White Paper: Wireless Business Email for Individuals on the Road

Wireless Business Email for Individuals on the Road:

Palm MultiMail® Deluxe and the Palm i705 Handheld

Contents

Introduction

As business professionals become increasingly mobile, the need for an easy-to-use wireless email solution is greater than ever. Dial-up connections to the corporate mail server are often slow and unreliable. And carrying a laptop computer just to retrieve email can be cumbersome. With so much time-critical communication now conducted over email, individuals on the road need their business mail to come directly to their Palm™ handheld, enabling them to respond quickly just as if they were at their desk.

The new Palm MultiMail® Deluxe email solution takes advantage of advances in wireless data networking to deliver secure mobile access to corporate email for individuals traveling away from the office. The new wireless Palm i705 handheld is always on[1], continuously checking for new messages received by the corporate Microsoft Exchange server[2]. Palm MultiMail Deluxe Desktop Link software installed on the desktop PC encrypts the messages and automatically sends them to the user's Palm i705 handheld, which notifies the user that mail has arrived. Individuals receive their business mail effortlessly and securely.

Remote management capabilities built into Palm MultiMail Deluxe enable the user to configure filters and store or delete messages directly from the Palm i705 handheld. For example, users can delete messages from their desktop Inbox wirelessly—at the same time as they delete them from the handheld. In addition to business email, the Palm MultiMail Deluxe solution supports up to six personal email accounts and a Palm.com email account, for convenient management of personal and business correspondence while on the road.

This paper provides an overview of the architecture and security features of the Palm MultiMail Deluxe email solution.

[1] Unless user manually turns off radio.
[2] The Palm i705 handheld requires a Palm.Net account, sold separately. Service not available in all areas.

Accessing Corporate Email from the Road

The Palm MultiMail Deluxe email solution gives individual mobile professionals secure, continuous access, within coverage area, to their corporate email from their Palm i705 wireless handheld. With Palm MultiMail Deluxe, mobile professionals can automatically receive business emails, and can create and send business correspondence while away from the office, without having to carry a laptop computer or search for dial-up access. The Palm MultiMail Deluxe solution supports many important remote email management features, including:

- All messages are encrypted before being sent between the Palm i705 wireless handheld and the user's desktop PC.
- The i705 handheld automatically retrieves new business email messages and notifies the user of their arrival with a configurable alert.
- Messages are delivered over a secure wireless network.
- New messages, replies, and forwarded messages sent from Palm MultiMail Deluxe client software appear to the recipient as if they had come from the user's desktop.
- Filters allow users to define exactly what messages they wish to receive on their Palm i705 handheld. Filters can be set on the To, From, Subject, CC, and Date fields and on the message size, and can be changed at any time using the handheld.
- Remote management of email is under user control. For example, the user can delete a message after reading it and specify that the message should be deleted from the desktop InBox as well. The operation is performed wirelessly, not later when the user synchronizes the handheld with the desktop.

Palm MultiMail Deluxe System Components

The Palm MultiMail Deluxe email solution is built on four main components.

- Palm MultiMail Deluxe Desktop Link software running on the user's desktop PC
- The Cingular wireless network
- The Palm i705 wireless handheld
- Palm MultiMail Deluxe Email Client software running on the Palm i705 handheld

Figure 1 shows how Palm MultiMail Deluxe routes business email to the mobile user's Palm i705 handheld.

1. When mail arrives for the handheld user at the corporate Microsoft Exchange Server, the server notifies the Palm MultiMail Deluxe Desktop Link software running on the user's desktop PC.
2. Palm MultiMail Deluxe Desktop Link encrypts a copy of the message and sends it to the user's Palm i705 handheld.
3. The encrypted message is routed via the Internet and the Cingular wireless network.
4. The handheld receives the message in the background, decrypts it, and notifies the user of its arrival.

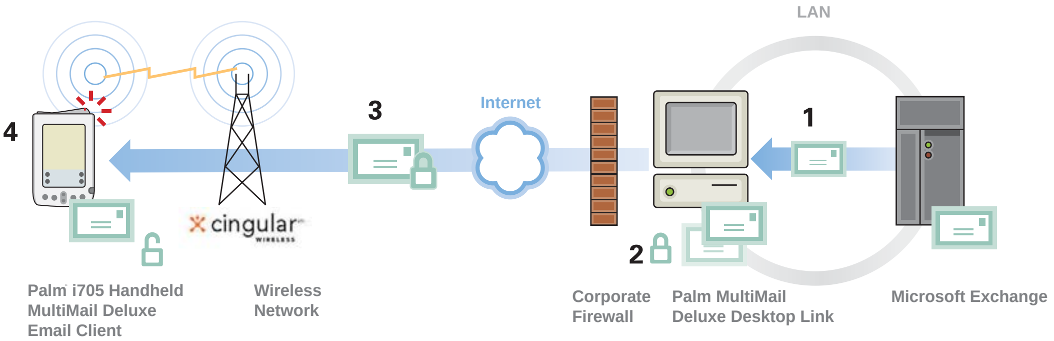


Figure 1 – Receiving Corporate Email Using Palm MultiMail Deluxe

Wireless Business Email for Individuals on the Road:

Palm MultiMail® Deluxe and the Palm i705 Handheld

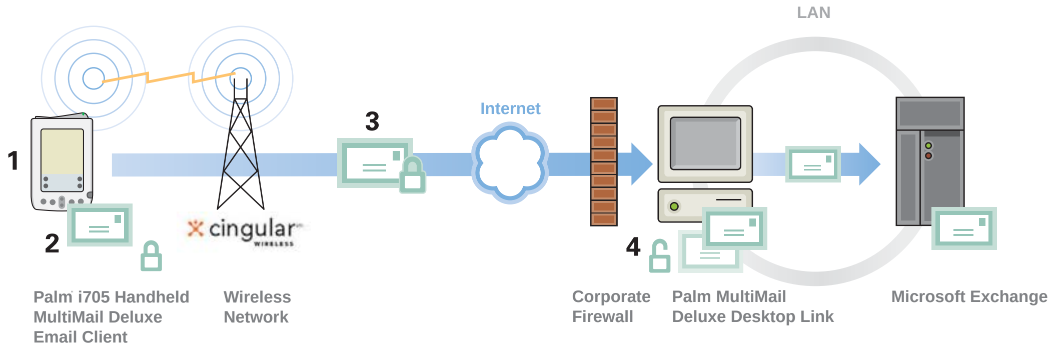


Figure 2 – Sending Corporate Email Using Palm MultiMail Deluxe

Messages created and sent from the handheld follow the same steps in reverse (Figure 2).

1. The user creates an email message. This could be a reply to a received message, a forward of a received message, or a new message.
2. When the user taps Send, the MultiMail Deluxe Email Client encrypts message and sends it.
3. The encrypted message is sent over the wireless network and the Internet, through the corporate firewall, to the user's desktop.
4. The MultiMail Deluxe Desktop Link software on the user's PC decrypts the message and sends it out using MAPI, placing a copy in the user's Sent Items folder.

Whether the message is composed using the Palm MultiMail Deluxe Email Client software on the Palm i705 handheld or the user's desktop Microsoft Outlook email client, it appears to the recipient to originate from the user's corporate email address.

Support for Additional Email Accounts

The Palm MultiMail Deluxe email solution lets Palm i705 handheld users stay connected to personal as well as business email. In addition to secure access to corporate mail, the Palm MultiMail Deluxe Email Client also supports wireless access for up to six personal email accounts (POP or IMAP-accessible) and a Palm.com email account. Users can easily manage and organize email from all these accounts as well as seamlessly switch between accounts. Several widely used service providers, including Yahoo and EarthLink, are pre-installed on the Palm i705 handheld to make setup and configuration easy for the user.

System Requirements

The Palm MultiMail Deluxe Desktop Link software requires the following system configuration on the user PC:

- Pentium 400 MHz processor or better
- 64 MB RAM
- 35 MB of free space on the hard drive
- Windows 98, NT 4.0, 2000Pro, or XP
- Microsoft Outlook 98, 2000, or XP

The Palm MultiMail Deluxe Desktop Link and the Palm MultiMail Conduit support the following corporate mail servers:

- Microsoft Exchange 5.5
- Microsoft Exchange 2000

MAPI

Palm MultiMail Deluxe Desktop Link software accesses the Microsoft Exchange enterprise mail server using Microsoft's Messaging API (MAPI), a widely used messaging architecture that enables multiple applications to interact with multiple messaging systems seamlessly across a variety of hardware platforms.

Palm MultiMail Deluxe uses MAPI to enable the following features:

- Provide immediate, automatic notification of new incoming mail to Palm MultiMail Deluxe Desktop Link, enabling messages to be delivered to the i705 handheld. This allows the user to receive mail anywhere within coverage area without having to manually connect to the corporate mail server.

- Allow Palm MultiMail Deluxe Desktop Link to send outgoing messages that were composed on the handheld through the corporate mail server so that the message originates from the user's corporate email account with a copy placed in the user's Sent Items folder.
- Enable Palm MultiMail Deluxe Desktop Link to perform address resolution against corporate and personal address books. Typically, a Palm i705 handheld user sends messages to SMTP email addresses, both internal (jsmith@usercompany.com) and external (jsmith@othercompany.com). MAPI allows the user to also send messages to non-SMTP addresses. For example, the user can compose a message to "Jan Smith," and Palm MultiMail Deluxe Desktop Link can be configured to examine the Global Address Book on the Exchange server, the Personal Address Book on the user's Outlook desktop, and the Contacts on the user's Palm handheld for a matching entry.

Control Messages

Users can remotely manage their email Inbox and the operation of Palm MultiMail Deluxe from their Palm i705 handheld. Remote management capabilities include deleting messages on both the handheld and the user's corporate Inbox. Users can delete messages that they have read and do not want, reply to and forward messages, and set filters.

These operations are performed by sending control messages from the handheld to the user's Inbox. These control messages have a proprietary format and are encrypted using a DESX encryption algorithm, ensuring the integrity of the user's Inbox by making it impossible for hackers to send unauthorized control messages to (spoof) Palm MultiMail Deluxe Desktop Link.

Security

Whenever business email is transmitted outside the corporate firewall, the security of communications and systems must be ensured. The Palm MultiMail Deluxe solution provides multiple layers of security, including DESX message encryption, wireless network and data center security, and password protection on the Palm i705 handheld.

Firewall and Server Security

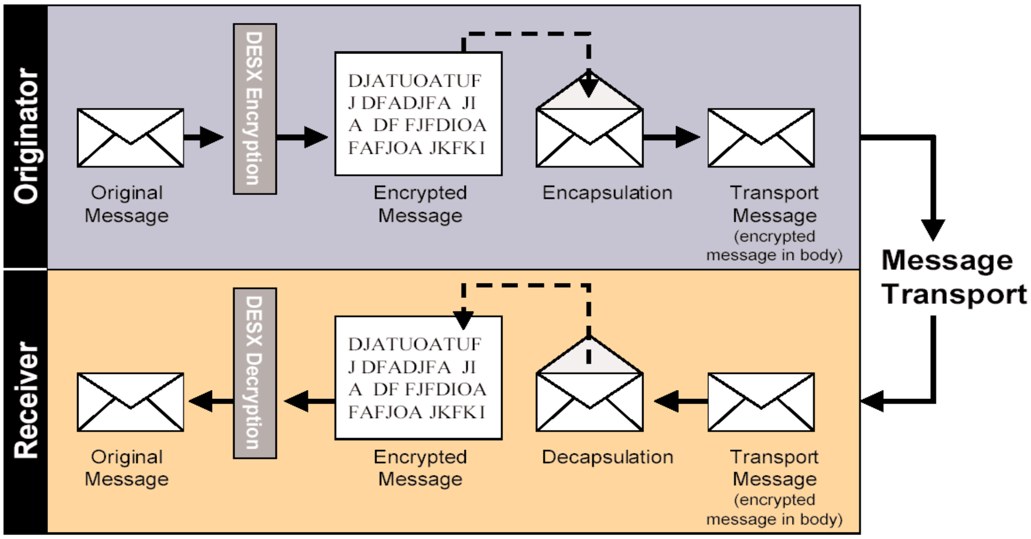
Provided a few configuration requirements are met, Palm MultiMail Deluxe requires no changes to the corporate firewall or corporate security policy. The corporate Exchange mail server is be configured to allow outbound and inbound SMTP, this is how messages are sent to and from the handheld. Additionally, in order to properly set-up the Palm MultiMail Deluxe solution the firewall must all outbound HTTP requests.

Encryption

Figure 3 illustrates the points at which the email message exists in its unencrypted and encrypted forms. Email messages are unencrypted only when behind the enterprise firewall or when on the Palm i705 handheld. All intermediate transmission is encrypted.

In order to send an encrypted email through the Palm MultiMail Deluxe system, the entire email message, including the header information, is encrypted and placed in the body of a wrapper email message before being transmitted across the network. The original email header (To, From, Date, Subject, etc.) is encrypted and placed in the body of the new email. The original body is encrypted and appended to the new body. Any attachments are omitted. The new Subject is

Figure 3 – End-to-end Encryption and Decryption Process*


Originator
Original Message
DESX Encryption
DJATUOATUF J DFADJFA JI A DF FJFDIOA FAFJOA JKFKI
Encrypted Message
Encapsulation
Transport Message (encrypted message in body)
Message Transport
Receiver
Original Message
DESX Decryption
DJATUOATUF J DFADJFA JI A DF FJFDIOA FAFJOA JKFKI
Encrypted Message
Decapsulation
Transport Message (encrypted message in body)

* When messages are sent to the Palm i705 handheld, Palm MultiMail Deluxe Desktop Link is the originator and Palm MultiMail Deluxe Email Client is the receiver. Conversely, when messages are sent from the handheld, Palm MultiMail Deluxe Email Client is the originator and Palm MultiMail Deluxe Desktop Link is the receiver.

an encrypted version of the original Subject. The encrypted message content is formatted to ensure that the encrypted parts of the new message are not changed as the new message travels through SMTP servers and email systems.

During installation, the MultiMail Deluxe Conduit generates a symmetric DESX encryption key using a non-predictable, random generation process. This key is stored in encoded format, and is shared between the desktop PC and the Palm i705 handheld during a HotSync® operation. Since the HotSync operation is performed using a cradle hard-wired to the desktop or via a LAN, the transfer of the keys is secure and is not susceptible to the security problems associated with key exchange over public networks. For added security, the user can configure the MultiMail Deluxe Conduit to generate a new key each time the handheld is synchronized with the desktop.

DESX is a cryptographic algorithm developed in 1984 by Ron Rivest for RSA Data Security. It is essentially a smaller, lightweight version of 3DES, in which secret values are combined using an ‘exclusive-or’ operation with a message block before and after an ordinary DES operation (the X in DESX stands for exclusive-or).

DESX uses three distinct keys, 56 bit + 64 bit + 64 bit, providing an effective key size of 184 bits with essentially no impact on encryption and decryption time while offering significant resistance to exhaustive key search decryption attacks on encrypted message information.

Cingular Wireless Network Security

Cingular is the wireless carrier for Palm wireless handhelds and the Palm MultiMail Deluxe system. The Cingular network is a closed network. The wireless network protocol provides a security feature called Closed User Groups (CUG). Only members of the Palm CUG are allowed to communicate with each other. Palm wireless handhelds communicate with the Palm.Net service via a single proxy address, which is mapped by the Cingular network to a specific set of Palm.Net servers in the same CUG. Traffic cannot be sent from a Palm handheld to a non-Palm.Net server, or from a non-Palm.Net server to a Palm handheld.

Upon connecting to the Cingular network, Palm wireless handhelds send encrypted authentication information to the network. If the authentication fails, the handheld is not allowed to communicate on the network.

Desktop Security & User Login Protection

Palm MultiMail Deluxe requires that the user’s PC be running and logged in to the corporate email network. A password protected screen saver is recommended security for the user’s desktop.

When MultiMail Desktop Link connects to the corporate Microsoft Exchange server, it uses (by default) the same login information supplied when the user logged into Microsoft NT. If the login fails, the user is prompted for their domain, username, and password. These dialogs are not part of Palm MultiMail Deluxe Desktop Link; they are part of the MAPI implementation from Microsoft. Palm MultiMail Deluxe Desktop Link does not store the domain, username, and password.

The Palm MultiMail Deluxe MultiMail Email Client software running on the Palm i705 handheld accesses the Palm.Net infrastructure using a username and password. This username and password are not connected in any way with the user's corporate username and password. The Palm.Net username and password are stored on the handheld as Palm preferences in clear text.

Before being transmitted to the Palm.Net infrastructure, these values are first base64 encoded within the protocol data payload to ensure that they are not recognized. Even if these Palm.Net values were known, the intruder could do nothing with them since the Palm.Net servers are not readily available on the Internet and the data contained within them is encrypted.

Handheld Information Protection

As more and more enterprise applications are developed for the Palm OS® platform, the need to secure information stored on handhelds has become a top priority for IT managers. Data security begins with basic password protection for locking access to the handheld and hiding records. Local password security is built into the Palm OS platform.

In addition, Palm OS version 4.x, which runs on all Palm i705 handhelds, supports security enhancements such as automatic password locking options, new encryption capabilities, and password hinting for forgotten passwords.

A number of Palm OS developers are delivering products that provide enhanced password protection. For example, one option requires pressing a specific combination of buttons, another requires the use of a stylus to write a unique character on the handheld screen, and yet another requires tapping a unique ID on an ATM-style keypad on the handheld screen before access is permitted. For more information on handheld security, see the Palm white paper, "Securing the Handheld Environment" http://www.palm.com/pdfs/securing_env.pdf.

Virus Protection

Any electronic platform can be susceptible to hackers who create viruses, and IT organizations need to be prepared. But safeguards built into the Palm OS platform protect user data on many levels, making Palm handhelds by nature very secure from these kinds of attacks. In contrast, handhelds based on the Windows CE operating system are far more vulnerable to the thousands of viruses that currently permeate the Windows world.

Palm handheld computers are not susceptible to viruses designed to attack the Windows platform (email attachment-based or otherwise), and also cannot be used to stage viruses passed to the handheld and then back to the desktop. For example, third-party products developed for the Palm OS platform, such as Documents To Go from DataViz, Inc. (www.dataviz.com) and QuickOffice from Cutting Edge Software (www.cesinc.com), remove macros from Microsoft Word and Excel files upon transmission to the handheld.

Conclusion

Palm MultiMail Deluxe gives mobile individuals a secure, convenient, fully manageable mobile solution for business and personal email. Because it runs on the user's desktop PC and the Palm i705 handheld and may require no changes to the corporate Exchange server or firewall, and because of "its secure architecture, the Palm MultiMail Deluxe email solution imposes no burden on corporate IT. It is a powerful way to give mobile individual workers access to their corporate email, enhancing their productivity and satisfaction.

For larger communities of enterprise users, Palm also offers a centrally managed enterprise solution for wireless, always-on email. The Palm Wireless Messaging Solution combines all of the established benefits of Palm handhelds—comprehensive information management with leading ease-of-use and wide solution breadth—with wireless email and wireless Internet/ intranet access. IT organizations benefit with easy, centralized installation that streamlines the process of providing wireless enterprise email access to large user communities.

The Palm Wireless Messaging Solution provides robust security features that ensure confidentiality and integrity of mission-critical wireless transmissions and extends Palm's proven track record for reliability throughout all elements of this enterprise-level solution including server software, client software, service and support, and wireless services and infrastructure.

palm™

Palm, Inc.
5470 Great America Pkwy.
Santa Clara, CA 95052
www.palm.com