PGP Mobile for Palm OS 2.0

Overview:

PGP Mobile for Palm OS provides equivalent capabilities to PGP Disk and PGP Mail on Palm OS devices. With their synchronization abilities, PDAs contain the most sensitive personal and business-related information on a user's personal computer: passwords, account information, contacts, etc. PGP Mobile protects that information, and also syncs PGP-specific information like your keyring between your computer and your PDA. (The PGP Palm conduit is only available on Windows.)

Since they're so small, these devices are easily lost or stolen. PGP Mobile keeps the important data on your PDA encrypted, and secure from unauthorized access. In addition to secure storage, PGP Mobile also provides secure communications facilities for wireless PDAs, allowing PGP Mail-compatible messages to be sent and received securely.

PGP products keep your confidential information secure. Whether it's in transit over a network or stored on desktops, laptops, or mobile devices, PGP prevents unauthorized access to your data. PGP products have developed a reputation for excellence based on high technical standards and long-term proven encryption solutions.

PGP Mobile for Palm OS 2.0 introduces a new feature which keeps the databases containing your confidential information encrypted whenever you're not using them. Just tell PGP Mobile which applications (Date Book, Address, Memo Pad, for example) you would like to secure, and all data used by those applications will automatically be encrypted, and subsequently decrypted only while you use it. If you lose your Palm, your data remains safe.

Key Features:

PGP Mobile for Palm OS, the most comprehensive product available for keeping the information on your Palm OS device secure, offers the following features:

* Database Encryption
* Automatic Record Encryption
* PGP Vault - Secure Memo Pad
* Synchronize PGP Vault with Desktop
* Signed and Encrypted E-mail
* Integration with most popular Palm E-mail apps
* Digitally Signed Memos
* Decrypting and Verifying Clipboard
* Full RFC 2440 OpenPGP Compatibility
* Local Key Storage
* Synchronize Keyring With Desktop (Windows only)
* IR Key Transmission ("Beaming")
* File Wiping
* FreeSpace Wiping

Key Benefits:

Strongest & Trusted Encryption

The core of all security solutions is the quality and integrity of the underlying encryption. PGP supports a variety of encryption algorithms, but only those with a 128-bit or greater symmetrical crypto key length. PGP products do not interoperate with products using low-security and easily compromised encryption systems. To ensure the integrity of its products, PGP publishes source code for peer review.

Key Benefits (continued)

Time & Customer Tested

The true test of product quality is how it performs in real customer environments over a long period of time. PGP holds nine patents with more pending, its underlying technology has been in use for over a decade, and the current product line has evolved over the last six years. PGP products have proven themselves to be reliable and scalable during their time in use by thousands of enterprise and government organizations, and millions of individual users, including the experts in the cryptographic field.

Enterprise Manageability

Implementing effective security solutions requires the ability for security managers to set and enforce policy for encrypted messaging & data storage. PGP enterprise tools permit the pre-configuration of desktop software to conform to policy requirements, simplify its deployment, management, and ongoing use, and guarantees compliance with security policy. PGP provides a full solution from desktop, to policy and deployment, to key management and PKI.

Interoperable and Standards Based

Open standards are required for secure messaging and data security to be interoperable and therefore widely adopted; PGP is committed to non-proprietary, open standards including OpenPGP, also known as RFC 2440, and X.509. Though PGP has a full-function Keyserver product, it is PKI agnostic, supporting certificates and PKIs from all standards-conforming vendors. PGP supports LDAP-based directories inluding, iPlanet, Microsoft Active Directory, Novell NDS as well as wide range of SmartCards and other PKCS#11 tokens. PGP is has been certified as FIPS 140-1 compliant, a standard used by the U.S. and Canadian governments.

Multiple Platforms & Mail Systems

Security issues have proliferated with the growth of portable, and personal electronic devices. For security to be effective, users of all platforms and mail systems must be able to work together using the same products and keys. On Windows, PGP supports versions from Windows 95 to Windows XP. On Macintosh, PGP has products for both Mac OS 9 and Mac OS X. For mobile users, PGP currently offers Palm OS and Windows CE solutions. Via its SDK, PGP supports a variety of Unix systems. PGP products work in environments with Microsoft Outlook and Exchange, Lotus Notes, Novell GroupWise, and Eudora solutions.

End-to-End Security

A complete security solution requires messages and data to be protected in transit, at rest, and at every point in between. PGP solutions protect user data while stored on the sender's desktop, when it's within an outbound encrypted email message, while in transit within the perimeter of firewall-protected company network, across all its stops across the Internet, within the receiver's company network, to the receiver's desktop email folder, and in storage on the receiver's desktop. PGP solutions protect information end-to-end.

Advanced Key Features

The reconstruction, and recovery of keys is part of the practical reality of managing corporate security. A balance must be struck between keeping information secure and the need for a company to recover proprietary information held by its employees. PGP offers a variety of options including key reconstruction, integration of additional corporate decryption keys (ADK), and split keys that require multiple individuals to cooperate to recreate a key, such as an ADK.

Technical Specifications

Public Key Formats
OpenPGP RFC 2440
X.509

Symmetric Key Algorithms
AES with up to 256-bit keys
CAST
TripleDES
IDEA
Twofish

Hashes
SHA-1
MD5
RIPEMD-160

Public Key Formats
Diffie-Hellman
DSS
RSA v4 up to 4096-bit

Network Protocols
TLS/SSLv3 with OpenPGP Extensions

System Requirements
Palm OS 3.1 or above
200k of free memory