White Paper: Handheld and Smartphone Security for Mobile Business

palmOne™

Mobile Computing: Opportunities and Risk

By providing on-the-go professionals with convenient mobile access to email, business applications, customer information and critical corporate data, businesses can help employees become more productive, streamline business processes and enable better decision making. But these benefits are not without risks. Sensitive corporate information stored on and transmitted by mobile devices is vulnerable. With the new ease of access to information comes a responsibility to protect the corporation's data as well as the investment in mobile devices.

In many ways, security risks for mobile computing are similar to those for other computing platforms. There are the usual concerns of protecting data, authenticating users, and shielding against viruses and other malicious code. But because of their mobility and compact size, handhelds and smartphones present some additional challenges:

- Handhelds and smartphones are more easily lost or stolen than laptop or desktop computers.
- Users often treat handhelds and smartphones as personal devices and must be trained to consider the security risks when they use these devices to access corporate data and networks.
- Because handhelds and smartphones frequently connect wirelessly, robust wireless security becomes essential.

Fortunately, the technology necessary to secure mobile access to corporate networks exists today for palmOne™ handhelds and smartphones. Strong security is multi-layered and must be woven into the very fabric of an organization. This paper examines some of the key issues in mobile security and discusses security solutions for palmOne handhelds and smartphones.

Foundations of Handheld and Smartphone Security

As more and more mission-critical data is accessed with mobile devices, securing that information becomes a top priority for IT. The key to reducing the risks associated with mobile computing is establishing, communicating and enforcing strong corporate security policies. However, security threats and solutions seem to change continuously. What criteria can be used to choose security standards and policies with confidence?

Start with Standards

Industry and federal standards and best practices provide an excellent starting point for formulating your business' security strategy. Standards are a critical component of the information industry, enabling hardware and software from different manufacturers to work together. Organizations such as ISO (International Organization for Standardization) and IEEE (Institute of Electrical and Electronics Engineers) bring together experts to solve hard problems and create new standards.

Depending on the nature of the business, government regulations and laws may influence technology selection. In the United States, the National Institute of Standards and Technology (NIST) develops standards and guidelines for federal computer systems, which are issued as Federal Information Processing Standards (FIPS). Many U.S. federal agencies are required to use FIPS-certified technology, and many private-sector businesses regard FIPS certification as evidence of high quality security.

palmOne's Crypto Manager is FIPS 140-2 certified. Crypto Manager can be used to provide strong cryptographic services to Palm OS® applications, ensuring that critical security functions such as encryption, decryption, key generation, checksums, and pseudo random number generation are performed correctly. For more information on Crypto Manager, see Certificate #322 at http://csrc.nist.gov/cryptval/140-1/1401val2003.htm

The Health Insurance Portability and Accountability Act (HIPAA) sets standards for healthcare plans, clearinghouses and providers that handle protected health information. The safeguards that comprise HIPAA's Final Security Rule focus on protecting "data integrity, confidentiality and availability" of individually identifiable health information. The many strong security solutions for palmOne handhelds and smartphones

enable healthcare entities to implement HIPAA-compliant mobile solutions. For more information on making mobile devices conform to HIPAA, see *Achieving HIPAA-Compliance with palmOne™ Handheld and Smartpho Solutions* at: http://www.palmone.com/us/pdfs/HIPPA8a.pdf.

When forming your corporate security strategy, industry and government standards are an excellent source of guidance. At palmOne™ , our philosophy is to use standards whenever possible. Choosing palmOne means your devices will interoperate with a wide selection of operating systems and applications.

Establish Security Policies

Sound corporate policies are the foundation for preventing costly security breaches. Convicted hacker Kevin Mitnik testified that social engineering was his primary method of gaining entry to corporate systems. In Mitnik's own words: "I was so successful in that line of attack that I rarely had to resort to a technical attack." [1]

One of the best ways to counteract social engineering is to establish, communicate and enforce strong corporate policies. Even before issuing devices to users, it is wise to first train them on your organization's security policies and practices. Here are some best practices for creating security policies:

1. **Extend current security policies to mobile devices**. For example, if corporate desktops require an eight-character alphanumeric password, so should the handheld or smartphone. Every machine that stores or accesses corporate data is a point of vulnerability and should be protected. Also, consistent policies reduce both administration and user training time.
2. **Leverage existing infrastructure.** Your existing infrastructure, such as user directories and monitoring systems, can be leveraged to reduce redundant systems and enforce security policies. Many mobile business solutions support LDAP (Lightweight Directory Access Protocol), Active Directory, RADIUS and other user directories. Server-based solutions should generate logs that can be analyzed by your corporate monitoring system. Leveraging your infrastructure will lower total cost of ownership, reduce administrative overhead, and minimize human error.
3. **Choose standards-based practices and solutions.** Using open standards enables hardware and soft-ware from disparate manufacturers to work together. Industry, government and de facto standards provide vetted guidance (e.g. FIPS, Common Criteria, EAP-LEAP)

Once corporate policies have been established, it is wise to continuously check and enforce your policies. Systems management solutions are a good way to automate policy enforcement. For example, systems management software can enforce password policy and ensure only authorized users can synchronize to the network. Many palmOne Solution Providers offer systems management solutions with useful features such as:

- Asset inventory
- Knowledge of who is synchronizing to your network
- Synchronization prevention if user authentication fails
- Synchronization prevention if the security application is not installed
- Distribution of software and configurations

To go a step further, if company policy calls for strong passwords, Administrators can test whether users have set sufficiently strong passwords with tools like L0phtCrack.

Some forward-thinking companies have a Chief Security Officer who determines security policies for the entire organization. More commonly, security experts are dispersed throughout the organization. For such organiza-tions, it is helpful to convene these experts as needed to create corporate policies, share best practices, and select core systems.

When the corporation demonstrates that security is taken seriously, employees will also take it seriously. Security policies should be consistent, centrally administered, and enforced. Such policies simplify management and reduce error while ensuring that all parts of the organization are protected.

Know Thy Enemy: Security Risks

When forming a security strategy for mobile devices, the first step is to first analyze the potential risk factors. Based on the relevant risks for your organization and applications, form a security plan that effectively counters each risk. The major security threats with mobile devices are theft and loss, password cracking, data interception, malicious code and host intrusion.

Theft and Loss

The same factors that make handhelds and smartphones attractive to mobile users— their portability, conven-ience and access to mission critical data— also make them attractive to thieves. Despite a user's best efforts, a device may be stolen or lost, placing sensitive data at risk.

1. Schneier, Bruce, *Secrets and Lies,* 2000

To prepare for this eventuality, IT should implement the following precautions for every handheld and smartphone that contains corporate data:

- **Mandate authentication**. Power-on authentication prevents unauthorized users from gaining access to the device itself and any networks accessible by the device. While all palmOne™ handhelds and smartphones allow the user to activate password protection, users can also turn off password protection. If users are carrying sensitive data, palmOne™ recommends installing security applications that allow Administrators to enforce authentication policies. Administrators then control attributes such as whether or not a password is required, length and strength of password, and expiration.
- **Encrypt sensitive data**. Any data that the enterprise wants to protect should be encrypted when not in use. Data should also be encrypted before it is transmitted. Effective encryption protects data from thieves and hackers.
- **Back up data regularly.** A recent backup enables quick restoration of lost applications and data in order to minimize user downtime. Administrators should practice configuration management and conduct regular backups so that user data and profiles can be easily restored.
- **Establish procedures for revoking access permissions.** Permissions dictate who can access the corporate network from the mobile device. If a device is lost or stolen, Administrators must be ready to quickly remove access permissions to all corporate resources. Centralized directories such as LDAP make revoking permissions quick and easy.

If these measures are taken, corporate data will be protected even if the device falls into the wrong hands. And the user will be able to return to productivity quickly.

Password Cracking

With the availability of automated password cracking tools, the security threat of password compromises has received a great deal of publicity. The most common automated attack is a "dictionary attack," where a cracker launches a program that uses a dictionary to generate password after password until a successful combination is found. To thwart dictionary attacks, follow these best practices:

- **Limits login attempts.** Many operating systems can be configured to lock a user ID after a set number of failed login attempts. This is the single best way to defeat dictionary attacks.
- **Use password generators.** If users are not allowed to generate their own passwords, they cannot pick easy-to-guess passwords. Some generators create only pronounceable non-words to help users memorize their password.
- **Enforce password policies**. Users can be instructed, or the system can force them, to select passwords (a) with a minimum length, (b) with special characters, (c) unrelated to their user ID, or (d) that are not in an online dictionary. The downside of suggestions 2 & 3 is that users are more likely to write down their passwords.
- **Change passwords regularly.** Periodic password changes can reduce the damage done by stolen passwords. Too frequent changes, however, can be irritating to users.

Despite the very real threat of automated password cracking tools, the most common method of compromising passwords continues to be social engineering. By applying the best practices above And training users to defend against social engineering, your systems will be well-protected against password cracking.

Data Interception

Today's handhelds and smartphones offer a variety of ways to access and transmit data, including wireline, infrared (IR), wireless LAN (Local Area Network) technology like Bluetooth and 802.11, and wireless WAN (Wide Area Network) connectivity. As handhelds and smartphones become increasingly connected to public networks, the danger of data interception rises.

Wireless networks are particularly vulnerable to data interception since data is transmitted over the air and it is harder to enforce a physical boundary. There has been a flurry of press recently about the ease of intercepting wireless transmissions, particularly in 802.11 networks. If unencrypted data is intercepted, not only is the current data compromised, but the eavesdropper may be able to determine the identities of the communicating parties. Once an identity is obtained, the perpetrator can masquerade as a legitimate user and send false messages or access system resources. (This is often referred to as a "man-in-the-middle attack"). By implementing sound security procedures such as authentication, data encryption and message integrity checking, corporations can safeguard their data and communications. We discuss network specific security technologies and products below in *Protect Data Across the Network*.

Malicious Code

Malicious code can take the form of viruses, worms, or Trojan horses. Viruses are codes that attach themselves to host programs and propagate to other programs when the infected program executes. As they execute, they can

3

destroy or alter data. Worms perform pre-programmed attacks on networked computers. Trojan horses are programs that masquerade as a harmless application while performing a hostile action (such as creating a vulnerability on the computer or covertly sending data back to the code's creator).

The malicious code may execute on the device itself or on networked computers once an infected file is transferred onto the network. Infections are generally transmitted through email attachments. A messaging server that inspects attachments before sending them to the device can mitigate this risk. In addition, an anti-virus program with up to date signature files is essential for preventing infection of critical enterprise files and data. IT Administrators should have enforceable policies for running virus scans whenever new files are downloaded and for keeping the virus signature files up to date. If data is corrupted, a recent backup can quickly restore the system to health.

Digitally signed code can be used to verify authenticity and integrity. Authenticity means that the code is indeed from the stated developer or another trusted party. Integrity means that the code has not been altered since it was signed. Signing code entails taking a hash of the code, then encrypting that hash with the code signer's private key, or digital signature. This digital signature is then embedded in the code. Before installing or running the code, the receiving party verifies the validity of the digital signature, using the signer's public key. Signed code should be verified prior to installing or launching applications.

Host Intrusion
Intrusion typically refers to a hacker or cracker taking advantage of background services to break into your machine. Background services give hackers an entrance into your system. Preventing just such an event is why personal firewalls have become such a big business. By this definition, intrusion is not possible with today's palmOne devices. Why? Simply, Palm OS® does not run application services in the background. Thus, palmOne™ handhelds and smartphones today do *not* need a firewall. Currently, the only way for a hacker to put malicious code on your palmOne handheld or smartphone is through beaming, synchronization or wireless downloads. These routes can and should be protected by authentication, antiviral software and security policies, as discussed in previous sections.

Intrusion detection is equally as critical as prevention. Logging and monitoring are powerful tools in intrusion detection. Server-based applications should incorporate logging and SNMP (Simple Network Management Protocol) support to provide a foundation for detection and response. Logging is the process of recording system actions and events. When events are logged, normal usage patterns can be discerned by analyzing logs over time. Deviations from normal usage patterns may be a red flag. A management solution, such as Intellisync™ Mobile Suite, generates transaction logs of user activity. These logs can be loaded into the organization's monitoring system to automate analysis and alerts.

Extending Security to Handhelds and Smartphones
When extending business applications to handhelds and smartphones, it is important to maintain the same levels of performance, privacy and reliability that users have become accustomed to within the walls of the corporate office. Organizations face the challenge of selecting security measures that balance resource protection with usability and cost.

palmOne handhelds and smartphones incorporate security at all levels: operating system, built-in applications, and innovative security solutions from palmOne Solution Providers. Palm OS 5 is an ARM-based operating system that features a strong encryption architecture, secure communication using SSL, and unique device identification. Palm OS® Garnet, an enhanced version of Palm OS 5, introduces new features such as a JVM, full motion video, and always-on communications.

The recently announced Palm OS® Cobalt is a robust, frameworks based operating system. Palm OS Cobalt features multi-threading, multitasking, STREAMS-based communications, enhanced multimedia and graphics capabilities, and a strong security framework. Look for Palm OS Cobalt, formerly named Palm OS 6, in future palmOne handhelds and smartphones.

Protect Data on the Device
Handheld and Smartphone Authentication
The purpose of authentication is to prove that a party is who he or she claims to be. The first level of authentication involves accessing the device itself. Authentication protects corporate data and network access in the event of theft. Desktop computers can easily be physically secured: they can be locked in an office and bolted to a desk. Because handhelds and smartphones are more difficult to secure physically, it is important to ensure that if an unauthorized person gains possession of the device, they will not be able to activate it. Every device running Palm OS has built-in password protection. This simple yet effective application has no back doors and includes features such as automatic locking options and hints for forgotten passwords. To ensure privacy, the password is hashed using MD5 and only the hash value is stored.

Select palmOne™ Tungsten™ handhelds include Security 5p, an enhanced security application that features:
- **Data Encryption.** Users have the choice of two 128-bit encryption algorithms: AES (Advanced Encryption Standard) or RSA Security's RC4. Also, users can choose to encrypt all data or only selected data.
- **FIPS-certified cryptography.** AES encryption services are provided by palmOne's™ FIPS 140-2 certified Crypto Manager
- **Intrusion Protection.** The best way to guard against a dictionary attack is to limit the number of failed password attempts. With Security 5p, users can set a limit for failed password attempts, and then select an action to be taken when the limit is exceeded: delete all data or delete private records only.
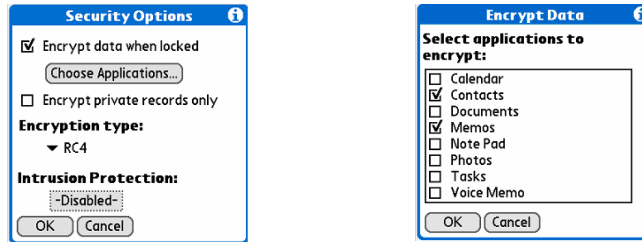
Exhibit A: Encrypting Data with Security 5p

Managed security solutions from palmOne Solution Providers enable the IT Administrator to enforce device security policies. The Administrator can make password protection mandatory for the user and set policies such as length and type of password, frequency of password change and timeouts, as well as control encryption and application access. In addition, such applications protect against dictionary attacks with data-wipe functionality. Policies are persistent on the device and can only be changed by the designated Administrator.

Biometric authentication combines convenience with strength. A variety of biometric authentication methods, such as handwriting and fingerprint recognition, are available for the Palm OS® platform. Authentication thresholds can be set to optimize data security (lower number of false positives) or to minimize user frustration (lower number of false negatives).

Data Encryption
Encryption is one of the pillars of data security and is an important tool for protecting sensitive data. Modern crypto-graphic techniques use a combination of a cipher and a key to maintain privacy. The strength of the privacy de-pends on the strength of the algorithm and the size of the key, measured in number of bits. Any data that is stored on non-secured media or being transported across a network is susceptible to attack.

Encryption of data stored on the device is vital to comprehensive, end-to-end encryption. Since handhelds and smartphones tend to be more accessible to intruders than servers or desktops, it is prudent to be even more vigilant when protecting mobile device data. Multiple data encryption solutions are available for the Palm OS platform. Man-aged security solutions from palmOne Solution Providers allows the IT Administrator to control what data must be encrypted and offers the option of protecting individual databases with an additional level of password protection. A variety of encryption algorithms are available including AES, TDES, and Blowfish. For example, Administrators can enforce the rule that all users in the sales group will encrypt their customer data, while all users in the engineering group must encrypt their Memo Pad database. Since sensitive data can reside not only on the device but also on expansion cards, many applications extend encryption to SD (Secure Digital) and MMC (MultiMedia Card) expansion cards.

palmOne Solution Providers also offer a wide selection of applications for handheld and smartphone data encryption. This functionality is typically combined with advanced password protection and other features. See Appendix for more information.

Antivirus Protection
Protection from malicious code begins with good anti-virus software. Best practices include frequent updates for the latest virus signatures and scanning of files immediately after receiving data. To date, there have been no success-ful virus attacks on the Palm OS platform. Since viruses are platform specific, palmOne™ handhelds and smart-phones are not susceptible to the thousands of viruses developed for the Windows platform and cannot pass vi-ruses back to the desktop during synchronization. But when it comes to security, it is best not to be complacent. Any connected system can be at risk for malicious code, and IT departments should be prepared. Best-in-class anti-virus software vendors such as Symantec, McAfee, Trend Micro and Computer Associates create anti-virus applications for palmOne™ handhelds and smartphones.

Digital code signing is a new feature of Palm OS Cobalt® . Code signing enables organizations to control which ap-plications are run on, or beamed to, Palm OS® devices. Administrators can choose to only allow programs that have been signed by a trusted party to be installed and run. Digital signing ensures the authenticity and integrity of the code, thus preventing malicious applications from compromising your data.

Protect Data Across the Network
Authentication
User authentication ensures that only authorized users can gain access to system resources. Corporate networks and servers should require users to authenticate with a username and a secret and/or unique identifier before

5

access is granted. For example, before Mary can access the system, she must present credentials to prove that she is indeed Mary. These credentials may simply be a username and password. For valuable assets, multi-factor authentication is advisable. The first factor is typically something a user knows (like a PIN, password or passphrase), and the second factor may be something a user has (such as a hardware or software token, certificate or smartcard). Biometric authentication (something the user is, such as a fingerprint or iris pattern) can be used alone or in combination with the other authentication mechanisms.

Server authentication allows Mary to confirm that she is indeed talking to Company A's server and not to a bogus server masquerading as Company A. Server authentication should be used in transactions where the user is providing sensitive information such as a credit card number. To prove its identity, a server could use protocols such as Secure Socket Layer (SSL) or Secure Electronic Transaction (SET) to send a digital certificate, signed by a Certificate Authority, to the user.

Palm OS® has built-in PPP support using popular authentication protocols including the Challenge-Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), and Password Authentication Protocol (PAP). palmOne™ handhelds and smartphones also have multiple methods of unique device identification, including Hardware Serial Number (HSN), and Flash ID. Any of these unique identifiers can be used to authenticate the device for network access, allowing palmOne handhelds and smartphones to be used as a physical token for two-factor authentication. Popular authentication tokens, such as RSA SecurID, can be used for two- or three-factor authentication. Up to eight RSA SecurID tokens can be stored on a palmOne device, eliminating the need to carry multiple key fobs. Trio Security offers a unique solution that turns your palmOne handheld or smartphone into a token, while incorporating biometric authentication and single-sign on functionality.

Ideally, security policies should be integrated with a central user directory and be consistent across all systems. Such best practices simplify administration, ensure a base level of security on all systems and prevent common mistakes such as removing a user from only one system rather than all systems.

Communications Encryption

End-to-end communications encryption ensures that even if data is intercepted, it will be useless to the interceptor. There are two general categories of encryption algorithms: symmetric key encryption and asymmetric (or public) key encryption. Symmetric encryption uses the same key for both encryption and decryption. Asymmetric encryption uses two keys, one public and one private. The public key is widely known, while only the key owner knows the private key.

Mobile devices present unique data encryption challenges. Different algorithms require different amounts of processing overhead. In a mobile device platform, it is important to employ an efficient encryption algorithm that protects data without degrading performance or battery life. For example, AES (Advanced Encryption Standard) and DES (Data Encryption Standard) are faster and use less battery life than 3DES (Triple DES or T-DES).

The intended application also influences encryption algorithm and method selection. Symmetric key cryptography requires less computational overhead, so data can be encoded and decoded more quickly than with an asymmetric key. This type of encryption works well for applications such as encrypting data on the device since the encryption key never leaves the device. Public key cryptography is typically used to establish communication between two parties. In many applications, these methods are complementary. For example, wireless messaging may use asymmetric keys to establish a session between a client and server, and then use symmetric keys to encrypt the data that is exchanged.

The Crypto Provider Manager (CPM) in Palm OS® 5 and up provides encryption and security services. This cryptographic interface can support multiple encryption modules and has built-in algorithms including RC4 symmetric encryption, SHA-1 for hashing and RSA Verify for signature verification. The CPM was co-developed with RSA Security.

Data alteration can be undetectable to an unsuspecting recipient, but the results can be just as devastating as a physical theft. As an additional protection against data tampering, message integrity checksums can be used to ensure that data has not been altered. Checksums confirm that the message could only have been created by an entity that knew the appropriate key. Sufficiently robust authentication, encryption and integrity checking mechanisms can effectively counter the risks of data interception.

In addition, there are many cryptographic toolkits, Public Key Infrastructure (PKI) toolkits and cryptographic libraries available from leading security companies and open source code. A sampling of such toolkits is listed in the Appendix.

Solutions for Securing Wireless Networks

Handhelds and smartphones can send and receive data using either wireline communications (via synchronization cradle) or wireless communications. Since cradle synchronization is inherently private, this discussion focuses on the privacy of wireless communications.

palmOne™ handhelds and smartphones support a variety of connectivity options, from WANs to WLANs (Wireless LAN) and PANs (Personal Area Networks). In addition, every palmOne handheld and smartphone has a built-in IR port that allows simple, fast data transfer.

VPN

A VPN (Virtual Private Network) is a popular solution for securing access to intranet and extranet resources and data. Properly implemented, VPNs can provide user authentication, encryption, access control, message authentication and integrity controls. VPN technology is in wide use today for laptops and workstations, enabling mobile users and satellite offices to access centralized data.

An IPSec (Internet Protocol Security) VPN client is the most popular business-class VPN solution today. IPSec VPN offers strong security with authentication, encryption and data integrity checks. Most IPSec VPN clients offer a selection of encryption and authentication options, allowing an organization to choose the level of security that balances requirements for privacy and performance. PPTP VPNs are often used in small to mid-sized businesses. PPTP VPNs are easy to configure and are supported by most Microsoft servers, as well as many Cisco gateways.

VPN technology is a great choice for mixed network and devices environments. VPNs will work over a variety of networks, including WANs, LANs and WLANs such as 802.11 networks. If you already have a VPN infrastructure, extending VPN to corporate mobile devices leverages this existing investment.

SSL

SSL (Secure Sockets Layer) is a popular protocol for secure wireless communications. SSL is found in virtually every web browser on the market today. Many palmOne handhelds and smartphones include a built-in web browser that features SSL 2.0, SSL 3.0, and 128-bit encryption. Palm OS 5 and up incorporate SSL v2.0 and SSL v3.0.

"SSL VPNs" are a recent product category that challenges traditional IPSec VPNs. SSL VPNs take advantage of the SSL built into virtually all web browsers to authenticate and encrypt transmitted data. The big advantage of many SSL VPNs is that no additional client software is needed other than a standard web browser. Once a backend SSL server is in place, information is transmitted securely using the browser software already included on all palmOne smartphones and most handhelds. Another advantage is that this technology can be used over virtually any networks. One current limitation is that only browser-based applications can be secured using SSL VPN without additional client software.

802.11 Network Security

802.11 is a widely deployed and immensely popular WLAN standard. 802.11 security has received negative publicity due to vulnerabilities in the Wired Equivalent Privacy (WEP) standard. Most significantly, weak initialization vectors (IVs) allowed recovery of the encryption key, rendering the encryption that was supposed to protect messages useless.

To correct WEP vulnerabilities, IEEE worked quickly to ratify WPA (Wi-Fi Protected Access), an interim standard. WPA is a subset of the 802.11i standard. 802.11i is supposed to be the gold standard for Wi-Fi communications security; however, it is still in-progress in the IEEE. WPA is a mid-step before the finalization of 802.11i and will be forward compatible with 802.11i

802.1x and LEAP

For 802.11 LANs, a security solution based on the IEEE 802.1x standard is an excellent option. With 802.1x, a wireless device must authenticate with the access point before accessing the WLAN (Wireless Local Area Network). 802.1x is an authentication standard for passing EAP (Extensible Authentication Protocol) over wired or wireless LANs. EAP is a general framework for authentication, allowing extensions to authentication methods without causing interoperability problems.
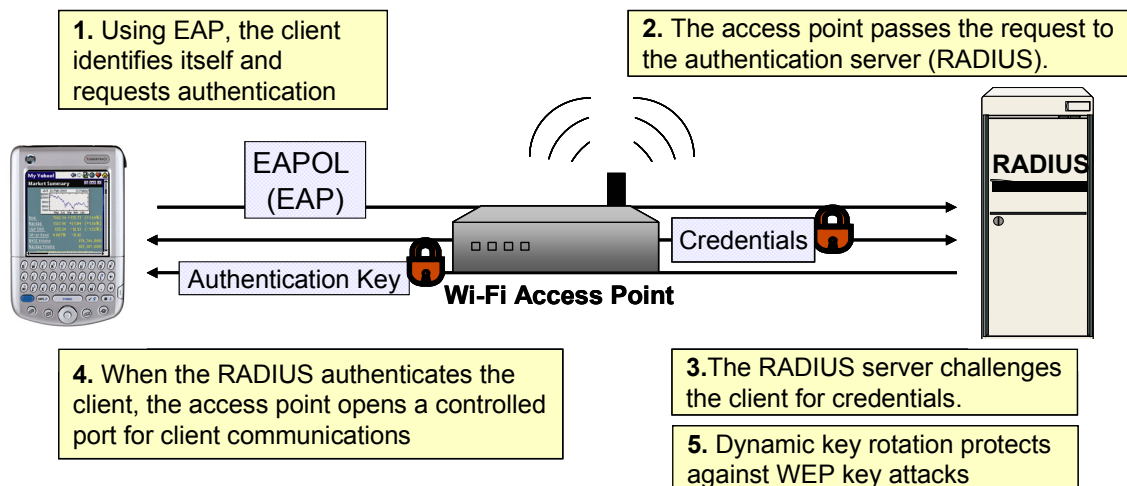
1. Using EAP, the client identifies itself and requests authentication

2. The access point passes the request to the authentication server (RADIUS).

EAPOL (EAP)

RADIUS

Credentials

Authentication Key

Wi-Fi Access Point

4. When the RADIUS authenticates the client, the access point opens a controlled port for client communications

3. The RADIUS server challenges the client for credentials.

5. Dynamic key rotation protects against WEP key attacks

Diagram A: 802.1x (EAP-LEAP) Security

Cisco's LEAP (Lightweight Extensible Authentication Protocol) is based on the 802.1x standard and provides mutual authentication based on password challenge-response. Mutual authentication means both the user and access point must authenticate to each other before network access is granted. LEAP also addresses the WEP key reuse weakness by exchanging dynamic WEP (Wired Equivalent Privacy) keys. The "Lightweight" in LEAP refers to the processing usage, not the level of security, making LEAP particularly well suited to mobile devices. LEAP is quickly becoming a de facto standard. It addresses the security vulnerabilities of WEP and, due to Cisco's dominance as a Wi-Fi equipment manufacturer, has a significant user base.

LEAP's one known vulnerability is the dictionary attack. Because LEAP relies on username and password for authentication, a hacker could run a dictionary attack until the password is guessed unless password attempts are limited. This vulnerability can be effectively counteracted by a limiting failed password attempts at the authentication server, typically a RADIUS server. With Cisco Aironet access points, each user is given a unique session key. Furthermore, LEAP encrypts the broadcast WEP key with the session key before transmission. Together, these measures nullify the network security risk of a lost or stolen device. AEGIS WLAN Security from Meetinghouse offers a LEAP client for 802.11-capable palmOne™ handhelds and smartphones. AEGIS combines LEAP's mutual authentication and dynamic key rotation with great performance and a transparent user experience.

802.11 and VPN
VPN is a weightier option for 802.11 security than 802.1x, both in terms of security measures and performance. Consider a VPN if your users need to transmit information over multiple networks, such as a WAN and a WLAN. One of the big advantages of VPN is that it will work over a variety of networks, including 802.11, GSM/GPRS, CDMA, Ethernet and Bluetooth. VPN is also a good choice if your IT organization is already running a VPN infrastructure and wishes to streamline the number of technologies it must maintain. If an IPSec VPN is used, the data will also be protected with enterprise-class encryption and data integrity checking.

Bluetooth Network Security
Bluetooth is an emerging wireless technology intended primarily for use in PANs. Bluetooth links devices within close proximity to one another (about 30 feet) using wireless communications to replace cables. PANs are spontaneous, or "ad-hoc," and require no infrastructure. palmOne™ believes that Bluetooth is the optimal technology for PANs because of its small chipset and low power consumption.

While the Bluetooth specification does a respectable job in stipulating security features, potential security risks in Bluetooth networks include man-in-the-middle attacks, as well as the possibility that other devices could try to access data by masquerading as connection-accepting or connection-seeking devices on the Bluetooth network.

The Bluetooth protocol includes features to protect Bluetooth communications against these types of attacks:
- User authorization required for data transmission. Bluetooth devices that accept user input, such as handhelds, require user permission before transmitting or receiving data.
- Frequency hopping algorithm. Bluetooth transmits signals using short bursts on a pseudo-random sequence of different frequencies. Thus, a receiver cannot simply be tuned to a given frequency to intercept Bluetooth traffic—it must use the same frequency hopping pattern as the transmitter.
- Encryption algorithm based on SAFER+. The E1 encryption algorithm used by Bluetooth is based on SAFER+, an algorithm that has been in the public domain since 1998 and was a thoroughly reviewed AES candidate.

8

- New encryption key for each session. Bluetooth transmissions use separate keys for authentication and encryption. The encryption key is regenerated for every session, further limiting damage that can be done through man-in-the-middle attacks.

All Bluetooth-capable palmOne™ handhelds use link level security with 128-bit encryption to protect privacy and prevent over the air attacks. Bluetooth connections are authenticated through passkey exchange. Users can designate devices as "trusted" by exchanging passkeys. When both device owners decide that they wish to trust each other, the devices exchange passkeys and Bluetooth IDs then store these identifiers. When these devices next attempt to communicate, passkey exchange occurs to ensure that each device has the other's passkey. If that is the case, data communication happens; otherwise it is aborted and the user is asked to enter the passkey explicitly.

In addition, all Bluetooth-capable palmOne handhelds also have a "Discoverable" setting. This is a popular Bluetooth security mechanism that controls the visibility of your handheld to other devices. Users can choose to hide their device so it will not be detected by other devices doing an inquiry.

Additional security solutions can be used with Bluetooth to achieve excellent security. Many VPN clients can run over Bluetooth. Or PKI can be used to add strong authentication, encryption, digital signing and non-repudiation. For more information about Bluetooth, please see the white paper at:
http://www.palmos.com/dev/tech/bluetooth/palm_bluetooth_mwp_r1.pdf.

Infrared (IR) Security
The IR port is a relatively secure means of communication. It requires close physical proximity (4 feet or less) to the beaming device. The recipient is prompted when a beam is sent and must tap on the screen to accept incoming data. This allows the user to control what he or she receives. palmOne handhelds also have built-in "sleep" thresholds (typically 1-3 minutes), and when sleeping the handheld cannot accept an incoming infrared beam. For organizations that need to deactivate the beaming feature, applications from CREDANT Technologies®, Trust Digital® and others include functionality to disable the IR port.

Backup and Recovery
When the worst happens, proper backup and recovery procedures are the key to quickly restoring users to productivity. Limiting and containing the impact of a security breach is critical. If an employee's handheld or smartphone is lost or stolen, their account should be quickly disabled on all systems, and their device segregated from the network.

To get the enterprise user back up and running, their data needs to be restored to another device. If backups are performed regularly, the data is safely within the corporate firewall and can be quickly recovered. Data backups can be performed via a PC-based HotSync® operation, network HotSync operation, server-based synchronization or Secure Digital Input/Output (SDIO) backup cards, which use the expansion slot available on most palmOne handhelds and smartphones.

Management solutions from palmOne Solution Partners help companies manage handhelds, smartphones, applications, and content from a central location. For example, Administrators can deploy applications for use in the field; manage, exchange, and deliver content; capture and store hardware and software information, automatically track mobile devices and their health; and provide automated system and data backup and restore capability—all from a central location.

Email and Groupware Solutions
One of the great benefits of palmOne handhelds and smartphones is the ability to access your email, calendar, contacts and other important data anywhere. Organizations can equip mobile users with the information they need increase productivity, and stay up-to-date with groupware solutions from palmOne Solution Providers such as Good Technology™, Seven™, and Visto.

Good Technology
With Good Technology GoodLink, users can exchange messages, access data, and manage phone calls from their Treo 600 smartphone. GoodLink delivers a laptop-like experience, with full Microsoft Outlook capabilities, rich attachment support, and interaction with third party applications. GoodLink goes beyond Outlook to provide sync and browser access to BTFW database applications. Cradle-free synchronization allows continuous two-way wireless sync.

In March, 2004, GoodLink was awarded FIPS140-2 certification on the palmOne Treo™ by NIST. GoodLink's layered security protects communications between the server and the mobile device:

| Client Security	**Authentication:** Security policies such as password expiration, length, and format can be enforced. This functionality is integrated with the Palm OS security application. **Remote data deletion**: If a device is lost or stolen, the Administrator can remotely delete sensitive data. **Backup:** An SD "recovery card" stores a duplicate image of the device configuration and data for quick data recovery.
Transport Security	**Encryption**: AES and TripleDES encrypt messages behind the firewall and only decrypt them when they have reached the device. **Message confirmation**: Positive confirmation architecture ensures messages have been delivered and provides persistent message storage and re-delivery.
Server Security	**BTFW server**: GoodLink Server is installed behind the corporate firewall and uses standard port 443. **Role-based administration:** IT can restrict security-related administration to a subset of administrators.
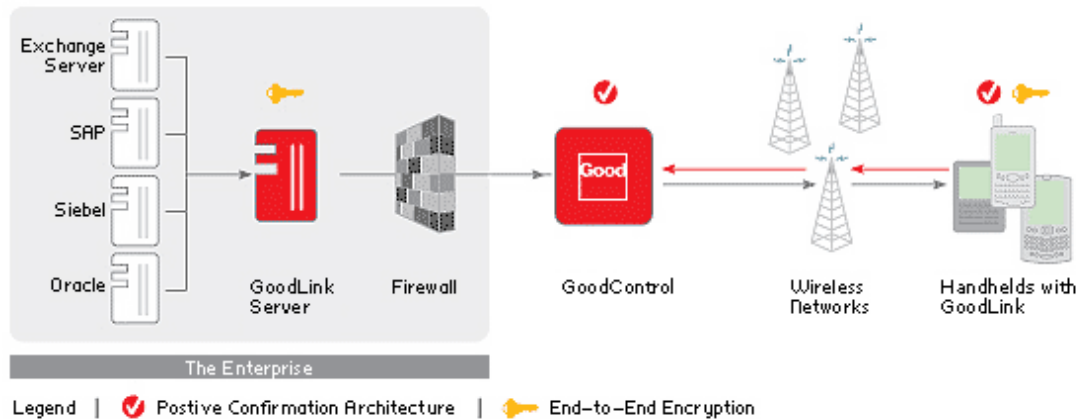
Diagram B: Security from GoodLinkServer to Treo smartphone

System SEVEN

System SEVEN is a mobile software architecture deployed within operator networks worldwide. System SEVEN provides subscribers with secure, real-time mobile access to Microsoft Exchange, Lotus Domino, IMAP4 and POP3 email, calendar, personal contacts, corporate directories and documents. System SEVEN works across a wide variety of mobile devices, including the palmOne Treo™ 600, 300 and 270.

System SEVEN has two business-class connectivity options: SEVEN Server Edition and SEVEN Enterprise Edition. Server Edition uses a behind-the-firewall server to connect corporate applications and operator network. Enterprise Edition is a zero-configuration, 100% operator-hosted service. Server Edition establishes and maintains a pool of outbound network connections from the corporate server to System SEVEN infrastructure at the network operator's data center.

| Client Security	**Authentication**: Password requirements for expiration, length and complexity are enforced. **Remote data deletion**: The Administrator can initiate a data removal request to remove all device data. **Password Protection:** User passwords are hashed before being stored, ensuring that the true password cannot be recovered.
Transport Security	**Encryption:** 128-bit SSL encryption is used to protect data when System SEVEN accesses, or is accessed by, industry-standard applications. End-to-end 128-bit AES encryption is used to safeguard all communications between System SEVEN components. AES is scalable to 192- and 256-bit key lengths. **Data Integrity:** Digital signature algorithms (e.g. SHA-1) secure data transported between System SEVEN components. The use of digital signatures protects data from modification during transport.
Server Security	**Credentials are secured** on the SEVEN Server and are never stored outside of the corporate premises. Upon registration, a unique, encrypted authentication token is exchanged with the mobile device or browser gateway enabling the user to access corporate resources via System SEVEN without requiring users to submit credentials upon each login. **Security policy control:** System SEVEN enables enterprise administrators to extend many of the security policies from their wired environment out to their mobile devices. E.g. with Server Edition, users' Microsoft desktop authentication policies are seamlessly extended to the mobile device.
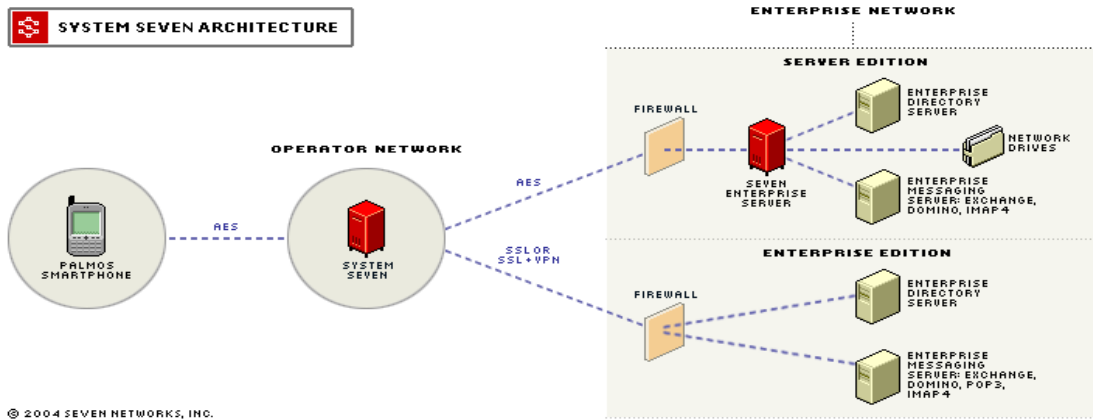
Diagram C: System Seven Architecture

Visto Mobile Access Solution

The Visto Mobile Access Platform (VMAP), Server Edition synchronizes with Microsoft Exchange Server, enabling mobile access from palmOne™ handhelds and smartphones. VMAP provides push email and scheduled synchronization for email, calendar and contacts, as well as attachment support. This hosted solution can be rapidly deployed, eliminating infrastructure, configuration, and deployment costs.

| Client Security	**Client authentication:** Users are authenticated with user name, password and device specific identification. **Server authentication:** Verisign digital certificates ensure that users are accessing the legitimate VMAP server. **Remote data deletion:** "Data kill" feature enables the Administrator to remotely delete device data.
Transport Security	**SSL transport security:** 128-bit SSL protects data transmissions. **AES data encryption:** Data is encrypted end-to-end with 128-bit AES encryption.
VMAP Security	**Data remains encrypted:** Data is stored and forwarded data in encrypted form. **Secure infrastructure:** A redundant infrastructure protected by intrusion detection systems (IDS); firewalls; and router Access Control Lists (ACLs) is hosted in a secure network operations center (NOC).
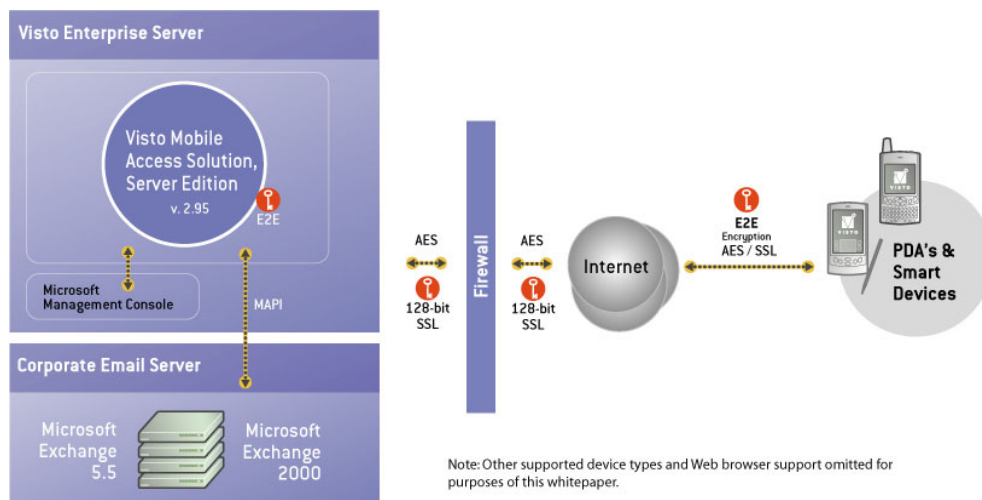
Diagram D: Visto Enterprise Server Security

The Future of Handheld and Smartphone Security

Security has become a top priority for business, government, and healthcare providers and many exciting developments are expected in the not-too-distant future. New developments in security such as Palm OS advances, biometric security, and smartcard technology will make strong mobile device security easier to use and administrate.

PalmSource® Operating System

Palm OS® Cobalt, will provide strong security without sacrificing the Palm OS® tradition of flexibility, openness, and ease of use.

11

Features include:
- **Secure Kernel** The basis of Palm OS® Cobalt security is the secure kernel, which relies on a capabilities model. Only components granted keys are permitted to communicate with other system components. This protects the system from rogue code. To ensure components and applications are accessing legitimate resources, all system shared libraries of Palm OS Cobalt are digitally signed by PalmSource®.
- **Security Services** The Security Services support a variety of mechanisms for specifying and controlling security policies. Applications and code modules can read OS policies for various operations and functionality. For example, a policy can be set to only allow the OS to load signed patches. In addition, users can indicate a desired level of security (None, Medium or High), allowing the system to react accordingly.
- **Cryptographic Services** The Cryptographic Provider Manager (CPM) is a system-wide suite of cryptographic services for securing data and resources. Using the CPM API (Application Programming Interface), any application can use its cryptographic services such as key generation, hashing, encryption, decryption, signing, and verification. The API allows the encryption of only selected data or of all data and resources.
  As in Palm OS® 5 and Palm OS® Garnet, CPM offers 128-bit RC4, SHA-1 and RSA- Verify. New in Palm OS Cobalt is a plug-in cryptographic architecture that allows developers to add cryptographic modules. A new FIPS provider (certification pending) supports 128-, 192- and 256-bit AES, 3DES, SHA-1, and SHA-2.
- **Secure Communication** PalmSource has partnered with RSA Security to add TLS (Transport Layer Services) to the SSL services in previously introduced in Palm OS 5. SSL v2, SSL v3 and TLS 1.0 services secure end-to-end communications over the Internet with strong encryption, for data privacy and secure e-commerce transactions.
- **Authorization Manager and Authentication Manager** A system-wide authentication and authorization system allows businesses and developers to control access to protected databases. With Authorization Manager, applications can specify rules for data access. The goal is to enable the secure storage of information and limit access to this information to authorized parties. The Authentication Manager manages any token used for verifying access, including such standard tokens as passwords, PINs, or pass-phrases. The Authentication Manager's extensible architecture permits licensees and developers to incorporate such methods as biometric verification and smartcards.
- **Digital Code Signing** Signed code enables organizations and developers to authenticate the integrity and source of applications and databases. Using the Authentication Manager, applications can restrict access to data, resources and trusted system components like patches, shared libraries, system overlays, and drivers. Any managed resource can be protected, including stored data, application code, and kernel resources. For instance, a signed application can create a protected object so only that specific application can access the object. Among other benefits, signed code helps organizations, carriers and developers manage the installation and maintenance of approved programs, while protecting data from malicious programs.
- **Digital Certificate Management & Signature Verification** A Certificate Manager, developed in cooperation with RSA Security, handles X.509 certificates. A signature verification library allows applications and system modules to easily verify signatures on code modules and resources
- **Data Synchronization and Backup** The synchronization and redundancy of data are an inherent qualities of the Palm OS platform. Businesses and developers can customize the synchronization of their mobile fleets using a Palm OS conduit API. To ensure data confidentiality during synchronization, the communication between the device and the desktop can be encrypted in trusted sync mode.

The latest Palm OS Developer Suite is designed to help developers produce enterprise-grade applications. The Palm OS Developer Suite is based on the industry-standard Eclipse environment, an open-source, Integrated Development Environment (IDE) originally developed by IBM that supports software development in a variety of languages, including C, C++, Java and COBOL. In addition, a wide variety of development tools are available for Palm OS® , including Metrowerks CodeWarrior, the Eclipse environment, Borland's tool suite and Microsoft .NET compatible tools from AppForge.

Biometric systems analyze unique physiological traits such as fingerprints, hands, voices and facial patterns. What makes biometric systems so effective is that physical characteristics such as these are unique and very difficult to counterfeit. Voiceprint matching, fingerprint recognition, facial and hand geometry patterning, iris scanning and thermal detection are all possibilities for mobile device security. The beauty of biometric authentication is that it merges strength with convenience. Users can gain access simply by uttering a passphrase, touching a screen or scrawling their signature.

Smartcards contain integrated circuits that provide tamper-proof storage of user and account identity and protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. Smartcards can work with palmOne handhelds and smartphones via the expansion slot, SIM card or a USB attachment. Potential applications include digital signing, strong authentication, and secure payment solutions.

The Common Access Card (CAC), a smartcard issued to US DOD (Department of Defense) employees, is an example of physical security, PKI ,and soon, biometrics in action. The first generation of the CAC was used for system and building access and incorporated a digital certificate for signing email and documents. The plan for the second generation of cards is to incorporate biometrics, such as fingerprint and iris recognition, to further increase security and convenience. This solution could be extended to palmOne™ devices by using an SD-or MMC-based smartcard as the CAC.

Building on the security services introduced with Palm OS® 5, Palm OS® Garnet and Palm OS® Cobalt launch a new era in Palm OS security. By combining Palm OS® and palmOne™ innovations with new developments in the security industry, such as biometrics and smartcard advances, organizations can secure their data without compromising usability.

Conclusion

Today, handhelds and smartphones have evolved into indispensable business tools that enable an increasingly mobile workforce to remain connected and productive. As mobile devices proliferate and become an integral part of the corporate technology infrastructure, security becomes a serious concern for every IT manager as well as for users. Protecting corporate information is essential to business survival and growth, and end-users must be trained to safeguard these resources.

A clear understanding of the challenges posed by handhelds and smartphones in a particular environment provides the basis for developing sound security policies, standards and practices. A security strategy must strike a balance between what is possible and what is feasible, basing decisions on industry best practices and clearly articulating guidelines and procedures. Encryption programs, anti-virus software, effective password use, training and awareness are all components of an effective business security program. palmOne™ and our Solution Providers are committed to developing products and solutions that enable organizations to adopt security best practices and minimize the risks involved in mobilizing their workforce.

Appendix: Solutions from palmOne Solution Providers

Authentication and Encryption Solutions

Product	Features
Asynchrony Solutions PDADefense Enterprise	PDADefense Enterprise provides enhanced password protection, 128-bit or 512-bit Blowfish encryption and hardware button password entry. IT managers can enforce password, encryption and beaming policies and set restrictions on application usage. www.asynchrony.com
Certicom™ movianCrypt™	movianCrypt uses 128-bit AES to encrypt data , provides advanced password security and auto-lock functionality. www.certicom.com
Communication Intelligence Corporation® Sign-On	Sign-On uses biometric signature verification to safeguard data on a device. Users simply sign their name or create a personalized drawing or design and Sign-On verifies it to unlock the device. www.cic.com
CREDANT Technologies® Mobile Guardian	Mobile Guardian addresses mobile security issues with centrally managed, policy administration and strong on-device user authentication and policy enforcement. www.credant.com
IS/Complete Restrictor	Restrictor allows an administrator to create profile categories for different users on a single device and enables users to automatically lock their devices and hide records. www.iscomplete.com
Kasten Chase Assurency™ SecureData	Assurency SecureData provides record-level encryption for all data stored on the device and decrypts only as required, ensuring a fast user experience. An enterprise version empowers the IT Administrator. www.kastenchase.com
TealPoint Software™ TealLock™	Corporate TealLock is a secure automatic locking program. Features include serial and infrared lockout, data encryption, administrator password, remote-unlocking, and password controls. www.tealpoint.com
Trust Digital® PDASecure™	PDASecure encrypts data on the device using AES. It features universal integration with all applications installed on the device and allows administrators to define security policies. www.trustdigital.com

Authentication

Product	Features
RSA Security® SecurID®	SecurID software, used in conjunction with RSA ACE/Server software, generates a random, one-time-use access code that automatically changes every 60 seconds. www.rsasecurity.com
Trio Security Trio VAULT™	Trio VAULT combines 3-factor user authentication, a single-sign-on solution, and access management into a single, integrated Palm OS application that interfaces seamlessly with the existing network security infrastructure and eliminates the need for authentication and single-sign-on servers. www.treosecurity.com

Virtual Private Network (VPN) Solutions

Product	Features
Certicom movianVPN™	movianVPN is an IPSec VPN client that provides strong authentication, encryption and data integrity checking to secure remote access to email and data. movianVPN supports a wide variety of popular gateways, including Cisco, Lucent and Nortel. www.certicom.com
Mergic™ Mergic VPN	Mergic VPN is a PPTP (Point-to-Point Tunneling Protocol) VPN client for securing remote access. www.mergic.com

Cryptographic and PKI Toolkits

Product	Features
Certicom Security Builder® Crypto™	Security Builder Crypto is optimized for small code size and includes a range of current and legacy algorithms that provide proven security. www.certicom.com
Certicom Security Builder® GSE™	Security Builder GSE enables you to incorporate a complete FIPS 140-2 Validated cryptographic module or individual FIPS-approved algorithms into your products. www.certicom.com
Copera AESLib	AESLib is a shared library for Palm OS that implements the AES encryption algorithm. Version 3.1 includes ARM support. www.copera.com
Diversinet™ Passport	Passport client/server security software facilitates digital signatures, authentication and encryption with PKI products specifically optimized for wireless environments and devices. www.diversinet.com
RSA Security® BSAFE®	The RSA BSAFE line of SDKs provides all of the components required to make any application safe and secure, including web services security, protocol implementations, certificate management and cryptography. www.rsasecurity.com
Ntru Cryptosystems Security Toolkit	Ntru offers a full range of public and symmetric key functionality, including encryption, decryption, signing and verification. www.ntru.com

Anti-virus Applications

Product	Features
Computer Assocates® eTrust™ Antivirus	eTrust Antivirus for Palm OS detects viruses and Trojans that infect devices running Palm OS v3.0 or greater. www.ca.com
McAfee® VirusScan™	Resides on the device and can be used anytime for scanning. If a virus is discovered, the user is alerted, and synchronization is blocked until the destructive code has been deleted.www.mcafee.com
Symantec™ AntiVirus	Scans files looking for signatures of viruses, Trojan horses and worms, and prompts the user if malicious code is detected. In addition, AntiVirus for Palm OS automatically updates virus definitions during synchronization with the PC. www.symantec.com
Trend Micro™ PC-cillin™ for Wireless	Provides automatic real-time launch scanning to prevent viruses that could enter the handheld via beaming, synching, email and downloads. www.trendmicro.com

Email and Groupware Solutions

Product	Features
Good Technoogy™ GoodLink	With GoodLink, users can exchange messages, access data, and manage phone calls from their Treo smartphone. www.good.com
Notify NotifyLink Enterprise Edition	NotifyLink Enterprise Edition Is designed for small to large-scale corporations requiring secure wireless push notification of email, calendar, contacts, and tasks, for their mobile professionals. NotifyLink supports multiple devices, multiple networks, global settings, and encryption of messages. www.notifycorp.com
Intellisync™ Handheld Edition for Enterprise	Intellisync Handheld Edition for Enterprise supports the desktop synchronization needs of handheld users with integrated sync of email, calendar, contacts and tasks. A companion product, Intellisync for Enterprise Managed, provides IT with tools for management and support such as remote installation/upgrades, device configuration, backup/restore, and asset inventory collection. www.intellisync.com
Intellisync Mobile Suite	This modular mobile-middleware software solution connects a wide variety of mobile devices, using virtually any type of connection, to synchronize application and PIM data, Email, and corporate files. Mobile Suite is comprised of four software modules: Email Accelerator, Data Sync, File Sync, and Systems Management. www.intellisync.com

14

Email and Groupware Solutions, cont.

Product	Features
SEVEN ® System SEVEN	System SEVEN is a mobile software architecture deployed at the operator network that provides access to email, calendar, contacts, documents and corporate directories. www.seven.com
Visto® Mobile Access Solution	Visto Mobile Access Solution TM, Server Edition provides secure mobile, wireless access to Microsoft Exchange and Outlook data. www.visto.com
Extended Systems® OneBridge® Mobile Groupware	One Bridge (formerly XTNDConnect Server) enterprise synchronization software enables mobile workers to access and synchronize e-mail, PIM and custom database information. www.extendedsystems.com

Glossary

3DES or TDES: Triple DES, a stronger version of DES encryption in which the input data is, in effect, encrypted three times.

802.11: A family of specifications developed by the IEEE for wireless LAN technology. The most commonly deployed 802.11 specification is 802.11b, also called Wi-Fi.

802.1X: An IEEE standard based on the Extensible Authentication Protocol that provides an authentication framework for 802.11 LANs.

AES: Advanced Encryption Standard, FIPS 197. Originally named Rijndael, AES is a block cipher algorithm that was selected by NIST as the "Advanced Encryption Standard."

Algorithm: A specific mathematical formula to perform a function (like encryption and decryption). Some algorithms are more secure than others, while some are faster than others.

Asymmetric Encryption: Any encryption scheme where the sender and receiver use a pair of different but related keys that cannot be derived from one another. Data is encrypted with one of the keys and decrypted with the other key.

Biometric Authentication: Any method for verifying identity that relies on a unique personal attribute, such as fingerprint, voice or the blood vessel pattern around a retina.

Bluetooth SIG: Bluetooth Special Interest Group. The trade association of wireless company representatives and other experts who define and maintain the Bluetooth specification for short-range wireless transmission.

Blowfish: A symmetric block cipher developed by Bruce Schneider in 1993. Blowfish has undergone considerable review and is gaining acceptance as a strong encryption algorithm.

Certificate: A public key digitally signed by some signing authority to guarantee its validity.

Certificate Authority: A trusted third-party clearinghouse that issues digital certificates and digital signatures.

CHAP: Challenge Handshake Authentication Protocol. A type of authentication in which the authentication agent (typically the network server) sends the client program a key to be used to encrypt the username and password.

Checksum: A technique whereby the individual binary values of a string of data are totaled at two points in time to determine if any data has been changed. Commonly used to check the integrity of data that has been transmitted or stored.

Cipher: The generic term used to describe a means of encrypting data. "Cipher" may also refer to the encryption algorithm itself.

Encryption: Any method of scrambling data so that it cannot be read during storage or transmission. The data is then kept confidential until it is decrypted (unscrambled).

Flash ID: Unique serial number for the ROM in a Palm device.

FIPS (Federal Information Processing Standards): Standards and guidelines for federal computer systems issued by NIST.

HIPAA (Health Insurance Portability and Accountability Act): U.S. legislation that, among other things, sets standards for the security of protected health information.

HMAC: Hashed Message Authentication Code. A message digest function and secret key used to create authentication codes using MD5 or Secure Hash Algorithm (SHA).

HSN: Hardware Serial Number. A unique number or alphanumeric combination assigned to a device.

IEEE: Institute of Electrical and Electronics Engineers. A large, international, non-profit, technical professional association that establishes consensus-based open standards.

IETF: Internet Engineering Task Force. A large open international community of professionals concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

IPSec: Internet Protocol Security. A tunneling protocol developed by IETF and often used to implement VPN security.

IR port: Infrared Port. A port built into many models of handhelds and smartphones for transfer of data between devices.

Glossary, cont.

ISO: International Organization for Standardization, a worldwide federation of national standards bodies from more than 140 countries.

Key: In cryptographic usage, an alphanumeric string used for encryption and/or decryption.

LDAP: Lightweight Directory Access Protocol. An open standard for directory lookups that uses a hierarchical structure.

LAN: Local Area Network. A network that encompasses a small physical area (e.g. one office).

MD5: A one-way hash algorithm used to create a message digest for digital signatures.

MMC: MultiMedia Card. A removable storage media that can be used in many electronic devices, including palmOne™ handhelds and smartphones.

NIST: National Institute of Standards and Technology, a nonregulatory agency within the U.S. Commerce Department that develops and promotes measurements, standards, and technology.

PAN: Personal Area Network. A wireless network that enables handhelds, smartphones, cell phones, and other mobile devices to communicate over short distances.

PKI: Public Key Infrastructure. A system of digital certificates, Certificate Authorities, and other registration authorities used to verify and authenticate each party in a transaction.

PPTP: Point-to-Point Tunneling Protocol. A protocol developed by Microsoft, commonly used for VPN security.

Public Key Encryption: An asymmetric encryption scheme such as RSA, Diffie-Hellman-Elgamal, and Elliptic Curve algorithms.

RADIUS: Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet service providers. The specification is maintained by IETF.

SAFER+: An encryption algorithm submitted by Cylink Corporation as an AES candidate. SAFER+ provides slightly less than the suggested 2128-order protection, given 128-bit keys, which is why it was not chosen for AES. Experts agree, however, that this academic imperfection does not compromise SAFER+ in practice.

SET: Secure Electronic Transaction. An open industry standard protocol developed for the secure transmission of payment information over the Internet and other electronic networks.

SD: Secure Digital card. A removable storage media that can be used in many electronic devices, including palmOne handhelds and smartphones. SD uses the same form factor as MMC.

SDIO: Secure Digital Input/Output.

SHA-1: Secure Hash Algorithm. A popular algorithm for computing cryptographic checksums. Checksums are commonly used to check if data has been modified.

SSL: Secure Socket Layer. A very popular protocol for managing the security of message transmission over the Internet. SSL is found in virtually all commercial web browsers today.

Symmetric Encryption: Any encryption scheme where the encrypting and decrypting parties share the same key.

TKIP: Temporary Key Integrity Protocol. An interim fix to WEP encryption problems. TKIP can be applied to existing hardware through driver and firmware upgrades.

USB: Universal Serial Bus, a plug-and-play interface between a computer and add-on devices.

VPN: Virtual Private Network. A network which emulates a private network, although running over a public network. The use of encryption and a tunneling protocol maintains privacy.

WAN: Wide Area Network. A computer network that encompasses a wide physical area. Multiple LANs are often connected to form a WAN.

WEP: Wired Equivalent Privacy. A security protocol for wireless local area networks defined in the 802.11b specification.