A biometric access personal optical storage device

David Davies

A miniature optical storage disc drive features highly secure encrypted data recording and employs biometrics to control access.

There is a need for personal data storage technology that offers portability, archival content retention, data security, and a high level of confidentiality while preserving ease of access and low cost. Potential uses include personal portable electronic records, individual financial information, health records, PC data backup, and digital picture storage. The critical advantage is that, should the media be lost or stolen, it is virtually unreadable.

The DataPlay small form factor storage media and drive offers a 32mm optical recordable media and an optical drive (read and write) with dimensions less than $50 \times 50 \times 11$mm. Although described previously,\textsuperscript{1,2} it has now been combined and newly implemented with DataPlay’s PassPlay digital password protection scheme,\textsuperscript{3} permitting content security and media interchangeability through storage of encrypted passwords on the media itself. These alone permit decryption of content. In this new application the small form factor optical engine is embedded in a stand-alone USB 2.0-based system, which includes an integrated biometric scanner.

Initial devices use fingerprint biometrics as passwords, but other biometrics, such as retinal scan, are possible. The disc can be removed together with the digital templates defining the biometric image stored on the media in secure encrypted form. Provided the image is validated, the media is thus interchangeable and can be removed from the system for use in other devices. Data security is the primary attribute of this device, achieved through use of trusted sources and secure validation before the biometric-based password can be accessed.

**System description**

The DataPlay engine is configured with a Cypress FX2 USB 2 IC interfaced to a UPEK scanner and encoding electronics. The imaged fingerprint is processed to biometric templates derived from minutiae consisting of digitized data abstracted from the image by a defined protocol. These are saved on the disc for comparison with the current biometric scan. A typed password can be used in place of the fingerprint.

**System attributes**

Passwords can coexist with biometric access, and both require PC application software to manage security features such as adding and deleting a password or biometric template. However, after a biometric has been used to initialize a PassPlay, disk access can then only be granted by a valid biometric.

DataPlay’s implementation saves the biometric template to the disk so that access is tied to the disk, not the device. This is a requirement for removable media that supports true interchange.

The biometric templates encrypted by the engine are stored in a secure location on the disk. They can only be accessed by an authorized host after creation of an authenticated channel, which depends on a successful match. The host is granted access to a password key that is unique for every disk, not based upon the biometric templates. The password key is securely sent to
Figure 2. The USB storage device with integrated scanner.

the engine over the authenticated channel to perform a PassPlay 'log-on,' enabling user access.

One additional important security feature is that the biometric password key is not the encryption key. This means that the actual encryption key is never transferred over the host interface.

**USB biometric access personal storage device**

Our device essentially combines the features of miniature optical storage devices with a high level of multiple (TDES/AES) encryption into a compact reader/writer that needs no battery and is driven off power from the USB 2.0 port alone. The readily available media has proven archival properties. For the device as shown in Figure 2, the data rate is 1MB/s and the R/ROM media capacity holds up to 0.5GB. These concepts are also being applied to DVD and HD DVD formats, following Trusted Computing Group standards.

**Author Information**

David Davies  
DPHI, Inc./Dataplay  
Longmont, CO  
http://www.dataplay.com

Dave Davies is chief technology officer and cofounder of DPHI/DataPlay, Inc. He worked several years at 3M’s Optical Storage Division and held VP positions at Ampex and the pioneer holographic storage firm Siros. For his work in helping establish the CD ROM standard, he was made a SPIE Fellow.

**References**