



GoodLink 3.0 Security

White Paper
March 2004

Good Technology, Inc.
1-866-7-BE-GOOD
www.good.com

Contents

- I. Introduction..... 1
- II. GoodLink 3.0 Overview..... 3
- III. GoodLink 3.0 Security Architecture 6
- IV. Conclusion 10

I. Introduction

The Wireless Revolution Is Here

Executives and professional field forces are spending more time on the road doing business. These mobile professionals must be readily accessible to customers, partners, and fellow employees. In the past, this required that they carry laptops and use cumbersome and expensive remote-access systems such as virtual private networks (VPNs). Today, advances in handheld and network technology mean that laptops are no longer needed for secure mobile access to e-mail and mission-critical corporate information systems.

No longer just a luxury for top executives, mobile technology has become a necessity for field forces. Mobile access to corporate IT systems drives productivity and efficiency. Handheld and mobile applications are changing the way that companies, employees, and customers conduct business. These technologies can improve business processes in sales, service, marketing, and logistics, yielding substantial ROI.

The Security Challenge

For all the promise of these new technologies, security is the Achilles heel of the mobile revolution and must be addressed before the benefits can be fully realized.¹ Surveys of CIOs consistently show that security ranks as their top IT priority, ahead of such concerns as application integration, enterprise resource planning, and customer relationship management.²

Security breaches put at risk companies' most valuable information, including intellectual property, proprietary business processes, and customer data. As a result, CIOs demand stringent security standards to ensure that mobile users are allowed access to key enterprise data only as authorized, and that such data are safeguarded both during transmission and while resident on handheld devices.

¹ Matthew Kovar, Director, Security Solutions & Services Planning Service, The Yankee Group.

² "Morgan Stanley CIO Survey Series: Release 4.5," David M. Togut and Evan Bloomberg, Morgan Stanley Research, December 8, 2003.

Wireless Security Overview

Protecting the corporate IT infrastructure requires a deep understanding of the risks associated with mobile applications, devices, and networks. The move toward mobile data access extends the perimeter of the corporate network and, like earlier innovations, raises many security issues. In any client/server wireless system, a number of security challenges must be addressed. These include:

- **Network Perimeter Security.** When a corporation wishes to make Exchange information and intranet Web pages available wirelessly, the first priority is to maintain the security of the internal network. Any programs running inside the firewall must not open avenues of attack to programs running outside.
- **Transmission Security.** When internal information is transmitted over the public Internet and/or over a wireless network, the data must be protected against eavesdropping.
- **Handheld Security.** Once internal information is received and decrypted for viewing on a handheld device, that information must be protected against access by unauthorized users or programs on the handheld device.
- **Authentication.** Each component of a wireless system must be able to prove that it is authorized to communicate on the network. It must not be possible for an attacker to impersonate a device or server, thereby misleading authentic services into communicating with it.
- **Administrative Security.** In addition to traditional encryption and authentication, companies need to ensure that only the most senior system administrators can modify the infrastructure.
- **E-Mail Security.** E-mail programs are frequently attacked by users attempting to deliver viruses or unwanted messages. E-mail programs must defend against attacks that waste system storage, bandwidth, and the time of bona fide users.

GoodLink 3.0 was built specifically with corporate security in mind. This white paper will outline in detail the security features of the Good system.

II. GoodLink 3.0 Overview

The Good system is an end-to-end wireless real-time messaging and data-access system that enables mobile professionals to stay up-to-date. GoodLink provides mobile workers with an encrypted connection between their Microsoft Exchange Server®-based data and wireless handhelds (see Figure 1). Users can easily access up-to-date e-mail, contacts, calendars, tasks, and notes. They can also view rich attachments, including graphics, Word, and Excel files. GoodLink Forms provides wireless access to Web-based applications and information from corporate systems and public Web sites.

GoodLink is built on industry standards to provide enterprises with maximum flexibility when choosing wireless networks, platforms, and handhelds. With GoodLink, companies avoid getting locked into a proprietary wireless system. Today, GoodLink is available on the new Palm-OS-based Treo 600 Smartphone, Good™ G100 handheld, and RIM 950™ and RIM 957™ handhelds. Support for Pocket PC is coming soon.

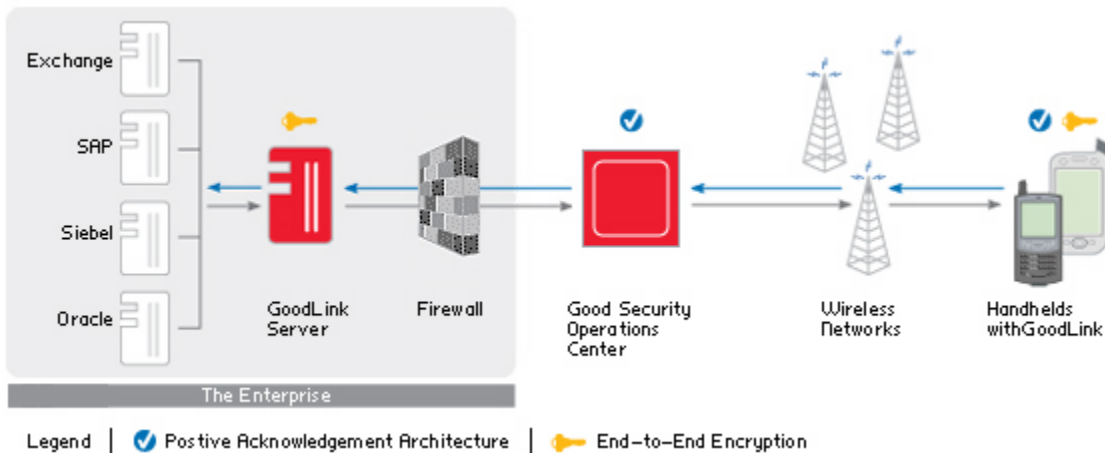


Figure 1. The Good System

The Good system is an integrated product suite that includes all the components necessary to support enterprise mobile workers.

GoodLink – offers up-to-date wireless access to all of Microsoft Outlook®, corporate intranets, and corporate data on Web-enabled enterprise systems for CRM, ERP, and SCM. The cradle-free system continuously synchronizes data between the wireless handheld and databases behind the firewall.

- **GoodLink Server** – offers enterprise-class security, exceptional reliability, and centralized fleet management. Specifically designed to meet the needs of IT managers, it reduces costs of deployment and support via its zero-desktop software architecture. GoodLink Server software monitors the user's Exchange mailbox and synchronizes any mailbox activity with the Good Security Operations Center, which then passes the e-mail and data through the wireless network to the user's handheld. Changes made on the handheld are sent to the Good Security Operations Center via the handheld's radio transmitter and the wireless network and return from the operations center via the GoodLink Server to Exchange. As a result, e-mail and data are available on both the user's desktop and handheld, ready to be read and filed from either location. Messages sent over the GoodLink System are encrypted end-to-end using AES and Triple-DES security technology.

- **GoodLink Forms** – provides wireless access to valuable corporate data, so that mobile users can complete critical tasks such as entering new customer information, checking order statuses, or reviewing a price list. Users can easily submit queries and receive responses via GoodLink e-mail. When out of coverage, users can queue requests, go on to other tasks, and receive responses once back in coverage. Responses are stored on the handheld and can be accessed whether online or offline until the user actively deletes them. GoodLink Forms relies on standards-based Web technologies including XML, CGI, and HTTP. Developers can leverage familiar tools to create lightweight forms that are easily distributed to users via e-mail. Installation is simple, with just one button to click.
- **GoodControl™** – provides IT managers with the centralized management and troubleshooting tools they need to manage a fleet of wireless handhelds. Tight integration with Microsoft Management Console (MMC) facilitates streamlined administration of users and servers.
 - **Good Management Console**

The Good Management Console simplifies user and server management, providing an integrated, centralized management console from which an administrator can set up, manage, and view users, as well as monitor servers and handhelds. IT managers can distribute management tasks across a hierarchy of administrators by using Role-Based Administration, which offers a set of roles, with varying permissions, for administering the GoodLink Server and users. By assigning appropriate roles to administrators, IT can better manage assets and increase security. Routine tasks, such as loading software, can be delegated to a wider group of administrators across multiple locations. More sensitive tasks, such as setting global policies or remotely erasing a handheld when it is lost or stolen, can be restricted to a smaller group.
 - **Good Monitoring Portal**

The Good Monitoring Portal is a Web-based monitoring system that allows administrators to manage GoodLink Servers and handhelds remotely. Administrators can easily use any Web browser to access server and handheld status. Potential problems can be tracked and resolved before they become serious. IT managers can provide higher levels of service, and users can achieve increased uptime. Administrators have access to server information including current server status, connection history, and a list of connected handhelds. They also receive alerts about available server software upgrades. Finally, IT administrators can also track current handheld status by device ID or by user e-mail address, and they can view connection history, server status, and coverage history; troubleshooting tools are available to resolve end-user problems.

- **Good Security Operations Center** –ensures reliable delivery by means of a unique multi-level Positive Acknowledgement Architecture that ensures that even when a device goes out of coverage, messages will be appropriately queued and then sent in order once the handheld is back in coverage. All data flowing through the Good Security Operations Center is encrypted with a unique, identical key known only to the customer to ensure maximum security (Figure 2).

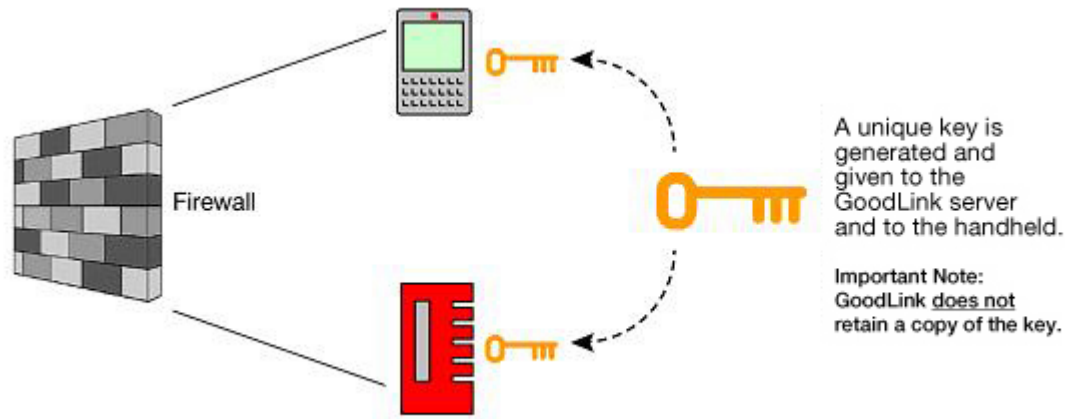


Figure 2. GoodLink Uses Shared-Key Exchange

The Good Security Operations Center also provides the following benefits:

- Customers benefit from 24x7 monitoring of carrier network status, which enables IT to troubleshoot potential problems before end users encounter them.
- Customers can deploy handhelds that run on several different networks—CDMA 1xRTT, GPRS, and Mobitex.
- Customers can create a single firewall configuration for the GoodLink Server.
- Customers get more timely delivery of messages and more efficient battery use on the handheld. The Good Security Operations Center is designed to contact handhelds that may have timed out on the network or have temporarily gone out of coverage. This approach is much more efficient than requiring the handheld to check for new messages on a scheduled basis.

III. GoodLink 3.0 Security Architecture

GoodLink 3.0 has been specifically designed to meet the security needs of even the largest, most security-sensitive corporations. It provides an end-to-end system designed to protect corporate information at all times—while it is being transmitted over the wireless network and while it resides on the handheld. The Good system combines industry security standards, such as AES and FIPS 140-2, with Good's own patent-pending security technologies. Installation of GoodLink does not require any modifications to the customer's firewall, and it renders other security software unnecessary.

Network Perimeter Security

Connections from the GoodLink Server to the Good Operations Center use HTTP and are protected by the Secure Sockets Layer (SSL). Since the connection is established in the outbound direction, there is no need to create an inbound opening in the corporate firewall. Most corporate security policies allow this type of traffic through port 443 without reconfiguring the firewall, but IT managers may use port 3101 or port 4662 instead.

Connections to the Good Operations Center are used only for sending data to and receiving data from handheld devices.

Transmission Security

End-to-End Encryption

When the IT administrator sets up a handheld device for a user, the GoodLink Management Console (GMC) generates an encryption key for that user and places identical copies of the keys on the handheld device and in the user's Exchange account. Once these keys are established, the GoodLink system uses end-to-end encryption to protect every message from the server to the handheld device and vice versa. Since the client and server share encryption keys, any attempt to use a different encryption key would cause decryption to fail and the message to be discarded. The Good Operations Center does not have access to the keys and cannot decrypt messages flowing through it.

The GoodLink Server can be configured to rotate the encryption key wirelessly for handheld devices, providing protection against unauthorized use of a compromised key, and/or simply changing the encrypted form of messages every 30 days.

AES

When a GoodLink 3.0 server is communicating with a GoodLink 3.0 client, all messages are encrypted using the Advanced Encryption Standard (AES). AES is a new Federal Information Processing Standard (FIPS) selected by the U.S. National Institute of Standards and Technology (NIST) for its combination of resistance to attack, ease of implementation, efficiency, and scalable design. GoodLink's implementation of AES uses key lengths of at least 128 bits.

Triple-DES

When a GoodLink server or client is using a version prior to 3.0, all messages are encrypted using VeriSign® Triple-DES encryption technology. Triple-DES is a strong encryption algorithm endorsed by NIST as a successor to the Data Encryption Standard (DES). Triple-DES uses the 56-bit DES calculation three times, for a total key length of 168 bits.

FIPS 140-2 Certification

The GoodLink wireless e-mail and data system is presently undergoing testing with NIST to obtain FIPS 140-2 certification. FIPS certification is a critical security standard for many government organizations. FIPS 140-2 certification covers the operation of GoodLink's cryptographic module, which implements AES

and Triple-DES. FIPS 140-2 also ensures the integrity of the cryptographic module in the field. Testing for FIPS certification is done by independent and accredited third-party laboratories.

Reliable Message Delivery

GoodLink uses a unique Positive Acknowledgement Architecture to confirm delivery of all messages, in the correct order with no duplicates, from the server to the handheld and vice versa.

Handheld Security

Locking the Device with a Password

The handheld device may be configured with a password. When the handheld device is locked, GoodLink will not display any of the user's data, and the device operating system turns off access to the serial (or USB) port, which could otherwise be used to download data from the handheld device to a PC. Access can be restored only by entering the correct password.

If an unauthorized user tries to guess the password too many times, the GoodLink client software will delete any GoodLink data stored on the handheld device.

IT Administration of Password Policies

The IT administrator can specify policies for the password provided by the user. These policies address:

- the requirement to have a password on the handheld device
- requiring the password to contain both letters and numbers
- requiring the password to contain both upper- and lowercase letters
- requiring the password not to have repeated characters
- requiring the user to choose a new password after a specified length of time
- requiring a new password to be unique among passwords recently chosen by the user
- the minimum length of the password
- the amount of time the device may be idle before the password screen is activated
- the number of failed password attempts allowed before the device clears all GoodLink data

When the user attempts to set a new password on the handheld device, the new password will be accepted only when it conforms to any policies set by the IT administrator.

Lost or Stolen Devices

If a user's handheld device is lost or stolen, the IT administrator can use the GoodLink Management Console to remotely disable the device and remove all GoodLink data.

Security Considerations for Treo 600 and Pocket PCs

On the Treo 600, GoodLink can use the external Secure Digital (SD) card to back up the GoodLink Client software and basic information, allowing GoodLink later to reconnect to the enterprise. This backup can be useful in the event that the battery drains completely, which causes memory on the Treo to be lost. Without the SD backup, the user would need to return the Treo to IT for reprovisioning. Information on the SD card is strongly encrypted with a passcode and is matched to the serial number of the handheld device, thus providing two-factor authentication for the SD backup.

On Pocket PC devices, GoodLink encrypts the local databases, which store the user's e-mail, calendar, contacts, notes, and tasks. Users can therefore choose to store GoodLink's databases either in RAM or on an external memory card. In either case, sensitive corporate data are protected using strong AES encryption.

If a Treo 600 user or a Pocket PC user is using desktop software (e.g., HotSync or ActiveSync) to synchronize other handheld applications, GoodLink's databases will not be copied onto the PC.

Authentication

GoodLink provides a number of safeguards against unauthorized access. The GoodLink Server resides behind a corporate firewall, and any handheld device attempting to contact it requires a three-step authentication process among

- the Good Operations Center and the GoodLink Server
- the handheld and the Good Operations Center
- the handheld and the GoodLink Server

Authenticating the Server

The Good Operations Center must first authenticate itself to the GoodLink Server before it can send data to or receive data from the handheld. It does this using SSL server authentication. Then the GoodLink Server authenticates itself to the Good Operations Center using a user name and password provided with the software-licensing package. Now the Good Operations Center is authorized to communicate with the GoodLink Server.

Authenticating the Handheld Device

The handheld connects with the Good Operations Center, and two checks are performed to ensure that the handheld is authorized to access GoodLink. First, the Good Operations Center ensures that the handheld has a valid service plan. Second, the handheld provides the unique serial number burned into its ROM and requests permission to communicate with a specific GoodLink server. The Good Operations Center checks its database of handheld serial numbers and GoodLink Servers with which each handheld is authorized to communicate. If the handheld device passes both of these tests, it is authenticated to the Good Operations Center, but is not yet permitted to access enterprise data managed by a customer's GoodLink Server.

Connecting Server and Client

The handheld must be explicitly authorized to talk to the GoodLink Server. This authorization is handled for customers by the Good Operations Center. Once the handheld is authorized to communicate with a customer's GoodLink Server, the user can access enterprise data and can send and receive information. Any unauthorized traffic cannot be routed to a customer's GoodLink Server and is discarded.

Administrative Security

GoodLink 3.0 offers role-based-administration (RBA) features that allow system-administration permissions to be customized according to the needs and qualifications of each user. By controlling users' access according to their roles and the associated permissions, RBA provides a tool for managing IT assets and increasing security. Routine tasks—such as adding a new user or loading software—can be delegated to a wider group of IT managers across multiple locations. More sensitive permissions, such as those required for setting global policy, can be restricted to a smaller group, increasing the overall security of the system. RBA also encourages the most efficient use of IT resources, since permissions can be based on skill and job function.

Among the permissions that can be granted to administrators:

- Create new user
- Load handheld software
- Delete user
- Erase handheld data
- Manage GoodLink Server
- Set global policy
- Change user policy
- Manage roles

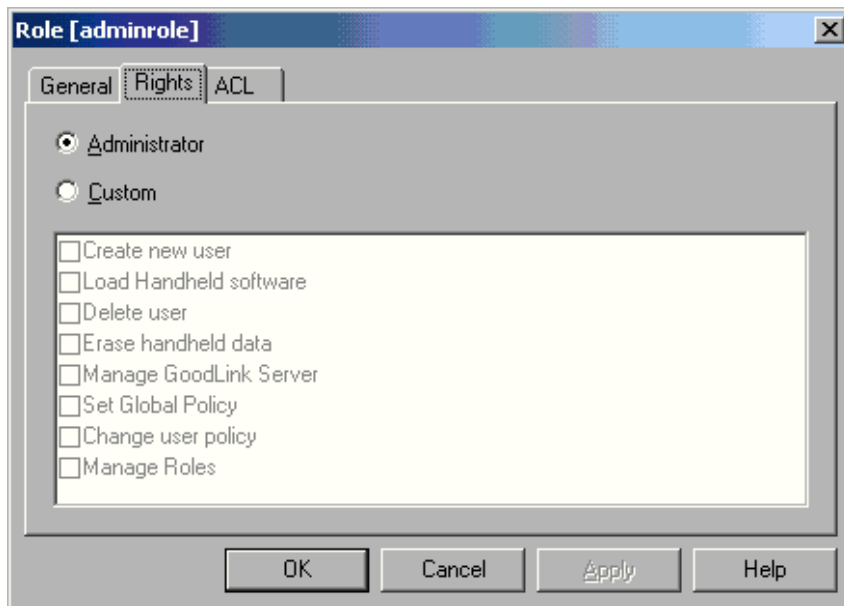


Figure 3. The GoodLink 3.0 Role-Based-Administration Screen

E-Mail Security

Protection Against Viruses

Preventing the spread of viruses is of increasing concern for IT departments and end users. Viruses commonly infect a user's system by delivering executable code, such as .EXE files or Visual Basic scripts, via an e-mail or an e-mail attachment, and getting the user to run the code inadvertently. The GoodLink application will not run executable code within an e-mail or attachment and thus is less vulnerable to viruses from e-mail. GoodLink users can use their handhelds to read e-mails or attachments without concern about viruses. If the user suspects an e-mail to be malicious, he/she can safely delete that e-mail from his GoodLink device rather than risk opening it from the laptop or desktop.

Signed Messages

GoodLink also incorporates VeriSign's technology for digital-ID-signed e-mail, which serves as an electronic substitute for sealed envelopes and handwritten signatures. This security feature enables users to digitally sign e-mail messages to assure recipients as to the sender of such e-mail. E-mail contents and attachments are also further encrypted, protecting them from being read by online intruders. Only the intended recipient can decrypt and view these messages.

IV. Conclusion

No longer just a luxury for top executives, mobile technology has become a necessity for field forces. Mobile access to corporate IT systems drives productivity and efficiency. However, for mobile deployments to succeed, they must be planned and executed with security in mind. Protecting the corporate IT infrastructure requires a deep understanding of the risks associated with mobile applications, devices, and networks. In any client/server wireless system, a number of security challenges must be addressed. These include security for the following areas: network, transmission, handheld, authentication, administrative, and e-mail. When deployed securely, handheld and mobile application technologies can improve business processes and yield substantial ROI with lower TCO.