



The ultimate security solution for PDAs

Thanks to the PDA, true business mobility has finally become a reality. For many areas, a whole new world of opportunities is opening up – and a whole new world of risks. The very fact that PDAs are so portable means they are easily lost or stolen, along with the confidential data saved on them. In addition, Plug & Play functionality and wireless connection capabilities make them a serious threat to the security of company networks.

Current PDAs are not equipped to combat these risks so comprehensive protective measures are imperative. **SafeGuard PDA** provides the protection that is needed and keeps the mobile workforce secure. The strong encryption keeps data confidential – even in transit over the Internet. Innovative authentication mechanisms, such as biometric signature recognition or symbol PIN, offer optimal user convenience and peace of mind for business managers and IT staff. Transparent background operation means users do not need training or elaborate new work routines. And easy central implementation and enforcement of the company security policy keep the environment consistently protected.

User convenience is critical in any authentication solution. **SafeGuard PDA** meets this requirement and is the optimal choice for companies that must enforce a PDA security policy via central administration along with efficient recovery functions.

Together with our **SafeGuard Easy**, **SafeGuard PrivateCrypto** and **SafeGuard PrivateDisk** products, **SafeGuard PDA** builds a perfect security solution for the complete IT infrastructure, including servers, PCs, and mobile devices.

About Utimaco Safeware

Utimaco developed its first IT security software in 1983. Today, Utimaco is a global leader in enterprise information security. Using the most advanced techniques, Utimaco software provides unmatched information security. Highly reliable, easy to use, and easy to administer, Utimaco products ensure low total cost of ownership. For more information, visit www.utimaco.com

Enhanced security

- Perfect protection of PDAs against unauthorized access
- Transparent protection of data in PDA memory and removable media against unauthorized access
- Simple, encrypted data exchange with PC platform via removable memory cards or E-mail
- Efficient company-wide enforcement of uniform security policy

Easy to deploy

- Smooth integration in existing IT environment
- Scalable roll-out mechanisms for software and configuration
- Support for existing administration and distribution mechanisms e.g. Microsoft Active Directory or PDA Software management tools from third party vendors
- Flexible, centrally enforceable configuration rights for end-users

Easy to use

- Intuitive user interface, adaptable to company needs
- Flexible logon methods, adaptable to user needs
- Reduced help-desk workload through simple reset of forgotten passwords

Key Features/Functionality

Security

- Secure user authentication
 - Alternatively via password, symbol or numeric PIN, biometric signature^{*)} or fingerprint (for IPAQ 545x / 555x)
 - Organization specific password rules
 - Increasing delay time with increasing number of false tries
 - Alarm sound or complete memory erase in case a definable threshold of false tries is exceeded^{*)}
- Secure Screen Saver
- Device lockdown functions securing the configuration
 - Optional central blocking of infrared port, Bluetooth, WLAN or phone functionality^{*)}
 - Configurable prevention of ActiveSync with non-company devices^{*)}

Comprehensive encryption capabilities

- PIM databases (calendar, contacts, tasks, E-mails/SMS)
- Files in local RAM, flash file store
- All current storage card formats
- Encryption keys derived from password via PKCS#5 standard to harden password guessing attacks
- Encryption compatible to SafeGuard PrivateDisk and SafeGuard PrivateCrypto, exchange of encrypted data between PDA and PC via e-mail or memory card^{*)}

Support for Windows Mobile PDA Phones

- Configurable option whether active calls require authentication
- Centrally definable "emergency numbers"
- Optional GSM SIM lock to prevent unauthorized change of SIM card

System administration

- Central configuration via Microsoft Management Console (MMC)
- Configurable user appearance, security settings, encryption and password rules
- Administration rights for end users, collectively or individually configurable by system administrator
- Central distribution of security settings via:
 - Active Sync with Windows Active Directory Group Policies^{*)}
 - Active Sync with Windows System Policies^{*)}
 - Dedicated third party software management tools (e.g. Extended Systems, Novell ZenWorks for Handhelds)
- Protection against unauthorized deinstallation
- Optional automated re-activation after a hard reset including the recently valid settings and passwords for continuous protection of the PDA rendering it useless to a thief (on PDAs with persistent Flash Filestore and autorun capability^{*)})

Ease of use

- Automated encryption without user intervention
- Efficient algorithms – negligible performance impact
- Secure and powerful challenge/response procedure to reset forgotten passwords without the need for on-line connection
- Single Sign On to most common VPN systems (e.g. IBM WECSM, Columbitech WVPN, Netseal MPN, NCP VPN^{*)})
- API for integrating security functions in custom written applications^{*)}

System Requirements

Operating System

- Windows Mobile 2003 incl. Phone Edition
- Windows Mobile 2003 Second Edition incl. Phone Edition
- Symbian Series 80 (Nokia Communicator 9300/9500)
- Symbian UIQ 2.1 (Sony-Ericsson P900/P910i)
- Minimum free memory: Windows Mobile 3 MB, Symbian 200KB, PC < 10 MB (if administration via ActiveSync is used)

Certifications

- Designed for Windows Mobile
- Symbian Signed (planned)
- FIPS 140-2 for SafeGuard PDA (cryptographic library in evaluation)



Complementary SafeGuard® products

- SafeGuard PrivateDisk for exchanging virtual encrypted volumes on storage cards with PC platform
- SafeGuard PrivateCrypto for exchanging encrypted E-mail attachments or files with PC platform
- SafeGuard Easy for protecting data stored on PC clients via harddisk encryption and pre-boot authentication

Interoperability

- SafeGuard PDA is compatible with all leading software distribution tools for PDAs
- VOICE.TRUST server for automated biometric challenge/response helpdesk
- Encryption format compatible to SafeGuard PrivateDisk, SafeGuard PrivateCrypto on PC^{*)}

Standards/Protocols

- AES (128 and 256 bit), X.509 Recovery Certificates^{*)}

Language Versions

- English, German, French

Contact Data

Utimaco Safeware AG

P.O. Box 20 26
DE-61410 Oberursel
Germany
Phone +49 (61 71) 88-0
Fax +49 (61 71) 88-10 10
info@utimaco.com

More information about SafeGuard PDA:

www.utimaco.com/pda

Utimaco Safeware Partner:

*) Function available for Windows Mobile only.

Copyright Information

© 2005 – Utimaco Safeware AG

SafeGuard® PDA 3.0 for Windows Mobile, SafeGuard® PDA 4.0 for Symbian and SG PDA 4.10 for Windows Mobile 5.0 planned for autumn 2005..

All SafeGuard Products are registered trademarks of Utimaco Safeware Ag. All other named trademarks are trademarks of the particular copyright holder.

Microsoft, Windows, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

utimaco[®]
safeware