



## Protector Suite QL 5.6 – Securely Protecting your Computer

### Application Note

Release <1.0>



Information furnished is believed to be accurate and reliable. However, UPEK, Inc assumes no responsibility for the consequences of use of such information not for any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of UPEK, Inc. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied. UPEK, Inc's products are not authorized for use as critical components in life support devices or systems without express written approval of UPEK, Inc.

UPEK, the UPEK logo, TouchChip, PerfectPrint, PerfectMatch and PerfectTrust are trademarks or registered trademarks of UPEK, Inc. All other products described in this publication are trademarks of their respective holders and should be treated as such.

© 2006 UPEK, Inc - All Rights Reserved

## 1 Protector Suite QL 5.6 Overview

### Main Features & Benefits

- **Always-on access**
  - Finger-activated logon to Windows
  - Finger-activated application launch
  - Finger-activated Windows lock
  - Finger-activated logon to websites
  - Fast User switching (Windows XP & Vista)
- **Password Management**
  - Encrypted capture and replay of login credentials – no need to remember usernames/passwords
  - Easy registration and replay of password dialogs for convenient access to websites
  - Support for Internet Explorer and Firefox
  - Exportable Passport & Password Bank for import into other computers (without enrolling or re-registering)
- **Encrypted File & Folder Protection**
  - Fingerprint-enabled encryption/decryption of important files and folders
  - Access control rights allow several users on a domain or network to securely access encrypted file or folders
- **Convenience Features**
  - Self-guided tutorial and enrollment wizard ensures quick and easy set up
  - Control Center provides easy access to fingerprint management, security and system & user options
  - Finger-activated launch of commonly used applications
  - User-selectable Biomenu skin for custom look
  - Lock/unlock computer with finger swipe
  - Window scrolling using the fingerprint sensor
  - Audible feedback confirmation
- **Windows Support**
  - Runs on Windows XP, Vista, 2000, 2003
  - Runs on 64-bit Windows XP & Vista
  - Runs on biometric-enabled notebook computers (using UPEK fingerprint hardware) from: Lenovo, Dell, Sony, Toshiba, Panasonic, Acer & Asus
- **Pre-Boot Security**
  - For TBX enabled Notebooks and Desktops pre-boot protection
- **Language Support**
  - US English, German, French, Italian, Spanish (Neutral), Japanese, Simplified Chinese, Korean, Traditional Chinese, Greek, Dutch (Netherlands),



Portuguese (European), Russian, Portuguese (Brazilian), Finnish, Swedish, Norwegian, Turkish

## 2 The need for better computer security

Increasingly, our computer systems at home and at the office contain more and more sensitive information about ourselves, our company and our customers. Protecting these systems is paramount to combat the rising tide of identity theft, corporate espionage and to comply with regulatory demands to help protect private data. Networking infrastructure and software has made gains in recent years to prevent intruders from getting in from the outside. But how do you protect your computer system from intruders when it is lost, stolen or connected on an insecure network? The only defense today is by using “strong” passwords.<sup>1</sup> Strong passwords make it more difficult to guess or hack into a computer system. However, the associated inconvenience to the user is extremely high. Corporate policies that force users to choose long, complicated passwords often lead to higher support costs due to the time spent by support personnel to reset forgotten passwords<sup>2</sup>. Multiply this cost by the number of computers, networks and applications that a user uses on a regular basis and the cost quickly rises. And strong passwords, tend to lead to less security in cases as users write down complex passwords so that they can refer to them later. In the case of “home” users, they often store their sensitive passwords on the computer itself, leading to potential password theft from Trojan horses and other malware.

## 3 The move to stronger authentication

To address issues of security while balancing user convenience, several solutions have been introduced to the market with varying results. Software solutions tend to work on the premise of a “master” password. The theory being that having to remember a single complex password is easier than remembering many. However, if the master password is compromised, every password and system can be compromised. Hardware solutions provide better security, but require users to carry cards or hardware tokens that are easily lost (or forgotten at home). In these cases, users must revert to traditional insecure access methods (until their hardware is replaced or recovered), lowering security to the lowest common denominator. Other methods utilize “multi-factor” authentication – a combination of “what you know”, “what you have” and “who you are”, often combining software & hardware authentication techniques. While generally considered to be more secure, these multi-factor solutions are also much more complex for the user and fraught with all the problems mentioned previously.

But what if there was a way to have hardware-level security without the associated problems of losing the means to authenticate your identity? That would provide the most compelling solution of all.

---

<sup>1</sup> Definition of a strong password: A password that is difficult to detect by both humans and computer programs, effectively protecting data from unauthorized access. A strong password consists of at least six characters (and the more characters, the stronger the password) that are a combination of letters, numbers and symbols (@, #, \$, %, etc.) if allowed. Passwords are typically case-sensitive, so a strong password contains letters in both uppercase and lowercase. Strong passwords also do not contain words that can be found in a dictionary or parts of the user’s own name. (Source: [webopedia.com](http://webopedia.com))

<sup>2</sup> Most analysts report that password reset costs companies an average of \$51 (best case) to \$147 (worst case) per incident.

## 4 Fingerprint Authentication – Security with Convenience

One means of authenticating a user is by challenging them to provide information unique to them as an individual. UPEK biometric fingerprint solutions provide a means to securely and uniquely identify a user. Users initially enroll themselves in the fingerprint device. This process involves having the user create samples of their fingerprints through the fingerprint enrollment tutorial. The fingerprint hardware in turn creates a mathematical representation of the fingerprint that is stored and can later be used to authenticate the user to preserve their privacy. Any existing infrastructure and authentication methods can remain in place. Users can have any number of strong passwords without the need to remember them or write them down, solving both security and convenience issues. The fingerprint device can automatically authenticate the user to the computer system, network or application and securely provide the user's credentials. Finally the issues of improved security without impacting the user are solved!

## 5 Data Encryption – Protecting sensitive information

Security of data on computers is also of concern and has received public attention through many recent high profile cases where notebook computers that contained employee or customer information have been lost or stolen. Everyone today needs to be concerned with identity theft and the potential risks that create exposure. Protecting sensitive user, corporate and customer information has become mandatory through the adoption of many new laws and regulations including HIPPA, Sarbanes-Oxley, Gramm-Leach-Bliley and California 1386. Encrypting data provides a means to securely protect this sensitive information and make it inaccessible in the event that the computer falls into the wrong hands. Encryption involves having a passphrase or key to open the encrypted information. In the same way that fingerprint biometrics can protect access to computers and applications; it can also be used as the key to protect sensitive information, ensuring that access to sensitive files can only be accessed by an authorized user.

## 6 Protector Suite QL – a complete security solution

UPEK's Protector Suite QL provides a complete, integrated fingerprint security solution – protecting Windows logon, application & website logon and sensitive information on notebook and desktop computers. Used in combination with a fingerprint sensor built into a notebook computer or an external peripheral, Protector Suite QL provides convenient access to a strong authentication technique with just the swipe of a finger.

Protector Suite QL is intuitively easy and convenient to use and can be managed by end users or IT staffs with minimal setup costs. Protector Suite QL protects and secures the user's computer and data by requiring a finger swipe to logon to the computer. This enhances traditional password-based authentication. Once logged on, Protector Suite QL's "always-on" convenience features allow users to automatically and securely login to websites, encrypt & decrypt sensitive files & folders, navigate (scroll) through windows and launch applications with just the swipe of their fingers.

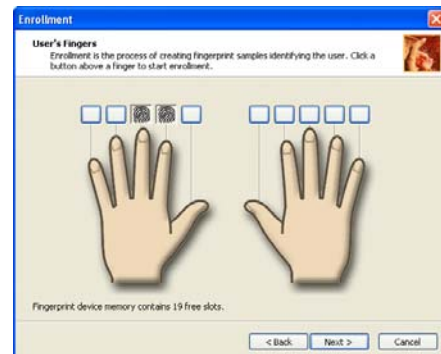
Protector Suite QL is a proven solution and ships with industry-leading biometric-enabled notebook computers from Sony, Toshiba, Panasonic, Acer, Asus, and others. A Lenovo Thinkvantage-branded version of PS QL ships on Lenovo Thinpad notebooks for enrollment

& windows logon.

This section highlights the key features and benefits of Protector Suite QL.

## 6.1 Self-guided Enrollment

To assist in the enrollment process, Protector Suite QL provides a self-guided fingerprint enrollment wizard that teaches the user the correct swiping technique to use the fingerprint sensor and enrolls the user's fingerprints. Successful enrollment is key to a successful user experience, and Protector Suite QL provides an intuitive interface that allows users to enroll themselves. During enrollment, users supply their Windows password. This password is encrypted and stored so that it can be replayed during logon and unlock of Windows.



## 6.2 An "always-on" user experience

Once enrolled, users have immediate access to the features and benefits of Protector Suite QL. In this way, the fingerprint sensor operates in the same way any other connected device does. By simply swiping a finger over the fingerprint sensor Protector Suite QL will authenticate the fingerprint (or provide feedback on the failure to match) and display the biomenu. This pop-up menu provides access to the key functionality of Protector Suite QL so users can use the convenient and powerful features without having to launch an application to access them.



## 6.3 Security

Protector Suite QL provides security on multiple levels, protecting your computer and applications from unauthorized access.

### 6.3.1 Boot Security

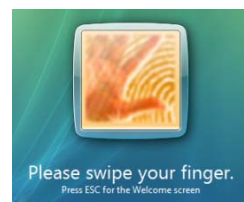
On UPEK fingerprint-enabled notebook computers, Protector Suite QL can provide "boot" level protection, requiring the user to authenticate their fingerprint before the Windows operating system boots. This hardware-level security protects notebook computers that are lost or stolen. Without an authorized fingerprint, the computer system cannot be accessed. For convenience, a single sign-on option can also be activated, allowing the user to automatically log onto Windows after successful authentication at pre-boot, without an additional swipe at the Window logon prompt.

### 6.3.2 Windows Logon Security

Protector Suite QL, works seamlessly with Windows logon to replace the normal username/password prompt with a finger swipe. On successful authentication, Protector Suite QL will automatically replay the Windows logon username & password for the user. This secure, convenient feature, allows users to select strong passwords without the need to

remember them. Password changes (as may be required by IT organizations) are automatically re-captured by Protector Suite QL without any user intervention making Windows logon both secure and convenient for the user. Protector Suite QL works with the conventional Windows logon interface in Windows 2000, 2003 & XP (Windows GINA) as well as the new logon interface of Windows Vista (Windows Vista Credential Provider).

The logon interface can be selected to enable fingerprint or password logon (default), fingerprint-only logon, or disable fingerprint logon.

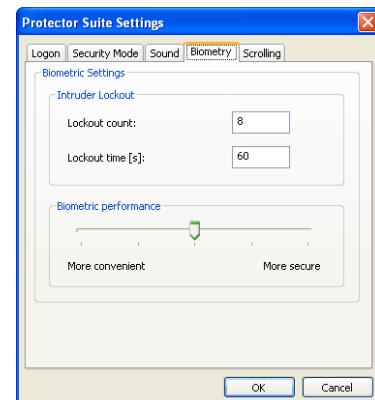


### 6.3.3 Windows Lock Security

Users can easily lock their computer through the biomenue option. Once the computer is locked, it can also be unlocked by the user by simply swiping their finger. Once re-authenticated, Protector Suite QL automatically provides their password to Windows to unlock the computer.

### 6.3.4 Intruder Lockout

Protector Suite QL is pre-configured to provide intruder lockout. Intruder lockout locks the fingerprint sensor for a period of time if a finger is rejected a number of times – protecting the computer system from attempts to gain unauthorized access.



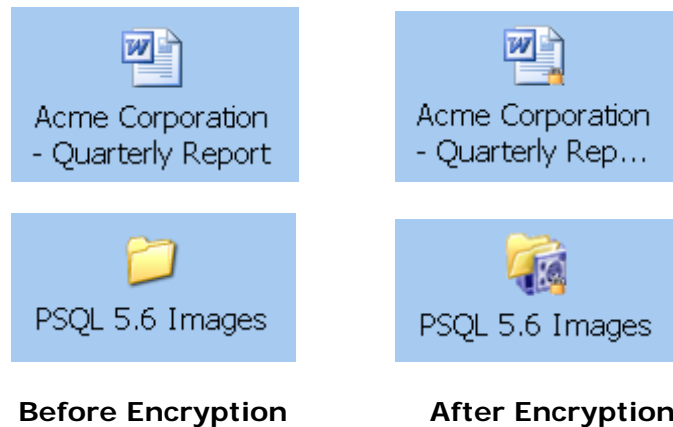
### 6.3.5 Integrated Password Bank

For application logon, Protector Suite QL provides an integrated Password Bank that securely registers user credentials and allows them to be replayed later after the user authenticates themselves with a finger swipe. The Password Bank works with Windows and website logins. Credential information is encrypted and can only be accessed with a successful authentication. The Password Bank provides convenient access to applications and secure websites allowing users to use strong passwords without the headache of managing and memorizing multiple passwords.

The Password Bank provides “tips” that helps new users discover the power of registering their credentials for later playback. Each username/password registration is stored and self-manageable by the user. Each user may create an unlimited number of registrations and for web-based applications, conveniently launch a new webpage and login automatically from the biomenue. Protector Suite QL supports browser choice – supporting both Internet Explorer and Firefox.

## 6.4 Encryption

To protect data security, Protector Suite QL provides file & folder encryption that is tied to a user's fingerprint. Users can select the file or folder (through the Windows user interface) that they wish to encrypt and then encrypt them with a swipe of a finger. Users may also provide access to other users in shared computer environments by adding them to the access control list for the encrypted file or folder. To access an encrypted file or folder, users are prompted to provide a valid fingerprint. Once a valid fingerprint is provided, the file or folder opens as it normally would.



## 6.5 Convenience Features

Protector Suite QL provides convenience features that allow the fingerprint sensor to be used for application launching, Windows account switching and window scrolling.

### 6.5.1 Finger-activated Application Launch

During enrollment, a user can enroll any number of fingers. Any of those fingers can be used to authenticate. In addition, users can associate specific fingers with applications. This allows the user to conveniently launch a commonly used application using a finger swipe.

### 6.5.2 Fast User Switching (Windows XP & Windows Vista)

Protector Suite QL supports fast user switching on Windows XP and Vista computers. This feature allows a user to log on (without logging another user off) by simply swiping their finger across the sensor. Instead of having to type CTRL-ALT-DEL and select the correct user and type in the password, the user simply swipes their finger. Protector Suite QL recognizes the new user and creates a new session using Windows XP & Vista's built-in multi-user capability.

### 6.5.3 Scrolling

Protector Suite QL supports window scrolling using the fingerprint sensor. Once invoked,

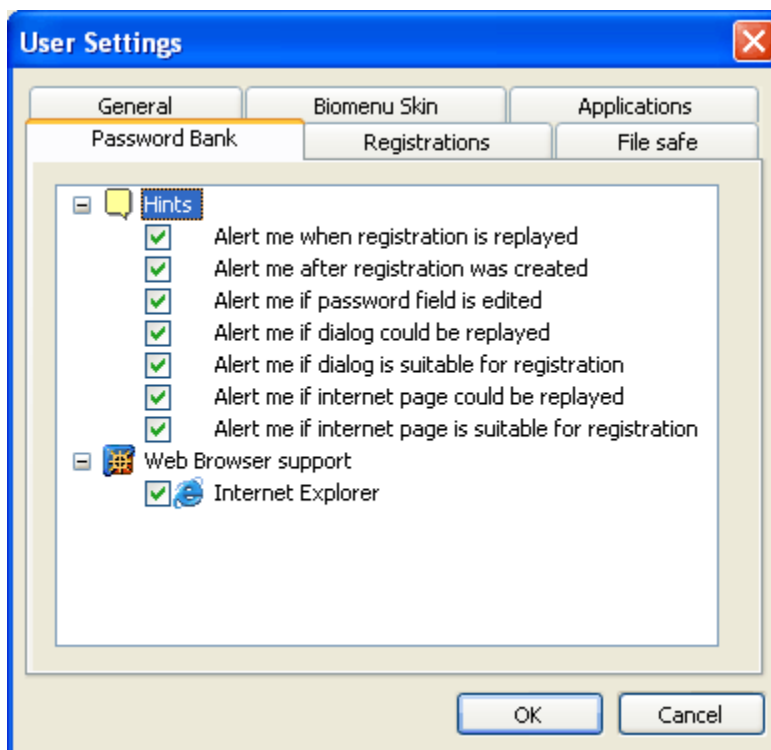
the user can conveniently scroll windows by sliding their finger up or down across the sensor.

## 6.6 Configuration Features

To provide a personalized experience, Protector Suite QL provides system-wide and individual user settings.

### 6.6.1 User

Protector Suite QL provides a number of personal configuration & management features including a number of "skins" that provide unique looks for the biomenue; file & folder encryption password setting; finger-activated launch settings; password registration settings and password bank hint settings. The user settings allow each user to manage and configure Protector Suite QL for a personalized experience.



### 6.6.2 System

To manage configuration items that apply to all users, Protector Suite QL provides a system setting dialog for management. System setting provide control on the type of allowed logon to Windows; default feedback sounds that are played; and intruder lockout options. In addition, Protector Suite QL supports policy-based management of user rights to make system level changes. Two types of users are supported – Fingerprint Administrators and Limited Users. This policy-based control gives administrators control over how users can

modify enrollment, fingerprint and power-on security settings.

Policy	Administrator	Limited User
Enrollment: Delete other users	No	No
Enrollment: Delete self	Yes	Yes
Enrollment: Edit other users	No	No
Enrollment: Edit self	Yes	Yes
Enrollment: Enroll other users	No	No
Enrollment: Enroll self	Yes	Yes
Enrollment: Enroll users without scanning fingerprints	No	No
Enrollment: Export other users	No	No
Enrollment: Export self	Yes	Yes
Enrollment: Import other users	No	No
Enrollment: Import self	Yes	Yes
Enrollment: Reveal password	Yes	Yes
Fingerprint Storage Inspector: Delete any fingerprints	No	No
Fingerprint Storage Inspector: Delete other users' fingerprints	No	No
Fingerprint Storage Inspector: Delete unused fingerprints	Yes	Yes
Fingerprint Storage Inspector: Use Fingerprint Storage Inspector	Yes	Yes
Power-on Security: Add fingerprints to Power-on security	Yes	Yes
Power-on Security: Enable\Disable Power-on security	Yes	Yes

## 7 Protector Suite QL – The solution to securely protect your computer

Protector Suite QL 5.6 provides users with an “always-on” biometric experience that allows them to securely and conveniently:

- **logon to their Windows computer;**
- **prevent intruders from unauthorized access;**
- **access websites and applications without having to type their credentials;**
- **encrypt sensitive files and folders on their hard drives;**
- **launch favorite applications;**
- **use the fingerprint sensor to scroll through windows.**

Protector Suite QL 5.6’s easy, self-guided enrollment and setup, allows users to quickly get

started for a rich user experience.