Palm OS 5 Security Features

A Flexible, Robust Security Platform

Mobile devices, lead by those based on the Palm OS® platform, are playing an increasingly important role in corporate environments. In this role, one of the key strengths of the Palm OS is its flexibility. This flexibility has resulted in innovation from both licensees and developers and has enabled the enterprise to deploy a diverse array of Palm Powered™ devices in increasing numbers. As the number and uses of these devices grow, security professionals require a mobile platform that supports a range of security options that can deliver the flexibility and scalability necessary to satisfy the needs of an organization.

As the most widely deployed mobile platform for the enterprise, the Palm OS continues to deliver on the promise of providing a stable, scalable platform with the widest range of security options available for mobile computing. The introduction of Palm OS 5 raises the bar even higher, incorporating a suite of robust security options without sacrificing the Palm OS tradition of flexibility, openness, and ease of use.

Cryptography Manager

The Cryptographic Provider Manager (CPM) in Palm OS 5 is a system-wide suite of cryptographic services for securing data and resources on a Palm Powered device. The CPM extends encryption services to any application written to take advantage of these capabilities, allowing the encryption of only selected data or of all data and resources on the device.

As part of the CPM suite, system-wide strong encryption (128-bit) is a standard feature of the new operating system. Through a partnership with RSA Security, the leading encryption provider in the security industry, Palm OS 5 includes RC4, SHA-1, and signature verification using RSA-verify. This partnership with RSA Security ensures that best-of-class security services are available within Palm OS. The CPM will also incorporate a plug-in cryptographic architecture, allowing businesses and developers to incorporate other encryption algorithms, such as Advanced Encryption Standard (AES), through a suite of APIs.

Palm OS 5 is built upon a 32-bit architecture and fully supports ARM®-compliant processors, enabling businesses and developers to activate these encryption features while maintaining the high level of performance expected from the Palm OS. With these capabilities, Palm OS 5 not only provides one of the world's most trusted encryption schemes as a standard feature, but it also delivers the flexibility required to meet the specific needs of various markets.

Secure Communication

Palm OS 5 incorporates Secure Socket Layer (SSL) services at a system level, extending encryption capabilities to communication, networking, and e-commerce applications. The SSL 3.0/TLS 1.0 services built into Palm OS 5 enable secure end-to-end connections over the Internet with strong (128-bit) SSL encryption, thereby facilitating the ability of applications to protect private data and secure e-commerce transactions.

By incorporating the RC4 encryption algorithm as a system-wide capability, Palm OS 5 provides as a standard feature the world's most commonly used and trusted encryption protocol for data transmission. As new transmission algorithms are developed, devices and applications for the Palm OS will be able to utilize these new

encryption schemes through a plug-in encryption architecture. With this set of capabilities, Palm OS 5 offers a complete solution for securing mobile communications.

Palm OS 5 also supports unique device identification. For Palm Powered devices, network administrators can use several methods to identify a unique device, including Flash ID, Mobile Access Number (MAN), and Electronic Serial Number (ESN). Any of these unique device IDs can be used to authenticate the device for network access. Moreover, these unique identifiers allow Palm Powered devices to be used as a physical token for two-factor authentication. Palm OS also supports Microsoft's Challenge Handshake Authentication Protocol (CHAP), and there are several VPN clients that support the Palm OS, including those from Certicom and SafeNet.

Authorization Manager and Authentication Manager

Requiring password entry to unlock the device is a standard feature of the Palm OS, and Palm OS 5 extends this capability by adopting a much broader approach to access control. Palm OS 5 will encompass a system-wide authentication and authorization system that will allow businesses and developers to use any of a number of methods to restrict access.

The Authorization Manager will enable applications to specify a set of rules that must be met in order to access data on the device. With this capability, any managed resource can be protected, including stored data, application code, and kernel resources. The Authentication Manager will manage any token used for verifying access, including such standard tokens as passwords, PINs, or pass-phrases. Featuring an extensible architecture, the Authentication Manager will also allow developers to incorporate such authentication methods as biometric verification (handwriting, voice recognition, fingerprints, etc.) and smart cards.

Additionally, the Authentication Manager will include support for signed code, so that only applications that have a valid digital signature may access certain data and resources. Among other benefits, this feature will assist businesses and developers in managing the installation and upkeep of approved software programs, while also ensuring that malicious programs cannot tamper with data stored on the device.

Data Synchronization and Backup

The synchronization and redundancy of data are an inherent quality of the Palm OS platform. Indeed, data synchronization and back up to a desktop computer have been a staple of the Palm OS since its inception. Seeking to deliver a synchronization platform that is both powerful and versatile, the Palm OS features a mature suite of conduit APIs, allowing businesses and developers to customize the manner in which the mobile device communicates with the synchronization target.

Additionally, there are a number of server synchronization and back up solutions available from software developers for the Palm OS. Each of these extends the synchronization architecture of the Palm OS platform to include back-end servers that can centrally manage and distribute the appropriate information to the appropriate individuals in an organization.

The Palm OS Advantage

The security of mobile computing devices is a vital concern to any organization, particularly as wireless connectivity becomes more commonplace across the enterprise. With the world's largest installed base of handheld devices – over 20 million units – and the widest range of mobile enterprise software, the Palm OS platform provides the strength, depth, and flexibility of security solutions needed by businesses to address these concerns, without compromising ease of use.

Features and specifications subject to change without notice. © 2002. Palm, Inc. Palm OS is a registered trademark, and Palm Powered, Palm, the Palm trade dress and the Palm logo are trademarks of Palm, Inc. or its subsidiaries. All other products and brand names may be trademarks or registered trademarks of their respective owners.