WHITE PAPER

January 2003

Prepared by
Smart Handheld Group

Hewlett-Packard
Company

CONTENTS

biometrics and FingerChip technology 3
overview 3
benefits 3
how it works 4
enrollment 4
verification 4
authentication software security levels 6
iPAQ Fingerprint solutions 7
PIN, password, and fingerprint setup utility 7
enrolling your fingerprint........8
setting the security options 9
SDK for the iPAQ Pocket PC h5400 10

biometric security with the iPAQ Pocket PC h5400 series

Biometric technology is the latest trend in security. From securing access to a building or preventing unauthorized logons, this technology and the software designed for it, work together to provide an extra layer of security for your iPAQ Pocket PC h5400 Series. This easy-to-implement security capability goes beyond requiring a simple logon name and password to gain access to the data on your iPAQ Pocket PC.

This paper discusses the biometric technology, notably the fingerprint, and how it is used with the iPAQ Pocket PC. The biometric software for administering this security feature is also discussed.

Notice

The information in this publication is subject to change without notice.

HEWLETT-PACKARD COMPANY SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

This publication does not constitute an endorsement of the product or products that were tested. The configuration or configurations tested or described may or may not be the only available solution. This test is not a determination of product quality or correctness, nor does it ensure compliance with any federal, state or local requirements. Hewlett-Packard Company does not warrant products other than its own strictly as stated in Hewlett-Packard product warranties.

Other product and company names mentioned herein may be trademarks and/or service marks of their respective owners.

First Edition January 2003

Part Number 5981-4266EN

biometrics and FingerChip technology

With the limitations of existing security tools (such as user IDs and passwords) becoming evident, biometrics have become a promising solution in providing security to computer systems. The following sections explain biometrics and the benefits of its implementation.

overview

Biometrics is the process of measuring a physical or behavioral characteristic of a person and using that measurement as a basis for later identifying that same person. This measurement could be a face or eye measurement or in the case of the iPAQ Pocket PC, the fingerprint. Two things are essential to the biometrics application for the iPAQ. One is collecting biometric information like fingerprint images. The other is classifying, analyzing, and identifying biometric data. The iPAQ Pocket PC h5400 Series is enabled with fingerprint capture technology known as the FingerChip that was developed by Atmel Corporation, a leader in the design and development of biometric technology. The iPAQ Pocket PC fingerprint identification technology is provided by Cogent Systems, Inc., a global leader in automatic fingerprint identification system.

Why the finger? According to studies, fingerprints are the most reliable biometric feature for identifying individuals. Even identical twins have different fingerprints. In over 100 years of use, fingerprints have proven to be a reliable tool for establishing identification.

This measurement of fingerprints can be accomplished using a variety of methods, but the most promising, and the one used for the iPAQ Pocket PCs is thermal imaging. Thermal imaging is one of the most reliable methods available.

Thermal imaging reads the differences in temperature between the ridges and valleys that make up a fingerprint. This method has several benefits. Among these benefits is that thermal imaging has a strong immunity to electrostatic discharge and the fact that it functions well in extreme temperature conditions. Additionally, thermal imaging is almost impossible to deceive with artificial fingerprints.

The thermal imaging technique is coupled with an image scanning process to deliver the best possible combination that provides for a lower cost to operate, reliable functionality, and security against artificial fingerprints.

benefits

The main reason for using a fingerprint for biometric security is the uniqueness of a fingerprint. The fingerprint can take a lot of wear and tear and still grow back in the same pattern (except in extreme cases). Combining the uniqueness of a fingerprint with scanned thermal imaging to take a reliable read yields a unique biometric for establishing identification. Processing of this biometric by highly accurate fingerprint matching algorithms provides a strong tool to ensure that only the person with authorization to use your iPAQ Pocket PC will be permitted to do so.

Another benefit of the iPAQ biometric solution is ease-of-use. The user interface is simple to understand and setup is a short and easy process.

Whereas your PIN or password may be stolen, this is not likely to occur with your fingerprint. Also, you may forget your PIN or password, but not your fingerprint.

how it works

Biometric security on your iPAQ Pocket PC works in two basic steps: fingerprint enrollment and fingerprint verification. Fingerprint enrollment involves fingerprint acquisition and image reconstruction, fingerprint image processing and feature extraction, fingerprint image quality evaluation, and template generation. Fingerprint verification involves fingerprint acquisition and image reconstruction, fingerprint image processing and feature extraction, fingerprint image quality evaluation, template generation, and template matching.

enrollment

Enrollment is the process of collecting, processing, and registering reference versions of the fingerprints of the person authorized to use the secured device, in this case, the iPAQ Pocket PC. This is the initial step. The user is guided through the process for selecting one or more fingers to enroll and swiping the selected fingers across the FingerChip sensor to capture associated fingerprint images. Enrollment assesses the quality of the captured images and directs the user, as required, to repeat the swiping activity until adequate images are obtained. This process may require several attempts to ensure good prints are captured. A dataset is extracted from the images for each finger enrolled. These datasets are the reference templates used to ensure that only the authorized user is allowed to logon to your iPAQ Pocket PC during verification. The iPAQ Pocket PC enrollment process includes user training designed to teach proper swiping of fingers across the FingerChip sensor.

These templates are stored locally on the iPAQ Pocket PC (in a *BioSwipe.dat* file) and are encrypted. The file is only decrypted when used by the BioSwipe software. Template coding is a Cogent private format. Only Cogent software can read and use the template data. The encryption code is also private. Only BioSwipe or Cogent software can decrypt the data.

verification

Verification is the process of collecting, processing, and comparing a person’s fingerprint with the fingerprints on record to confirm identification or deny access. Based on the designated authentication mode, the user will swipe an enrolled finger across the FingerChip sensor to capture the associated fingerprint image. Verification assesses the quality of the captured image and, if necessary, directs the user, to repeat the swiping activity to ensure that a good quality image is obtained. A dataset is extracted from the fingerprint, designated the sample template. The sample template is matched against the reference templates stored on your iPAQ Pocket PC. The result of the match is used by Pocket PC authentication to permit or deny access as appropriate.

As noted, there are several sub-processes, many of which are common, that support enrollment and verification. The next sections describe these sub-processes.

fingerprint acquisition and image reconstruction

As mentioned earlier, scanned thermal imaging works because the fingerprint is made up of ridges and valleys that each emits different thermal readings. Pyro-electric material converts the differences in these temperatures into corresponding voltages. Since fingerprints are unique, so to are the voltages that are derived from them.

The question now becomes how best to capture this thermal fingerprint image? The process that works best for this image capture is known as image scanning. With this process, a rectangular window (with a width the size of a finger) is used. The fingertip is swept vertically over this sensor window and the image is recorded in sections and then reconstructed by software.

Fingerprint acquisition and image reconstruction is used for both enrollment and verification.

fingerprint image processing and feature extraction

Reliable fingerprint feature extraction is the foundation of accurate fingerprint matching. Algorithms and software are developed to analyze a fingerprint image and to extract the information that can be used to uniquely identify a person. This is achieved in two steps. First, the fingerprint image is transformed into a form that facilitates feature detection. Second, the image is further analyzed to detect local and global features like ridge flow, minutiae points, fingerprint pattern, ridge counts, etc. The results are passed on to fingerprint image quality control.

Fingerprint image processing and feature extraction is used for both enrollment and verification.

fingerprint image quality control

Image quality control is introduced to maintain the quality of the data collected. This is very important to a fingerprint security application since data reliability contributes directly to verification accuracy. Each captured fingerprint image is evaluated and only those that pass the quality criteria are accepted for further use.

Fingerprint image quality control is used for both enrollment and verification.

template generation

In the process of enrollment, fingerprint features extracted, like minutia and ridge counts, are organized into templates. These templates are called reference templates, or the templates on record.

During verification, when you scan your fingerprint, a similar template is created. This template is called a sample template.

template matching

During template matching, the sample template is compared to the set of reference templates stored on your iPAQ Pocket PC. Because a 100% exact match is unlikely due to various factors, a probability is established. This is done by using a matching algorithm that tests various orientations of the extracted image and the degree of correspondence of the minutiae. The algorithm assigns a numerical score to the match. This score is then compared to a pre-established setting. If the numerical score is above the threshold, then a match is declared. Otherwise, logon fails.

Template matching is unique to verification processing.

authentication software security levels

The biometric software called BioSwipe is based on capabilities developed by Cogent for use in criminal Automatic Fingerprint Identification Systems that require highly accurate capabilities for performing 1-to-many searches of very large databases. The Cogent algorithms analytically model natural irregularities that define uniqueness in fingerprints, providing the scientific foundation for establishing positive identification. BioSwipe adapts the Cogent algorithms to the one-to-few verification requirements of the iPAQ Pocket PC. In establishing authentication, the biometric software can be set up to operate in three security level environments: Regular, High, and Extra High. These security levels are based on expected false rejection rates (FRR), false acceptance rates (FAR), and enrollment strategies (see the table that follows). As the security level rises, so does the intensity of the parameters that are used for enrolling a fingerprint and for achieving a match.

A false acceptance is achieved when sample and reference templates produce a numerical score that meets the pre-established threshold for acceptance, even though the images are not from the same fingerprint. A false rejection results when an enrolled person does not achieve an acceptable score when the sample and reference templates are compared. In establishing the different security levels, there is an inverse relationship between the FAR and FRR. When the security level rises, FAR decreases while FRR increases. In determining the best level, generally you would want to decrease the FAR based on likelihood of security breaches and database size. In the case of your iPAQ Pocket PC h5400 Series, the default security level is Regular as the device is for personal use and the threat of a security infringement is low.

The following table shows the iPAQ Pocket PC FRR and FAR performance test results for the various security levels.

Security Level	FRR	FAR	Average number of attempts
Regular	0.2331 % (1 out of 429)	0.0010 % (41 out of 4054737)	1.081967
High	0.4662 % (2 out of 429)	0.0001 % (4 out of 4054737)	1.107573
Extra High	0.6993 % (3 out of 429)	0.0000 % (0 out of 4054737)	1.153226

iPAQ Fingerprint solutions

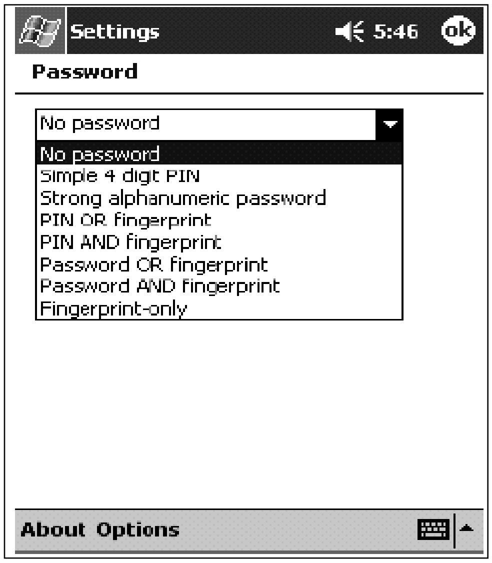
The iPAQ Pocket PC h5400 Series, combined with the FingerChip technology and the BioSwipe software, provides you with a complete biometric option for securing your data. The following sections highlight this security feature as it is used on your h5400 series.

PIN, password, and fingerprint setup utility

With the iPAQ Pocket PC h5400 Series you can augment your traditional password security features by implementing the fingerprint authentication function. This provides an added layer of security in preventing unauthorized use or access to your iPAQ Pocket PC.

A graphical user interface is provided for a PIN, password, and fingerprint setup utility and training (enrollment) along with user logon control (authentication). In establishing the security of your unit, you can use the following access profiles:

- **No Password (default)**—this profile requires no password, PIN, or fingerprint to log on to your iPAQ unit.
- **Simple 4-Digit PIN**—this profile is based on establishing a numeric PIN number just like you use for ATM cards or other personal accounts.
- **Strong Alphanumeric Password**—this profile requires the entry of a minimum seven character, case-sensitive alphanumeric password.
- **PIN or Fingerprint**—this combination requires either a PIN or fingerprint to be entered.
- **PIN and Fingerprint**—this combination requires both a PIN and fingerprint to be entered.
- **Password or Fingerprint**—this combination requires either a password or fingerprint to be entered.
- **Password and Fingerprint**—this combination requires both a password and fingerprint to be entered.
- **Fingerprint Only**—this profile requires only a fingerprint be entered.

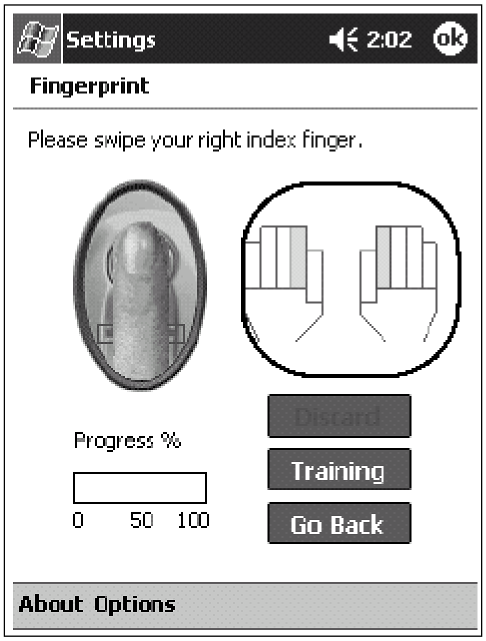


Password

No password

enrolling your fingerprint

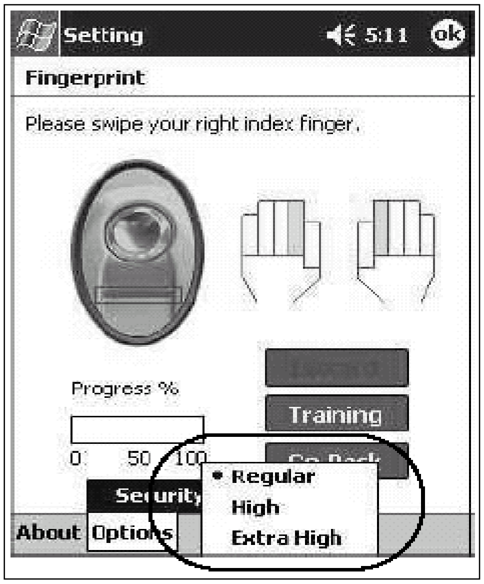
When you first setup the iPAQ Pocket PC h5400 Series, if any of the fingerprint-related authentication functions are selected, then one or more fingers must be enrolled. A reference template will be created for each enrolled finger. These templates will be used to compare to future fingerprint logon attempts. This process is aided by a training tool that is available with the iPAQ Pocket PC h5400 Series.


Please swipe your right index finger.

You have the option of enrolling any fingers on either hand. It is recommended that at least two fingers be enrolled in the event that one of the enrolled fingers is damaged. The index fingers of both hands are recommended. Because of the size of the images available, it is recommended that the little fingers not be used. In order to enroll a fingerprint, you must take between two and eight qualified finger swipes. A qualified swipe is one that produces an acceptable image. Feedback is provided to let the user know that: a swipe was too fast, a swipe was too slow, a poor quality image resulted, or a good image resulted.

setting the security options

The security level can be set to Regular, High, or Extra High. The security level dictates how stringent the criteria are in establishing a match between a reference (enrolled) fingerprint and the sample fingerprint. Due to the nature and use of the iPAQ Pocket PC h5400 Series, the recommended setting is Regular.



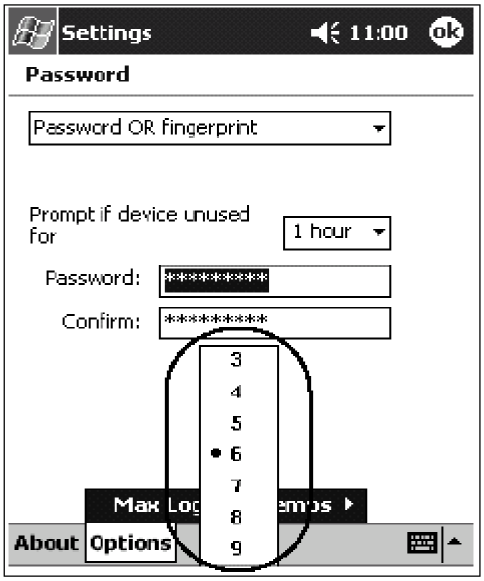
Setting

Fingerprint

Please swipe your right index finger.

Security: • Regular

Another option that can be entered is the maximum number of attempts allowed in establishing a match. Note that this is the number of attempts to gain access to the unit regardless if it is by way of password, PIN, or fingerprint. The acceptable range is three to nine attempts. The default setting for this option is six.



Settings

Password

Password OR fingerprint

Prompt if device unused for: 1 hour

Password: *********

Confirm: *********

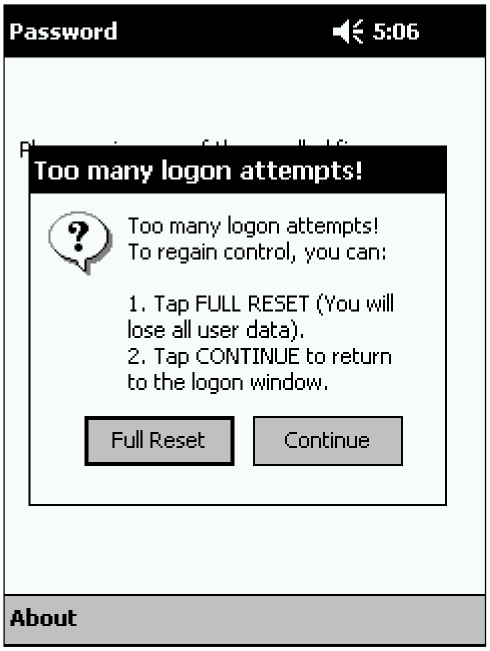
Max Log… emps: • 6

Care should be taken in establishing this control. If the maximum number of attempts is exceeded, then the user is prompted to indicate whether additional logon attempts are to be permitted, or if the user desires to do a full reset of the iPAQ unit. If the user selects the full reset option when prompted by the application, all information stored in RAM and the iPAQ File Store will be lost and the device will be returned to an as-shipped configuration.

Important: When a full reset is performed, the following will result:

- All data in RAM and the iPAQ File Store will be lost.
- The fingerprint image that is used to establish a match will be lost and must be recreated. Refer to the "enrolling your fingerprint" section in this document for instructions on establishing the fingerprint image.
- A full reset can only be initiated when the user fails to authenticate themselves to the unit.

Note: A full reset and a hard reset are not the same. A hard reset is performed by simultaneously pressing the two outer application buttons and the reset button on the bottom of the handheld. The hard reset does not delete the iPAQ File Store.



Too many logon attempts!

Too many logon attempts!
To regain control, you can:

1. Tap FULL RESET (You will lose all user data).
2. Tap CONTINUE to return to the logon window.

SDK for the iPAQ Pocket PC h5400

The new SDK for the iPAQ Pocket PC h5400 is now available on the support portal for the iPAQ Developer Program website. The SDK provides APIs found on the previous iPAQ Pocket PC platforms as well as a separate API and sample code for using the integrated wireless LAN radio. Additionally, biometric API specifications, library files, and sample code has been posted to the site to enable developers to authenticate local users in their applications using the biometric reader on the device.