Interface

With Windows Mobile, users don't necessarily have to be trained on a new system just to check their e-mail messages. Instead, they can view their messages—along with programs—using the already familiar interface of Microsoft Windows in its mobile form: Windows Mobile and Microsoft Office Outlook Mobile.

How user friendly is Windows Mobile?

Windows Mobile offers many of the same Windows user interface features people use every day on their PC desktops. For example, the familiar Start menu provides access to programs and features, just like Windows on personal computers.

Windows Mobile helps people work how they want, when they want. With rich functions in every Windows Mobile powered device—many featuring touch-screens, QWERTY keypads, digital cameras, and more—Windows Mobile powered devices come in a variety of form factors supporting GSM, UMTS (W-CDMA), CDMA, and PHS mobile operator network technologies. Many include Bluetooth radios for wireless peripherals, file sharing, and data connectivity, and support for WLAN connectivity and VoIP calling.

Windows Mobile provides the features most business users want. For instance, with Office Mobile, users can:

- Maintain an e-mail mirror image between the Windows Mobile powered device and the Exchange Server folders using Direct Push and Exchange ActiveSync.
- Get calendar, contacts and messaging—and access Global Address Lists (GALs).
- Search contacts with a portion of the first or last name.
- Accept and decline meeting requests.
- View full display names as opposed to a simple e-mail address.
- Manage Outlook Mobile folders and e-mail messages—and have those changes instantly appear on the desktop.
- Manage contacts with voice commands, photos and personal ring tones.
- Configure the size of messages that are delivered along with how many days worth of messages should be synchronized to the device.
- Handle Microsoft Office file attachments on a Windows Mobile powered Pocket PC, including viewing PowerPoint presentations, and editing Microsoft Word documents and Microsoft Excel spreadsheets.
- View PDFs easily using Adobe Acrobat Reader for Windows Mobile.
- Download and send attachments of any size—and even configure the device to download automatically based on the size of the attachment or only download manually. Overall settings can be controlled by IT administrators.
- Ability to add a voice reply to e-mail messages when typing is not convenient.
- Share Outlook/Outlook Mobile contacts with other mobile users using the infrared port.

Gaining the Benefits of an Open Platform

Unlike most closed third-party relay solutions that require all data and applications to be managed by a third-party NOC, Windows Mobile is a flexible, open platform. Microsoft makes APIs available to help make it easier to create and publish software.

An open mobile platform helps companies gain a significant value: The ability to choose applications, solutions and capabilities from the rich Microsoft partner ecosystem. With hundreds of Independent Software Vendors (ISVs) and System Integrators (SIs) supporting the Windows Mobile platform and more than 18,000 mobile applications running on Windows Mobile software today, Windows Mobile can meet the needs of companies across a broad spectrum of possible mobile solution requirements.

Why should I consider an open platform over a closed platform?

More than ever, businesses need their mobile workforces to stay connected to critical business information, including not just e-mail messaging but also LOB applications. Custom mobile LOB applications can be written on the Microsoft .NET Compact Framework or using the Microsoft Visual Studio® development system. They can also be ported from .NET Framework applications to allow access to internal data or allow mission critical data input that can only be done in the field.

For example, many companies take advantage of LOB applications such as customer relationship management (CRM) and enterprise resource planning (ERP) to increase revenue and boost operating efficiencies. The Windows Mobile open platform allows these core LOB applications to be extended to the mobile workforce. Companies such as SAP, Siebel, PeopleSoft, and Salesforce.com all offer mobile versions of their core LOB applications for the Windows Mobile platform; SAP and Siebel allow customers and other software providers to write mobile applications on top of their core solutions.

In addition, a wide range of industry-specific applications are also readily available for Windows Mobile, including real estate, healthcare, financial services, and manufacturing.

How can the Windows Mobile open platform increase my mobile security options?

There are many third-party independent software vendors that provide device management and security solutions (DMSec) to extend the native DMSec features of the Windows Mobile platform. Organizations that have more stringent security requirements, such as financial services, government and healthcare, have an array of options to choose from when developing the right DMSec solution. Examples include:

- **Trust Digital Mobile Edge Device Security:** A security platform that helps implement and enforce mobile security policies, synchronizes encrypted information in the background, and requires all devices to pass policy-based compliance verification checks before gaining network and application access.
- **Odyssey Software's Athena Device Management Suite:** A mobile device management infrastructure that complements the Administrator Console of Microsoft Systems Management Server 2003 (SMS) and Microsoft SQL Server to remotely manage, maintain, troubleshoot and fix mobile devices
- **CREDANT Mobile Guardian:** A product that helps secure the data on notebook computers, tablet PCs, PDAs and smartphones using a single management interface and provides centralized security policy by integrating with enterprise directories.

- **Soti MobiControl:** A mobile device management solution, including HelpDesk support, that provides organizations with integrated tools to centrally manage and control their mobile field force.
- **iAnywhere Afaria:** A mobile software solution that allows companies to centrally manage and secure the technology used at the front lines of their business. Its enterprise-ready security solutions protect mobile data and devices, while frontline systems management capabilities proactively manage all the devices, applications, data and communications critical to frontline success, regardless of the bandwidth available.

These solutions also go beyond the capabilities offered by standard third-party relay solutions without requiring a NOC or charging NOC gateway fees. Partner DMSec solutions can be customized to deliver what the enterprise requires. And once they are licensed and deployed, they are under the control of corporate IT without diminishing the inherent flexibility of the Windows Mobile platform.

Conclusion

Not only does a Windows Mobile solution address the cost, security, and ability to scale concerns faced by many businesses today, but it also offers many benefits not found in competing mobile products. Windows Mobile reflects a strategic commitment of Microsoft to meet the mobile needs of business customers both now and in the future, and is already a proven solution in large mobile messaging and line of business application deployments.

By using Direct Push Technology, organizations gain a solution that uses their existing Exchange Server infrastructure and delivers a push e-mail user experience—without the additional costs associated with third-party relay solutions.

A mobile deployment using Microsoft technology also helps offer enterprise-grade security without giving up the flexibility of an open platform or depending on external points of failure. With built-in data encryption features such as native SSL with RC4 and 3DES, S/MIME, VPN support, and the ability to actively control device access, organizations gain a powerful baseline set of data security features. These security features can also be augmented with Microsoft DMSec partner solutions as required. Enterprises that need specific security management solutions will find a wide array of Microsoft partner options worldwide from which to choose and that can be deployed off the shelf.

Finally, users can quickly master their Windows Mobile powered devices thanks to the familiar Windows interface used every day on desktops around the world. From the simplicity of e-mail messaging with Outlook Mobile to the familiarity of working with presentations, spreadsheets, and documents with Office Mobile and on to the power of running mobile LOB applications such as Microsoft Mobile CRM and thousands of third-party applications, mobile workers can remain productive, communicate, and collaborate, whether they are at their desk or on the go. To read more about how Windows Mobile is changing the way companies do business, visit the following:

Global Manufacturer Empowers Employees, Increases Efficiency with Mobile Solution
http://members.microsoft.com/CustomerEvidence/Search/EvidenceDetails.aspx?EvidenceID=14436&LanguageID=1

Oregon Education Executives Speed Mobile E-Mail Handling by 20 Percent:
http://members.microsoft.com/CustomerEvidence/Search/EvidenceDetails.aspx?EvidenceID=10674&LanguageID=1

Global IT Company Poised to Reduce Messaging Costs with Windows Mobile
http://members.microsoft.com/CustomerEvidence/Search/EvidenceDetails.aspx?EvidenceID=4102&LanguageID=1

WebCentral Provides Enterprise-Grade Mobility Solution to Midsize Businesses:
http://members.microsoft.com/CustomerEvidence/search/EvidenceDetails.aspx?EvidenceID=13607&LanguageID=1&PFT=Microsoft%20Exchange%20Server&TaxID=19731

Hewlett-Packard Gains Robust Mobile Capabilities with Global Messaging Upgrade:
http://members.microsoft.com/CustomerEvidence/search/EvidenceDetails.aspx?EvidenceID=13514&LanguageID=1&PFT=Microsoft%20Exchange%20Server&TaxID=19731

0601 Part No. xxx-xxxxxx (if applicable)