DATASHEET

Security and Palm OS

A Flexible, Robust Security Platform

palmsource™

Palm OS® enables a wide array of data security options through User Authentication, Anti-Virus solutions, secure SSL communications and VPN technology. These ensure both the integrity and the confidentiality of data on your handheld.

Remote Corporate Access

Many enterprise applications require the user to authenticate to remote systems. Palm OS virtual private network solutions and SSL encryption enable secure remote network access for corporations. Palm OS has built-in PPP support using popular authentication protocols including CHAP, MS-CHAP, and PAP. These secure solutions enable remote intranet and email accessibility.

The Palm OS provides handheld security options with:

- Secure user authentication including biometric solutions
- Anti virus solutions from leading providers
- Data integrity and confidentiality encryption options
- Secure SSL, PPTP, and IPSec communication options

Finding the right security balance is a challenge that companies face when protecting data in today's interconnected world. IT professionals need to ensure a proper level of security with the least impact on productivity.

To achieve this, Palm OS is laying the foundation for the new generation of security applications. With the new generation of devices, Palm OS can execute complex cryptographic operations and support higher security standards without affecting a device's performance or ease of use.

User Authentication

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

The Palm OS provides password protection and can automatically lock the device on power off, at a specific time, or after a certain period of inactivity. In addition, third-party Palm OS developers provide enterprise class security offerings that take advantage of built-in Palm OS Application Programming Interfaces (APIs) including Tranzoa's OnlyMe, which provides password protection using combinations of buttons and icons and CIC's Sign-on for Palm OS that uses personal signature verification to keep data safe. More advanced user verification methods are available that combine an Electronic Serial Number (ESN) and a user password for remote access, including PDA Defense from Asynchrony Solutions Inc. RSA SecurID from RSA Security is a two-factor authentication solution based on something the user knows (a password or PIN), and something the user has (an authenticator like the device and ESN) and provides dynamic user authentication instead of reusable or static passwords, support and more.

Anti-Virus

Malicious code can take the form of viruses, worms or Trojan horses. Viruses can be considered a particular type of unauthorized access and may cause damage, alter, or delete data. So far, the Palm OS platform has been remarkably safe from virus attack. Several anti virus solutions exist to provide additional assurance and make the Palm OS platform one of the safest mobile computer environments. Major vendors have ported their solutions to

the Palm OS platform including Computer Associates with InnocuateIT, Network Associates, and Symantec Anti-Virus programs.

Data Integrity and Confidentiality

In addition to preventing unauthorized access to the Palm OS device, the integrity and confidentiality of sensitive data needs to be guaranteed. In other words, ensure that the data has not been tempered with or altered.

End-to-end 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. Palm OS supports both types through built-in cryptographic API or third party solutions. Palm OS provides a cryptographic manager with strong encryption (128 bit) with the RC4 algorithm implemented by RSA Security, SHA-1 hashing and RSA verify. This API is exposed to developers to leverage the ability to add reliable secure functions in a variety of solutions encrypting data and applications on the device, and can provide a different level of security including FIPS 140 compliance.

This architecture is evolving towards a plug-in cryptographic framework that will allow businesses and developers to incorporate other encryption algorithms and schemes as they are developed and proven. Current solutions include MovianCrypt from Certicom and PDA Secure from TrustDigital.

Securing Communications

As wireless mobile devices become more prevalent, mobile platforms must support end-to-end communication encryption schemes like Secure Socket Layer (SSL). PalmSource has partnered with RSA Security to provide support for 128-bit SSL encryption on Palm OS. This allows mobile users to securely access remote data using standard applications like a web browser on an intranet or receive and send mail remotely.

A virtual private network (VPN) is the preferred method of providing secure access to intranet resources. The two major VPN transport protocols are Point-to-Point Tunneling Protocol (PPTP) and IPSec. PPTP is pervasive in small and medium sized businesses because major enterprise servers running Microsoft Windows operating systems. IPSec is the de-facto VPN standard and is widely used by Fortune 1000 companies that deploy a more complex VPN and network infrastructure. Palm OS supports both of these protocols with third-party products from Mergic, SafeNet, and Certicom.

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.

3rd party Enterprise applications:

http://applications.palmsource.com

Check our website for more information:

http://www.palmsource.com/enterprise/security.html

PalmSource, Inc.
1240 Crossman Avenue
Sunnyvale, CA 94089
U.S. (408) 400-3000
www.palmsource.com