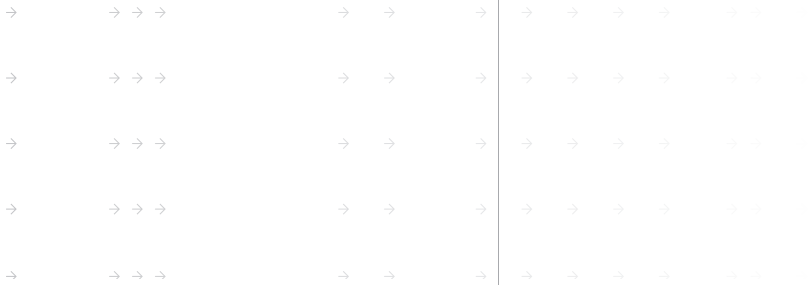




**Integrated**  
COMMUNICATIONS



↗ **GoodLink™ 4.0 Security** WHITE PAPER  
GOOD FOR BUSINESS, GREAT FOR YOU



# CONTENTS

<b>I.</b>	<b>INTRODUCTION</b>	<b>1</b>
<b>II.</b>	<b>GOOD SYSTEM OVERVIEW</b>	<b>3</b>
<b>III.</b>	<b>GOOD SYSTEM SECURITY ARCHITECTURE</b>	<b>6</b>
<b>IV.</b>	<b>GOOD SECURE OVER-THE-AIR (OTA) ARCHITECTURE</b>	<b>11</b>
<b>V.</b>	<b>CONCLUSION</b>	<b>14</b>

→ → →

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→ → →

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→ → →

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→ → →

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→ → →

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→



# I. INTRODUCTION

## THE WIRELESS REVOLUTION IS HERE

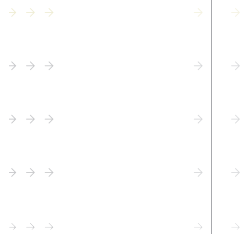
Executives and professional field forces are spending more time on the road doing business. These mobile professionals must be readily accessible to customers, partners, and co-workers. In the past, this required that they carry laptops and use cumbersome and expensive remote-access systems such as virtual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

No longer just a luxury for top executives, mobile technology has become a necessity for field forces. Mobile access to enterprise information systems drives productivity and efficiency. Handheld 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.<sup>1</sup> 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.<sup>2</sup>

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.



<sup>1</sup>Matthew Kovar, Director, Security Solutions & Services Planning Service, The Yankee Group.

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



## WIRELESS SECURITY OVERVIEW

Protecting enterprise IT infrastructure requires a deep understanding of the risks associated with mobile applications, devices, and wireless networks. The move toward wireless 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 enterprise systems like Exchange, CRM, ERP, or intranet Web pages accessible 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 from 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.
- **Over-the-Air (OTA) Provisioning and Software Installation.** To minimize IT costs, enterprises need the ability to securely deploy and manage a fleet of mobile handhelds and applications remotely, without having to physically touch the device. Good's Secure OTA capability encompasses several features, including provisioning, upgrading, installation of third-party software, and handheld policy updates.

The Good System was built specifically with enterprise security in mind. This White Paper will outline in detail the security features of the Good System.





## II. GOOD SYSTEM OVERVIEW

The Good System is an end-to-end wireless real-time messaging and enterprise application access system that provides mobile professionals with the up-to-date information when and where they need it. The Good System provides mobile workers with an encrypted connection between their behind-the-firewall enterprise systems and wireless handhelds (see Figure 1). Users can easily access up-to-date e-mail, contacts, calendars, tasks, and notes, as well as information from other systems like CRM, ERP, or business intelligence. They can also view rich attachments, including graphics, Word, and Excel files. GoodLink Forms provides wireless access to a range of enterprise systems, including packaged applications like CRM and ERP, legacy systems and databases, as well as intranets and public Web sites.

The Good System is built on industry standards to provide enterprises with maximum flexibility when choosing wireless networks, platforms, and handhelds. With Good, companies avoid getting locked into a proprietary wireless system. Today, GoodLink™ is available on the Palm™ OS and Pocket PC handhelds and smart-phones with Symbian support coming soon.

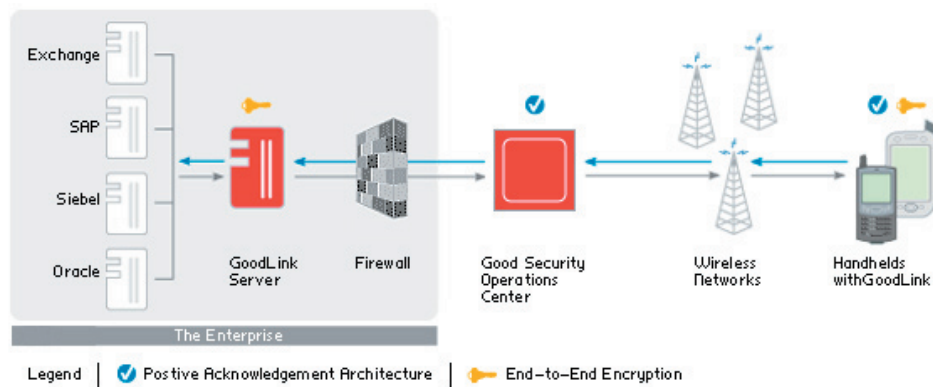


Figure 1. The Good System

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 the functions of Microsoft® Outlook®, including e-mail, calendar, tasks, and activities. The cradle-free system continuously synchronizes data between the wireless handheld and Exchange servers 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 Advanced Encryption Standard (AES) security technology.



- **GoodControl™**—provides IT managers with the centralized management and troubleshooting tools they need to manage a fleet of wireless handhelds and smartphones. Tight integration with Microsoft Management Console (MMC) facilitates streamlined administration of users and servers.

#### GOOD MANAGEMENT CONSOLE

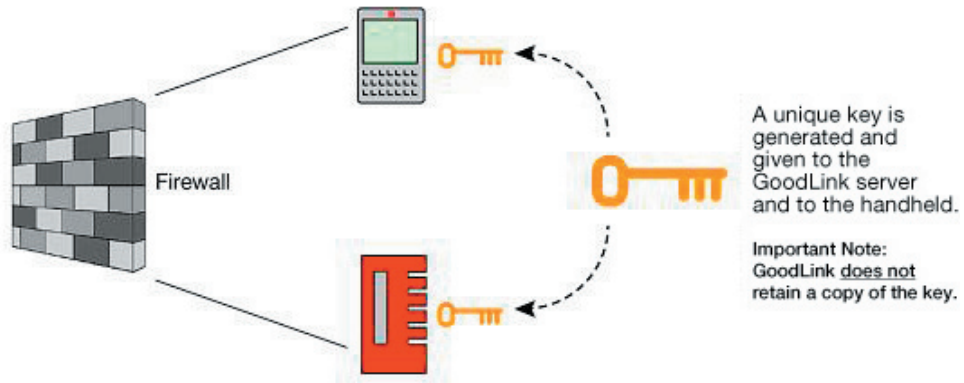
The Good Management Console simplifies user and server management, providing an integrated, centralized management console from which an administrator can set up, manage, and view users, as well as monitor servers and handhelds. IT managers can distribute management tasks across a hierarchy of administrators 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).

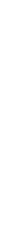
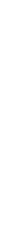
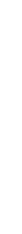
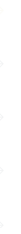




**Figure 2. Good System Use of Shared-Key Exchange**

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. GOOD SYSTEM SECURITY ARCHITECTURE

The Good System 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 Good applications does not require any modifications to the customer's firewall, and allows you to leverage your existing network security infrastructure.

#### NETWORK PERIMETER SECURITY

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

#### End-to-End Encryption

When the IT administrator sets up a handheld device for a user, the Good 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, GoodLink uses end-to-end encryption to protect every message and transmission 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 Security 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 server is communicating with a GoodLink client, all messages are encrypted using the AES. AES is a Federal Information Processing Standard (FIPS) selected by the US National Institute of Standards and Technology (NIST) for its combination of resistance to attack, ease of implementation, efficiency, and scalable design. Good's implementation of AES uses key lengths of at least 128 bits.

#### FIPS 140-2 Validation

The Good System has successfully completed testing with NIST and obtained FIPS 140-2 certification. FIPS certification is a critical security standard for many government organizations. FIPS 140-2 certification covers the operation of Good's cryptographic module, which implements AES encryption. FIPS 140-2 also ensures the integrity of the cryptographic module in the field. This certification applies to both the Treo and Pocket PC product families.



#### Reliable Message Delivery

The Good System 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, Good applications 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 Good client software will delete any Good application 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 uppercase 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 Good application 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 GMC to remotely disable the device and remove all Good application data.

#### Security Considerations for Devices with Secure Digital (SD) Cards

On handhelds that support external SD cards, Good applications can be backed up, allowing GoodLink to later reconnect to the enterprise. This backup can be useful in the event that the battery drains completely, which causes memory on some handhelds to be lost. Without the SD backup, the user would need to return the handheld to IT for re-provisioning or go through complete re-provisioning via Good Secure OTA. Information on the SD card is strongly encrypted with a passcode and is matched to the serial number of the handheld, 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 user is using desktop synchronization software (e.g., HotSync or ActiveSync) to synchronize other handheld applications, GoodLink's databases will not be copied onto the PC.

**AUTHENTICATION**

The Good System 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 Security 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 Security Operations Center using a user name and password provided with the software-licensing package. The Good Security Operations Center is then authorized to communicate with the GoodLink Server.

Authenticating the Handheld Device

The handheld connects with the Good Security Operations Center, and two checks are performed to ensure that the handheld is authorized to access GoodLink. First, the Good Security 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 Security 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 Security 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 a GoodLink Server. This authorization is handled for customers by the Good Security 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**

The Good System 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
- Set global policy
- Change user policy
- Manage roles

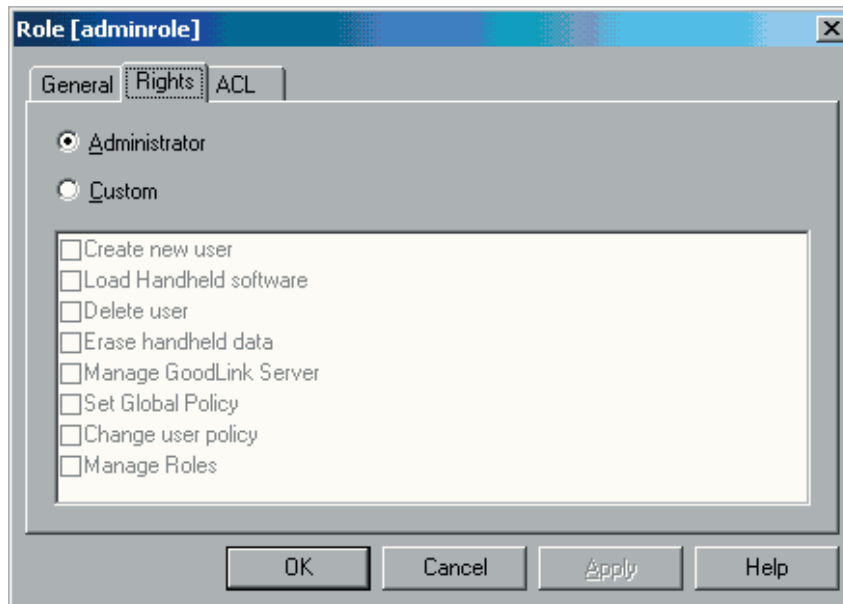


Figure 3. The Good Role-based Administration Screen



## 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 their GoodLink device rather than risk opening it from the laptop or desktop.

### Signed Messages

GoodLink also incorporates VeriSign® technology for digital-ID-signed e-mail, which serves as an electronic substitute for sealed envelopes and handwritten signatures. This security feature enables GoodLink users to read messages which have been digitally signed, even if the message body was not sent in clear text.

→ → →

→ → →

→ → →

→ → →

→ → →

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→

→



## IV. GOOD SECURE OTA ARCHITECTURE

### OTA PROVISIONING SECURITY CONSIDERATIONS

GoodLink 3.7 and earlier required every handheld to be physically connected to an administrator's PC behind the corporate firewall. Beginning with GoodLink 4.0, Good provides Secure Over-The-Air (OTA) setup of GoodLink, without ever giving the handheld to IT.

The Secure OTA capability encompasses several features, including GoodLink provisioning, GoodLink software upgrades, installation of third-party software, and handheld policy updates.

#### Good Secure OTA Process Flow

In order to explain the security model, the high-level process flow for Good Secure OTA setup of handhelds is as follows:

1. The IT administrator gives permission for a user to provision wirelessly OTA, not knowing anything about the handhelds the user will eventually try to provision.
2. The GMC generates a random 15-character PIN, and emails the PIN to the user, along with instructions for OTA provisioning.
3. Good's Security Operations Center stores the user's email address, GoodLink Server name, and a hash of the PIN.
4. The end user downloads the Good OTA Setup from <http://get.good.com> using the Web browser on the handheld.
5. When Good OTA Setup runs, it asks the user to enter their email address and PIN.
6. The Good OTA Setup initiates the authentication sequence.
7. After the authentication sequence succeeds, Good OTA Setup downloads a package of provisioning information from the GoodLink Server.
8. Once Good OTA Setup receives the provisioning info, it downloads the GoodLink client software and runs it.
9. When the client runs, it performs the normal provisioning process, connecting each of the client applications with its server behind the firewall.
10. This process may be repeated if the client application is deleted from the handheld, perhaps because the battery drained completely. Note that the PIN is not stored by Good's client software – it must be provided again by the end user. Once a handheld is provisioned using a PIN, the PIN can not be used with any other handheld.



### Access Control

IT administrators must explicitly give permission for users to provision OTA. Permission may be given for a group of users selected from the Exchange GAL. If the IT administrator has not given permission for a user to provision OTA, the Good Security Operations Center will prevent Good OTA Setup from communicating with the GoodLink Server behind the firewall.

### Network Perimeter

As described previously, the Good System does not require any inbound connections through the enterprise firewall. This advantage is maintained for Good Secure OTA. All communications between Good OTA Setup and the GoodLink Server run through the same outbound connection that GoodLink normally uses. Good OTA Setup initiates a connection to the Good Security Operations Center, and once the authentication sequence has succeeded, Good OTA Setup is permitted to use the network channel between the Good Security Operations Center and a GoodLink Server.

### Authentication

When the OTA Installer runs, it first authenticates to the Good Security Operations Center. Good's Security Operations Center does not store the user's PIN, rather it stores a one-way hash of the PIN and uses that hash to provide authenticated access to the OTA provisioning system, based on the user's email address.

Once the user is authenticated to the Good Security Operations Center, the Security Operations Center permits Good OTA Setup to negotiate an authentication protocol with the user's GoodLink Server. In the initial release of OTA, an authentication protocol is used where the client and server each encrypt data with the user's PIN. The PIN itself is not transmitted. If the authentication sequence fails more than 10 times, the Good System assumes that an unauthorized user is attempting to gain access, and that user is prevented from making further attempts.

The GMC contains a new right for which IT administrators can enable users for OTA provisioning. When an authorized administrator uses the GMC to generate a PIN, it is sent to the end-user via email. Since the PIN is confidential, it is not shown to IT by default. The GoodLink Service administrator may choose to make the PIN accessible to some IT administrators using a new right in GMC. This may be necessary to provision a user who does not have access to his or her corporate email. If desired, Good OTA Setup can use a PIN longer than 15 characters. The length of the PIN is provided in a Windows® Registry key on the GoodLink Server machine.

### Traffic Encryption

In order to protect all traffic between Good OTA Setup and the GLS, all communication during the provisioning process runs over HTTP/SSL. The package of provisioning information is further encrypted using an AES key derived from the user's OTA PIN. After the client receives the package of provisioning information, it begins to use the normal end-to-end encryption capabilities that GoodLink uses after provisioning a handheld at the management console.

## OTA SOFTWARE INSTALLATION SECURITY CONSIDERATIONS

The Good OTA software distribution system supports distribution of three classes of software: Good applications, Good partner applications, and custom applications provided by a customer's internal IT department.



### Digital Signatures

Good software and partner software is digitally signed using X.509v3 certificates. When Good OTA Setup downloads the GoodLink client, it checks the signature value and the validity of Good's certificate. If signature verification fails, we recommend that users not install the software. In addition, the certificate used to sign the software package is checked against the Certificate Revocation List (CRL) published by VeriSign, Inc.

### Encryption

When the IT department wants to provide an application for their users, it is possible that the application contains confidential information, e.g., a trading application for a financial services company. Therefore, before the custom software package is uploaded, it is encrypted using a key generated by the GMC using Microsoft's CryptoAPI. The key is then communicated to the client via Good's AES-encrypted communications channel.

### Software Versions

The GMC provides a policy for IT to specify the version of client software which will be installed. The OTA Installer receives this policy in the provisioning info, and downloads the correct version. In this way, IT can ensure that users receive the client software which has been tested and approved.

### Mandatory Installation

IT may mark software packages as mandatory or optional. If a software package is optional, users may decline to download and install it. If a software package is mandatory, the GoodLink client will automatically download and run the installer for that application. In either case, users may defer the installation for a short time if they are using the handheld and do not wish to be interrupted.

### Off-Peak Downloads

When IT changes a software policy for all users on a GoodLink Server, the GoodLink client will begin the download at a random time overnight. This is designed to prevent overloading wireless infrastructure by having a large population of users all downloading a large program at the same time. Individual users may override this setting and begin the download immediately.

