

AEGIS BIO FOR BUSINESS

Problem: Securing private information is critical for individuals and mandatory for business.



Mobile users need to protect their personal information from identity theft. Businesses are mandated by federal and state law to secure personal information stored in electronic format.

Securing mobile storage devices has become a primary concern for most companies. One such concern involves the implication of losing a portable hard drive containing sensitive or personal customer information. Compliance legislation like Sarbanes-Oxley and other state legislation of personal information mandates the security of mobile devices must be considered when developing compliance strategies.

Compliance and portable drives
California's SB 1386 mandates the notification of California residents in the event of unauthorized acquisition of their "personal information" that is stored in an electronic format. Personal information includes the first and last name and either a social security number; drivers license number, account number, credit or debit card number, along with the security codes, passwords or access codes that would allow access to an individual's account. Fortunately, California's SB 1386 has made allowances when this sensitive data has been encrypted; this includes data on mobile devices like the Aegis Bio. If users are issued an Aegis Bio for storing sensitive or personal customer data and the drive is lost or stolen, reporting the security breach is not required.

Compliance and networks

The exposure of personal information is not limited to portable devices. Corporate networks are also at risk of unauthorized access to this information, as long as passwords are inadequately protected. Weak password protection increases the risk of organizations suffering damage to their reputation and financial losses. When a breach of security occurs, consumers will ultimately lose confidence in the company. Enterprises are faced with a multitude of attacks and must make funding decisions on how best to increase their security infrastructure. Therefore, security products like the Aegis Bio that biometrically protect access to and encrypt data on portable drive as well as perform double duty as a biometric access point and password bank should be considered when making budget decisions.

Individuals protecting personal data

Key logger programs are more of an issue for individual users than corporate IT departments that are diligent about spyware and virus protection. These programs can be easily downloaded when visiting a website without the user even knowing it happened. Once the program hides itself in a root kit, it starts to capture the information from the keyboard as an on-line form is filled out. Key logger programs have been used very successfully by identity thieves.



© 2007 Apricorn, Inc.
All rights reserved.
Produced in the United States

Apricorn, Inc.
12191 Kirkham Road
Poway, CA 92064
1-800-458-5448

SOLUTIONS FOR SECURING DATA ON PORTABLE HARD DRIVES



Biometrics

What is biometrics?

Biometrics is a general term used alternatively to describe a characteristic or a process. As a characteristic: Biometrics is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. As a process: biometrics is described as automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics. (from the National Science and Technology Council's NSTC glossary of biometric terms)

There are many biometric methods and processes including: hand geometry, face and voice recognition, fingerprint, iris and retinal scans. But the biometrics method that offers the most promise in terms of available mature technology and affordability is fingerprint scanning.

Types of fingerprint sensors

Fingerprint scanners have used a wide variety of technologies including: optical imaging, ultrasonics, infrared gauging, mechanical force, temperature, and electrical capacitance. These methods rely on detecting patterns on the surface of the finger and converting those patterns into electrical signals. The most promising of the technologies utilize 3D sensing techniques to measure biological samples "live" skin layers to work with all fingerprint types and under all environmental conditions.

How reliable is fingerprint scanning technology?

Fingerprint technology has been around for over 100 years as a way to identify people because no two fingerprints are the same. Fingerprint recognition is by far the most mature of all the biometric technologies available. With the advances in sensor technology like 3D sensing techniques, fingerprint technology is the most convenient, reliable and cost effective form of biometric identification on the market today.

Encryption Types of Encryption

There are many types of encryption and many good resources with a complete explanation of the history of cryptography. This article examines why one type of encryption may be considered over another with respect to securing portable hard drives. If the primary objective is to have a solution that is seamless, readily adopted by users and meet the mandated encryption requirements then 128 Advanced Encryption Standard (AES) is the best choice. According to the Committee on National Security Systems (CNSS) Policy Number 15, Fact Sheet Number 1; "The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths."

As well, 128 AES is sufficient for all of local, national and International mandates for protection of personal information. Even though 192 and 256 key lengths offer better protection, the time it would take to encrypt the data creates a solution that is not transparent, easy to use or fast.

WHY CHOOSE THE SECURITY OF AEGIS BIO?



1) Access to the Aegis Bio is protected via a fingerprint biometric sensor. Once registered, just swipe a finger on the sensor for access to the files. Up to ten finger print profiles can be stored and can be accessed without software on the host system.

2) The Aegis Bio's encrypted hard drive seamlessly encrypts data in real-time with 128-bit AES encryption. The data on the drive remains impenetrable, even if removed from its enclosure, ensuring the utmost in protection for even the most sensitive files.

3) With the Aegis Bio's Windows Logon feature and Password Bank, users forgetting complicated passwords and having them reset will be reduced sharply. Writing down passwords on Post-it notes and sticking them to a monitor will all be a thing of the past. Now users can access their computer or logon to the network with a swipe of the finger.

specially formulated coating to provide optimum durability and robustness.

Superior fingerprint image quality

The Aegis Bio scans a larger fingerprint area to produce a better minutiae-based algorithm and providing the best biometric performance. The minutia is the area of the finger print where the fingerprint ridges either end or split in two. The actual fingerprint is not captured, but by scanning a larger area more minutiae points can be captured, mapped and saved as a mathematical representation of fingerprint. The resulting information is saved as a template and stored in a secured location on Aegis Bio. When a finger is swiped across the scanner for access to the drive, the information is compared to the template for verification.

Aegis Biometrics

Aegis Bio's fingerprint sensor technology

The Aegis Bio sensors offers UPEK's 3D Sensing technology (composed of 3-dimensional sensing techniques), which measures at the finger surface and into the "live" skin layers to work with all fingerprint types and under all environmental conditions. This eliminates the possibility of defeating the biometrics with photo copied fingerprints. Additionally, the sensor is protected by a

AEGIS BIO

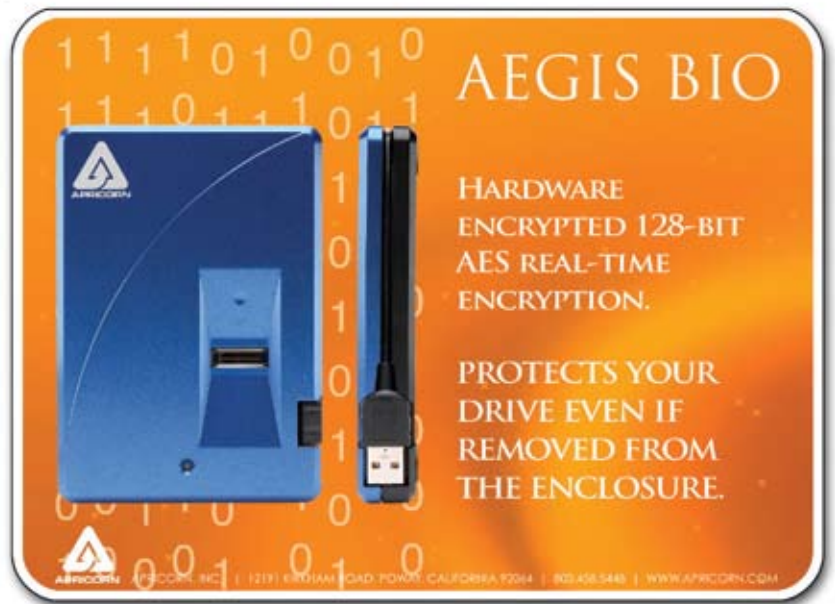
YOUR FINGERPRINT IS NOT STORED.

THE BIOMETRIC SENSOR MATCHES YOU TO YOUR SPECIFIC FINGERPRINT PROFILE

APRICORN | APRICORN, INC. | 12191 KIRKHAM ROAD, POWAY, CALIFORNIA 92064 | 800.458.3448 | WWW.APRICORN.COM

WHY USE HARDWARE ENCRYPTION?

Software solutions for hard drives have been available for some time now. They have often been criticized for being inconvenient, slow and like any other software, prone to needing updates.



Aegis Bio Hardware Encryption

The Aegis Bio offers 128 bit AES real-time encryption of the data as it moves on to the hard drive. It also creates a secure “Trusted Path” between the Aegis Bio and host computer that protects usernames, passwords and fingerprint template information from being intercepted by key loggers or similar spyware program. An additional security feature includes the way the Aegis Bio is recognized by the operating system. Once the USB cable is connected, the operating system sees the Aegis Bio as a removable device in ‘media not present’ state, so accessing the drive is not even possible. After fingerprint recognition is completed the device is unlocked and the operating system invokes a ‘media inserted’ event. Complete security is ensured with the data stored in 128 AES encryption; even if the drive is removed the data will be completely inaccessible.

This reduces the amount of time spent scrubbing the drive or erasing disk data, which in turn stretches the IT department budgets when redeployment of assets is necessary.

Passwords security and compliance

As pointed out in the problem section of the white paper, the exposure of personal information through inadequately protected passwords are a real threat to the corporate network. The solution is not to make the policies stricter, but rather use a safer system that is seamless for the user. The safest passwords are complex and hard to remember and simple or common passwords are easy to remember and far too easy for the determined hacker to crack. Using fingerprint access instead of a password for securing network logon is easy to use and if properly implemented, will fulfill the mandates that the compliance regulations demand.

Hardware Encryption vs. Software Encryption

Software solutions for hard drives have been available for some time now. They have often been criticized for being inconvenient, slow and like any other software, prone to needing updates. Hardware encryption is relatively new on the market but is very reliable, fast and convenient. Since hardware encrypted drives are not subject to updates, the costs related to traditional software solutions are eliminated. Another great advantage of hardware encrypted drives, they can be easily reset.

PS TOKEN™ SOFTWARE WITH PASSWORD BANK



PStoken™ Software

The PStoken software is the heart of the biometric system and the enrollment wizard makes this one of the most convenient biometric drives on the market today. There are many facets to the operation of the PStoken software including a complete installation on the host system. PStoken software can be used without installing on the host system and still enjoy all the functionality of the device. Once fingerprints have been enrolled on the Aegis Bio, it can be used on any operating system without additional software, just by plugging it in and swiping a finger. Then there are group of advanced and administration features that allows users to reset, reformat and change the backup password. Administrators can setup a backup password on the device before it is issued to a user, ensuring that the IT staff will always have access to the drive.

Fingerprint enrollment

The initial setup includes the enrollment wizard that takes the user through the fingerprint tutorial. The easy to follow step by step instructions include complete directions for swiping, a demonstration video and plenty of scanning practice. The wizard provides graphical feedback during verification process, eliminating the guess work and confirming that a good quality scan was made of the fingerprints. The fingerprint tutorial can be run anytime from the Protector Suite Token program menu that is accessible by clicking on the icon sitting the system tray.

Backup password enrollment

After fingerprint enrollment is completed the wizard continues with the Security Setup. The Aegis Bio is protected by a fingerprint, but in the event that fingerprint authentication is not possible, a backup password can be used to access the data. During the Security Setup, a password is entered and saved to a backup password file. The backup password file is not stored on the Aegis Bio but kept on the host computer or some other location that is easily accessible. The actual password is not stored in the file but rather the information needed to generate encryption from the password entered is stored in the backup password file. The backup password file and knowledge of the password are both required to unlock the Aegis Bio without the enrolled fingerprints.

Formatting the Aegis Bio

Formatting the Aegis Bio in FAT32 is the final step of the initial setup process. FAT32 offers the most compatibility with other operating systems and the Aegis Formatter formats the entire capacity of the hard drive and is not limited by Windows 32GB maximum hard drive partition size. During the format process the volume label can be personalized to make it more users friendly.

Password Bank and Windows Logon

The PStoken software includes a password bank and Windows Logon feature. This allows the Aegis Bio to act as a biometric access device as well as a secure storage facility for usernames and passwords. Instead of typing a username and password every time they are requested, simply swipe a finger and



ONCE REGISTERED THE AEGIS BIO CAN BE USED ON ANY COMPUTER NO SOFTWARE REQUIRED

they are entered automatically. They are sent via a secure channel between the Aegis Bio and the computer making it a completely secure transfer of information. A secure channel is the ultimate defense against a key logger attack where personal information is stolen without the user's knowledge. The password bank integrates with Internet Explorer, Firefox and Windows applications and it even prompts the user when a compatible form is available for registration. Once a website or application is registered, it can be launched from the system tray icon.

Logon Protector

It is not necessary to compromise network security because of weak and inadequately protected passwords. When IT departments implement strong password protection, they end up having to reset the more complicated passwords when they are forgotten. Offering a biometric solution for Windows logon can reduce the overall cost of IT departments and even supplement the cost of the device. Users are more likely to use secure passwords if they don't have to remember them. This solution is easy to use and it seamlessly integrates with the Windows logon screen. Both Fast User switching and domain logon are supported. The Logon feature is only available when installed on the host system, through the custom setup option.

Using the Aegis Bio on any computer
The PStoken software is not needed to operate the Aegis Bio on another computer. The Aegis Bio is

equipped with a self contained biometrics verification system, which works with any operating system. Once fingerprints are enrolled, take the Aegis Bio to any computer with a USB port and swipe a finger to unlock the drive. There is a red LED on the front of the Aegis Bio that starts flashing when a finger is swiped. Once the fingerprint has been accepted the LED turns green and the drive is unlocked.

PST Administration Tool

For corporate implementations, The PST administration tool allows the administrator to install a backup password and create an encrypted "Backup Password File" that ties it to each Aegis Bio's unique serial number. With knowledge of the password and the "Backup Password File", the administrator will always be able to unlock the Aegis Bio. When an end-user receives an Aegis Bio with the backup password installed by the administrator, the end-user will not be able to remove or change the backup password.

Password Unlock Tool

The password unlock tool is a stand alone program that allows device unlocking when fingerprint is not available. When an end-user receives an Aegis Bio with the backup password installed by the administrator, the end-user will not be able use this tool.

Device Reset Tool

This tool allows complete device reset (incl. user data) when both fingerprints and password are lost or redeployment is required. The reset tool is a valu-

able resource when IT managers are required to erase hard drives before redeployment. Once the Aegis Bio has been reset it is not necessary to use a hard drive cleaner or scrubber. Reset will delete all files and formatting from the device. No password is necessary. This will leave the hard drive in a preformatted state and it will be necessary to go through the initial enrollment process and format the hard drive. All data on the device will be lost and cannot be retrieved.

Supported Operating Systems

The PStoken software may be installed on Windows 2000, XP and Vista. As explained earlier in the white paper, the Aegis Bio can be also unlocked and accessed on all non-Windows operating systems with USB through built-in standalone verification.

Conclusion

The Aegis Bio offers a complete security solution that not only meets the needs of corporations that are obligated to secure their clients private information but also offers some unique features that will help protect users from identity theft.

The Aegis Bio's first line of defense is the biometric access to the hard drive. Upek's 3D sensing technology is used to capture the best sample possible of the fingerprint. Using minutia points, a template is created and stored to use later for comparison and authentication to the device.

The Aegis Bio will be adopted by users because it is fast, with 128bit AES real-time encryption, they will not have to give up any performance or worry about exposure to the data should it become lost or stolen. Even if the drive is removed from the enclosure the encryption would render the data inaccessible.

The PStoken software makes it easy to setup and use the device with its instructional videos and step by step wizards. The Aegis Bio creates a secure channel for usernames and passwords to move back and forth between the drive and the host computer and then stores them in a password bank where they can be launched for safe easy access to online forms and websites.

The Windows logon features allow users and organizations concerned about securing their computers and networks, to implement strong password protection policies. No longer will network administrators have to deal with users forgetting complicated passwords or writing them down on post-it notes that are stuck to their monitors. Once the password has been initially entered, the user only needs to swipe his or her finger to gain access to the computer or network.

All of these features are available in an attractive blue enclosure with an integrated USB cable that provides all the power necessary and eliminating the need to carry bulky AC power adapters. The Aegis Bio has a unique 16 point omni-directional shock mount system to secure the hard drive from accidental drops and bumps, making this the most secure drive on the market today.

*Whitepaper written by
David Sexton, Corporate Sales Manager
To request an evaluation unit please call
Direct: (858) 513-4431
Email: dsexton@apricorn.com
www.apricorn.com*

© 2007 Apricorn, Inc.
All rights reserved.
Produced in the United States

Product information provided is for information purposes only and does not constitute a warranty. Information is true as of the date of publication and is subject to change. Actual results may vary. This publication is for general guidance only. Photographs may show design models.

Apricorn, Inc.
12191 Kirkham Road
Poway, CA 92064
1-800-458-5448

