

## PDA-PROTECT™

May 2003

### IMPORTANT README

Please Read And Print For Reference Before Installing PDA-Protect

#### Crypto-Sign™ - PDA-Protect for Pocket PC 2002

##### Introduction

Crypto-Sign™ is a patent-pending remote authentication technology based upon the submission of a secret sign. PDA-Protect is a Crypto-Sign based product and has been developed for Pocket PC 2002 device access control. It is used to control the release of the password to enable the device at power-up or whenever a password is required. **This means that the Password will not have to be remembered or entered each time it is used and a record of it may be stored in a secure location for access, if needed, to set up an ActiveSync partnership at your workstation.**

Different Crypto-Sign software can be used to generate/release a key for encryption purposes or to attach an electronic signature to an electronic document.

PDA-Protect uses pen-based input from the PDA digitizer to record a secret sign, submitted with the inking turned off, in an area of the screen delineated by a rectangular box. The secret sign is then compared with a previously established reference template to establish authenticity.

##### Installation/Uninstall

The software is delivered via an email attachment as an executable file zipped with this document. The email will also indicate the number of licenses covering the number of workstations and devices onto which the software may be loaded.

##### IMPORTANT

##### Before Installing

- 1) **If your PDA is already Password protected prior to installing PDA-Protect, please remove the password protection using the Password option in Settings/Personal.**
- 2) **Complete your Owner Information and check the "Show information when device is turned on"**
- 3) **We recommend that you back up your Pocket PC data using the Backup/Restore tool in ActiveSync.**

##### Installing

- 1) Next, choose, make a note of and store in a secure location, a (new) password (minimum of 8 alpha numeric characters – case sensitive), which Crypto-Sign will use to grant access. Do not set the password at this time.
- 2) Place the installation software in a directory of your choosing and then place the Pocket PC upon a cradle or set it up for Infra Red communication with the workstation. Wait for synchronization to complete.
- 3) Run the PDA-Protect Setup software and follow the install prompts.
- 4) Remove the PDA from its cradle and perform a (soft) reset using the stylus to depress the reset button. This will replace the Password icon in Settings/Personal with the PDA-Protect icon in Settings/System.
- 5) If there is a need at a future date to uninstall the software, follow the Uninstall procedure (see below).
- 6) Open up the PDA, select Settings/System/PDA-Protect.
- 7) Check the "Enable Crypto-Sign" box. This enables you to register your authentic signature and your secure sign and to practice it before enabling the protection mechanism via "Set Password." Do not "Set Password" at this stage.

##### Registration Process

Tap "Register." The owner is asked first to register his/her authentic signature. This signature is displayed as it is written and the user is asked to accept or re-sign until a suitable signature is recorded. Following the acceptance of the authentic signature, the user is asked to submit the chosen secret sign (see below)

##### Choice Of A Secure Secret Sign

In order to give the sign a suitable level of security, it should contain sufficient information. Consequently, it is recommended that:

- 1) The sign time is at least 1 1/2 seconds.
- 2) The sign contains a number of pen-up segments.
- 3) The sign contains multiple "turning points" where a turning point is a change in X or Y direction.

A typical signature might contain these properties, as might a hand-printed word or number sequence. A combination of foreshortened signature and hand-printed characters, perhaps written on different "lines" will often display sufficient

complexity for a secure sign. Tests will be conducted during registration to ensure the sign exceeds a minimum of natural security. A screen (see below) depicting more and less secure signs is presented to help the sign selection.

**You Will Now Be Asked To  
Submit Your Secret Sign**

- 1) Choose the sign with care.
- 2) Choose a sign lasting at least 1.5 seconds.
- 3) Choose a multi-contact sign.
- 4) Choose a sign with numerous direction changes in both X and Y.
- 5) Choose a sign you can easily reproduce
- 6) There will be no inking as you write.
- 7) Practice your sign on paper first.

**Example of A More Secure Sign**



**Example Of A Less Secure Sign**



**Form the Crypto-Sign Template**

Following registration of the authentic signature, the user is requested to submit the first secret sign. Hit "Accept"(or "Re-sign" if you would like to re-do your secret sign before submitting it for analysis and inclusion in the template). Repeat this process until the system has determined that the signs are consistent, signaled by the display of your authentic signature in the box. At this point the Crypto-Sign template will be formed. It will take a minimum of three signs to form the template. Hit OK to proceed.

**Establishing the Template**

After registering the authentic signature and the secret sign, the user should hit "Verify" and then, after submitting the secret sign, "Accept" (or Re-sign). A successful test against the secret sign template returns the user to the PDA-Protect set-up screen where this process should be repeated until there is a level of comfort with submitting a successful secret sign. A failed sign will be indicated during this learning phase with a "Crypto-Sign Did Not Match " message prior to returning to the set-up screen for further attempts after hitting OK.

We recommend that users first become familiar with submitting a consistent well-chosen secure sign before enabling protection by tapping "Set Password." It is also recommended that the template establishment period cover at least 10 successful signs submitted over a period of time, some of which should be prior to powering off the device (this will leave the screen intact for another attempt at power-up). During this time the device will have no Password or Crypto-Sign protection so it is recommended that this procedure be completed within one day. Enter PDA-Protect from the icon in Settings/System during this time.

**Re-registration**

The owner may re-register his/her sign at any time by hitting the "Register" button. Prior to re-registration a successful Crypto-Sign test will be required. The password may also be changed at any time (after a successful Crypto-Sign test) without the need to remember the old password. The new one will be required at the next ActiveSync.

### **Keep Your Secret Sign Secure**

Your secret sign is much more secure if you keep it secret.

- Don't tell people what it consists of
- Don't let people oversee you when entering it on your PDA
- Keep it secret in the same way you keep your PIN secret.

### **Set Password and Time delay**

This is the point when the power-up protection offered by Crypto-Sign is enabled. The "Set Password" process requires password entry using the "keyboard" icon. Tap out a strong alphanumeric password or phrase (minimum of 8 characters). Make a note of the password prior to entering it. After entering and confirming the password set the time delay to a period you feel comfortable with. If the time delay is set for 15 minutes, for instance, Crypto-Sign will not be invoked until 15 minutes has expired from the next power down.

The password will be required at your workstation during the next ActiveSync. If you check the "Remember Password" box on your workstation you will not have to remember the password again. However, it is recommended that a note be made of the Password and that it be stored in a secure location, convenient for access from the workstation but not upon the person. In the event the password is lost and forgotten, it may be changed without remembering the old one using "Set Password" from the PDA-Protect screen via the icon. – after a successful Crypto-Sign test.

### **Choose The Level of Protection**

There are three levels of protection offered and it might be appropriate to start off at one of the first two levels where the action for three consecutive mis-matched signs is a Power-Down. One of these two actions results in the mis-match count being reset to zero and the other results in this count being reset to two (from three). When you are comfortable that you can submit your sign without triggering three consecutive mis-matched signs, then it is time to enable the Clear Memory or "Hard Reset" protection.

### **Hard Reset**

This action gives you the highest level of protection, for if the PDA falls into the wrong hands, there will only be three opportunities to submit the correct secret sign on the unit before it clears the memory of all data, including the Crypto-Sign program. In this instance the device will return to its original factory settings. It is strongly recommended that, if this level of protection is used, the data be backed up on the PC using the option in the ActiveSync software.

### **Normal Use**

**Following this process you can power up and sign on at any time by, simply and conveniently, submitting your secret sign, without having to remember or enter a password but with the knowledge that your system is securely protected. You can also enter PDA-Protect at any time from the PDA-Protect icon in Settings/System, to re-register or to demonstrate Crypto-Sign to a colleague or friend (using the "Verify" button)**

### **Disabling/Re-enabling PDA-Protect**

If you want to disable PDA-Protect temporarily, simply uncheck the "Enable Crypto-Sign" box. To re-enable PDA-Protect, re-check the box

### **Uninstalling (after gaining access)**

Should you feel the need, at any time to uninstall the software, this should be done using the original installation software.

#### **To Uninstall The Software And The Secret Sign template**

- 1) Place the device on the cradle and wait for synchronization to complete.
- 2) Run the Installation Software and follow the Remove instructions.
- 3) Remove the device from the cradle and perform a soft reset. This should remove the PDA-Protect icon and re-install the Password icon in Settings/Personal. If it does not, remove PDA-Protect using the "Remove Programs" icon in Settings /System and then perform another soft reset.
- 4) Enter the Password process from the Password icon now in Settings/Personal..
- 5) Reset to your required level of password protection.

In the unlikely event that you cannot gain access to your device using your secret sign you can use the uninstall procedure above or perform a Hard Reset operation using the facility provided on the Pocket PC or through submitting three wrong secret signs (if the Hard Reset action is chosen). This is why it is important to back up all your data using the capability in ActiveSync.

**Questions:**

In the first instance these should be addressed to your supplier.

**PDA-Protect  
Frequently Asked Questions**

**1) Why is the Secret Sign more effective than the Password?**

- a) If the Password is known (or can be guessed) by an impostor, the system is compromised with 100% certainty. If the Secret Sign is known (or can be guessed) by an impostor, it is still extremely difficult to reproduce the sign in the same manner as the legitimate author.
- b) Unlike the Password, the Secret Sign does not need to be entered via the keyboard icon. So, it is much easier to enter than an 8-character, case-sensitive Password.
- c) The Secret sign is much more easily remembered than an 8-character, case-sensitive Password and does not need to be changed if the Password is changed.
- d) The Password released by the Secret Sign can be changed at any time without the need to remember the old Password or change the sign.

**2) Why is it important to back up my data before installing PDA-Protect?**

If the installation sequence is not followed correctly, prior to and during installation, it is possible that you may be faced with a hard reset. If the data are backed up it is easy to return to the original state and recommence installation.

**3) Why is it important to remove Password protection before installing PDA-Protect?**

If you have set the Password from the Password icon in Settings/Personal, this record has to be removed before setting the new password from PDA-Protect. Failure to follow this procedure may result in the need to perform a hard reset (especially if these data have not been backed up), which will erase all data and programs.

**4) Why is it important to complete the Owner Information and bring the screen up when the device is first turned on?**

If the device is lost it provides the finder with the opportunity to return it to you.

**5) Do I need to remember the Password I set at Registration?**

You will need to enter the Password at the next ActiveSync (after you have gained access to your computer) This is one reason why it is important to make a note of the password and store it in a secure place, adjacent to your computer but not on the person. If you check the "Remember Password" on your computer you will not need to enter it again. If you cannot remember the Password at any time you can change it to a new one (after you have submitted the Secret Sign) without having to enter the old Password.

**6) What happens if I cannot gain entry at power-up when I submit my Secret Sign?**

The program can be Uninstalled from the Sign screen after synchronization or by performing a hard reset, restoring from the backed-up data and then Uninstalling.

**7) Why do I need to register my Authentic Signature?**

This becomes part of the Crypto-Sign template and future software releases may use it as an electronic signature to be released to a transaction or document after a successful match against the Secret Sign template.

**8) When I power up my device, sometimes I am not asked for a Secret Sign**

- a) Perform a soft reset in case this was not performed after installation.
- b) Inspect the value of the PDA-Protect setting – "Prompt if Device not used for."  
This timer takes effect from power off. If it is set to (say) 1 hour and the device is constantly switched off (automatically or manually) and on, with off-intervals less than 1 hour, then no Sign will be prompted.

- c) Set the time interval to a setting which reflects your frequency of use and which ensures you are prompted for a Secret Sign as often as you are comfortable with. A setting of zero is not recommended but may be needed for demonstrations.

#### **9) What Action should I set after three Crypto-Sign mismatches?**

Start with the action as a power down with the fail count reset to zero.

When you are comfortable with this action move to power down with fail count decremented by one.

When you are comfortable with this, if you are in a high-risk scenario you may want to set the highest protection level (hard reset) but you should ensure you back up your data first.

## **CRYPTO-SIGN™ PDA-Protect -Demonstration Guidelines**

If you are demonstrating PDA-Protect to a colleague or potential customer

### **1) Choose Your Sign Carefully and Establish it on the PDA**

See above for what constitutes a secure sign.

Ensure you are comfortable with the sign you choose. Register yourself and establish your template by launching PDA-Protect from the icon and by signing (using the “Verify” button) over an extended period of time with significant gaps between signs. Do not sign continuously during a short period of time while establishing the template. The last twenty signs submitted represent 95% of your template values

### **2) Demonstrate Your Own Sign As Owner**

Demonstrate PDA-Protect by signing on at Power-Up and emphasize the need to keep the sign secret by not allowing anyone to oversee you. Even if it means turning away from the person or people to whom you are demonstrating. This helps to emphasize the best practice of keeping the sign secret.

Power off and encourage your friend/colleague to try and gain access by reproducing your sign (even though they have no idea what it is). This helps to emphasize just how difficult it would be to reproduce a successful Crypto-Sign.

### **Do Not:**

- 1) **Do not allow an “impostor” to attempt to reproduce a newly registered sign – especially if (s)he has observed the enrollment of the genuine sign. Explain that the template is updated after each good sign and that it has not yet matured.**
- 2) **Do not allow people to observe the signs made by you or others. Explain that, just like a PIN or a password the sign is a secret.**
- 3) **Do not experiment or encourage others to experiment with their genuine sign. This can lead to a variable template, which can be both insecure and difficult for the genuine author to reproduce.**