SONY

White Paper 04-01

Revision History

1.0	9 February 2004	Initial Draft.
1.1	13 April 2004	Added info about private area and system area encryption.
1.2	10 May 2004	Corrected info about fingerprint storage, system area size, and 3DES key generation.

FIU-810 PUPPY® FINGERPRINT IDENTITY TOKEN: TECHNICAL ARCHITECTURE OVERVIEW

By John Harris, Marketing Manager, Biometrics

The Sony® FIU-810 Puppy® Fingerprint Identity Token is the latest in Sony's line of biometric products for the enterprise market. Featuring on-board fingerprint scanning, matching, and storage; on-board digital certificate / cryptographic capabilities, and 64MB of file storage; the FIU-810 device is a portable, USB-based token ideal for identity management and secure communications applications.

This document will explain in detail the specifications and internal operation of the unit as it pertains to fingerprint authentication and storage; digital certificate / PKI functions; and file storage.

Background

Sony's fingerprint token strategy revolves around the combination of multiple, on-board strong authentication mechanisms and standards-based cryptography, thus providing a full complement of technologies for security, authentication, non-repudiation, and data integrity. In this model, each fingerprint token is designed to be used by one user, like other smart cards and tokens.

FIU-710 Features
- On-board fingerprint scanning, matching and storage / capacitive Si fingerprint sensor
- Up to 1024-bit RSA key generation, x.509 digital certificate compatibility
- 512KB available memory for storage of fingerprint templates, keys, digital certificates
- Card-shaped form factor
- USB interface

The Sony FIU-710 token, released in April 2000, was the first product to achieve these goals. It was also the first device on the market to combine the capability to match users' fingerprints on-board the device while also using those fingerprints to grant access to private key operations using the public and private keys and digital certificates stored on the device.

Through 2002, work proceeded on the FIU-900, a Memory Stick® media-based fingerprint token that improved on the capabilities of the FIU-710, while also significantly reducing its footprint and increasing the integration of the chipset on-board the device.

FIU-900 Features
- On-board fingerprint scanning, matching and storage / capacitive Si fingerprint sensor
- Up to 2048-bit RSA key generation, x.509 digital certificate compatibility
- 512KB available memory for storage of fingerprint templates, keys, digital certificates
- Memory Stick media form factor

In the years since the introduction of the FIU-710, USB-based flash memory devices became increasingly ubiquitous, inexpensive, and popular. Yet, with rising capacities came concerns over security. If a user could store larger files on-board, it was more likely that users would place business-critical files on the device and travel with their flash drives, leaving their laptops behind. Additionally, in these years, USB authentication tokens continued to penetrate the market.

In late 2002, Sony began work on the FIU-810 Fingerprint Identity Token. The device features the high-end strong authentication and cryptographic features of the FIU-900, but is a USB-token shaped device that also carries flash memory in quantity sufficient for general file storage. Architectural changes were made to better highlight the encryption and signing features of the device and improve on the user & developer friendliness of the device.

High Level Architecture

The FIU-810 Puppy® Fingerprint Identity Token is built around three interwoven, but distinct capabilities:

- Fingerprint authentication
- Digital certificate functions (PKI)
- USB Mass Storage-based secure file storage / transport

(For reference, a block diagram of the FIU-810 unit's circuitry can be found on page 6.)

Fingerprint Authentication. The silicon sensor located at one end of the FIU-810 device manages fingerprint imaging. This sensor is designed by Sony's Semiconductor group, and is an improved version of the sensing chip used in Sony's FIU-710 Fingerprint Identity Token.

A DC capacitance method is used to image the fingerprint. The capacitance of the fingerprint surface is measured pixel-by-pixel, and the electrical charge present varies with the distance from the surface of the sensor to the surface of the skin. The sensing element is 192 x 128 pixels in dimension, with an approximate 320 pixel per inch resolution (80 micron pixels). The image that is produced is in 8-bit grayscale (256 levels of gray) and, if it could be viewed in raw form, would look nearly identical to (if not better than) an optical- or ink-based representation of the fingerprint.[1]

Finger detection occurs in hardware, based on the proper placement of the finger on the sensor's surface. Once detected, imaging begins, and the device captures an image of the fingerprint. This image is then routed into the 32-bit ARM7 for processing. In this pre-processing phase, the image is cleaned up and converted into a monochrome image to better allow for feature detection and pattern analysis. The original image is discarded.

The pre-processed data is then sent to the fingerprint verification core. Sony's proprietary fingerprint algorithm is based on pattern matching and correlation, rather than a minutia-based system. Our method is particularly effective, and has its own merits:

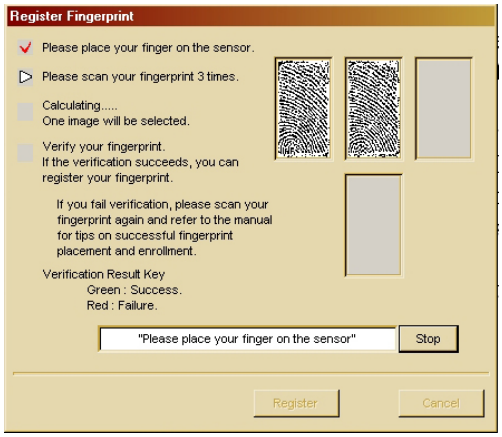
- More efficient for device-based fingerprint matching
- Small processing overhead
- Leverages Sony experience in pattern correlation techniques used for MPEG and other types of AV data compression

During fingerprint enrollment, the pre-processed data is sent to the fingerprint verification core for further processing and transformation into a template for storage and later use. During fingerprint matching, the pre-processed data is compared in the fingerprint verification core with a previously stored template.

This second phase of data processing commences with the division of the monochrome image data into a pre-defined number of segments. These segments are then analyzed in order to determine the sectors with the most differentiated data. These sectors are then selected and the patterns in each are stored to a template (for enrollment) *or* stored to SRAM for comparison with a template pulled from the FIU-810's flash memory (for matching). The manner in which the patterns are searched and stored is a proprietary technique.[2]

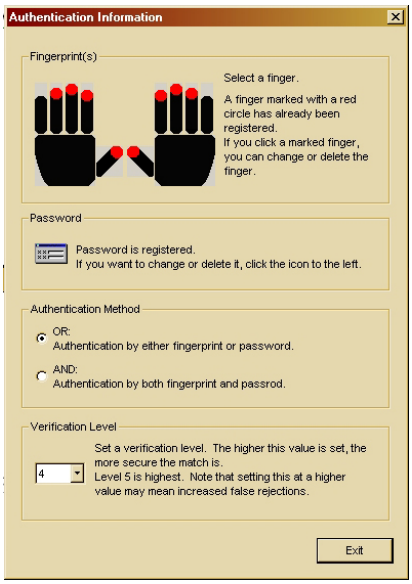
[1] Note that grayscale images (BMP) of the fingerprint are not exportable from the FIU-810 unit, and cannot be accessed via the API. All processing occurs on-board the device.
[2] For more information, ref. European patent EP0833274 A2.

During enrollment, a 'round robin' method is used to increase the quality of enrolled fingerprints. The user is prompted three times to place a specific finger on the sensor. The unit then stores these three temporary monochrome images and matches them against one another to determine the one with the best matching score. After one more finger placement to verify that the selected image is good, the template is generated and stored in flash memory, alongside keys, certificates, and other previously enrolled fingerprints.[3]



In matching, the monochrome data stored in SRAM is compared successively to each template stored in flash, until (1) a match is made or (2) no match is made with any template in memory. In the FIU-810 token, a 1:few match process is performed—the live print is matched against all templates in storage. A user does not need to specify which finger they are using, as was required by previous generations of Sony's fingerprint devices.

A successful match is based on a correlation of the data and a template that meets or exceeds the threshold set by the application or the device firmware. If this correlation succeeds, the device reports a match and permits an operation to proceed. Each matching operation (live image vs. template) takes approximately 100ms.



Sony's threshold system has five levels, one being the least secure (albeit with a low false rejection rate-FRR) and five providing the most security (a very low false acceptance rate-FAR, but a moderately higher FRR). At a level four threshold setting, Sony has measured a <0.001% FAR and a <1% FRR. The administrator or user of the device sets the threshold setting, but Sony recommends that no less than a setting of three is used regularly. Moreover, a setting of four or higher is required to maintain FIPS 140-2 Level 2 compliance.

Fingerprint templates are stored, encrypted in the 32KB of EEPROM located within the security/fingerprint LSI (see block diagram at the end of this document). Each template is 576 bytes in size, and up to 10 fingerprints can be stored, 1 per finger. The device is intended for use by only one user, so this limit is not restrictive.

Fingerprint management is handled by 'User Manager,' a software application which is carried on-board the public drive of the FIU-810 device. With this application, new fingerprints can be enrolled, existing fingerprints can be changed or deleted, and the authentication method changed.

Digital Certificate Functions (PKI). Public and private key operations are managed by the RSA engine within the central ASIC of the FIU-810 unit. This engine supports RSA key pair generation (up to 2048-bit), encryption, and digital signatures. This core is based not on a smart card processor, but rather on a Sony component featuring similar capabilities.

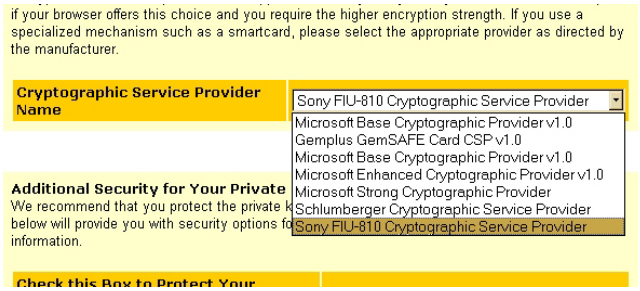
Industry standards are critical to the unit's compatibility with off-the-shelf software, and are followed throughout its architecture:

[3] Note that template data is stored, encrypted, in the 32KB EEPROM located within the Security/FP LSI.

- Public and private keys are generated using the RSA algorithm (512, 1024, 2048 bit)
- x.509v3 digital certificates supported
- Compatible with the most popular Certificate Authorities, including RSA®, Microsoft® Windows® CA, and Verisign®[4]
- Support for the PKCS #11v2.1 interface as well as PKCS#12 file import functions
- Support for Microsoft's CryptoAPI (CAPI) via dedicated FIU-810 CSP
- 3DES & DES encryption

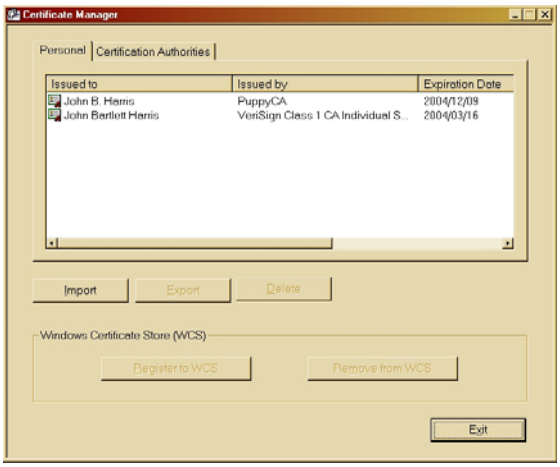
With this standards-based approach, the FIU-810 device can be used with off-the-shelf software and applications as long as the software supports PKCS#11 or CAPI. Once keys are generated and certificates received, the FIU-810 unit can be used directly in a wide variety of applications, including:

- Digital signatures / workflow improvement: Adobe® Acrobat®, Microsoft Office, Silanis ApproveIt®
- Secure e-mail clients: Outlook®, Outlook Express
- SSL 2.0 Authentication: Internet Explorer
- VPN: Cisco® & Nortel VPN clients
- Remote Access: Secure Computing SafeWord® Premier Access
- File encryption and security



The device operates in most respects like other PKI tokens or smart cards in that the device can generate a RSA key pair on-board the device itself, submitting the public key for signing by the certificate authority, or alternatively importing a previously generated key pair via PKCS#12.

Key pairs and certificates are stored on-board the device within the secure 2MB flash allocation. Private key operations can only proceed after a successful authentication by the user, typically by fingerprint, though passwords may also be implemented, depending on the application.



The FIU-810 token's PKCS#11 library and CSP need to be installed on the host machine to enable use of the token for cryptographic functions. Once installed, these libraries need to be specified within the application / browser being used for key generation to be sure that the FIU-810 device is selected for key generation.

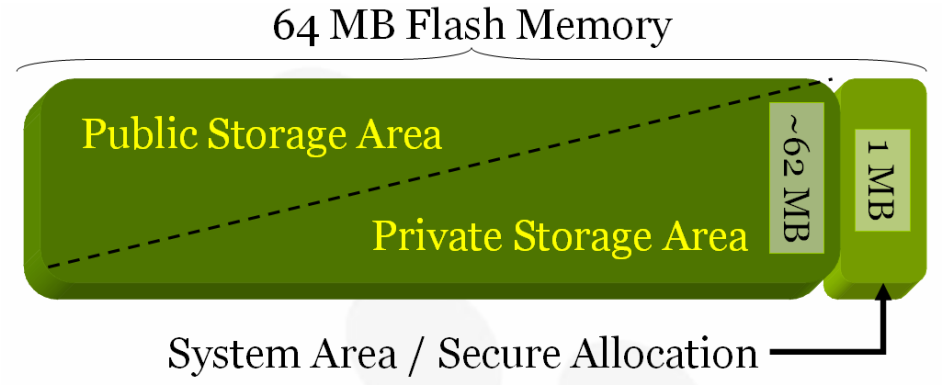
During key generation, user authentication is required. RSA 2048-bit key generation takes approximately 20-60 seconds.

A software application included with the FIU-810 unit, 'Certificate Manager,' allows a user to manage his or her digital certificates, import keys via PKCS#12, export keys, and populate certificates into the host computer's Windows Certificate Store (WCS) for use by Windows CAPI. This is

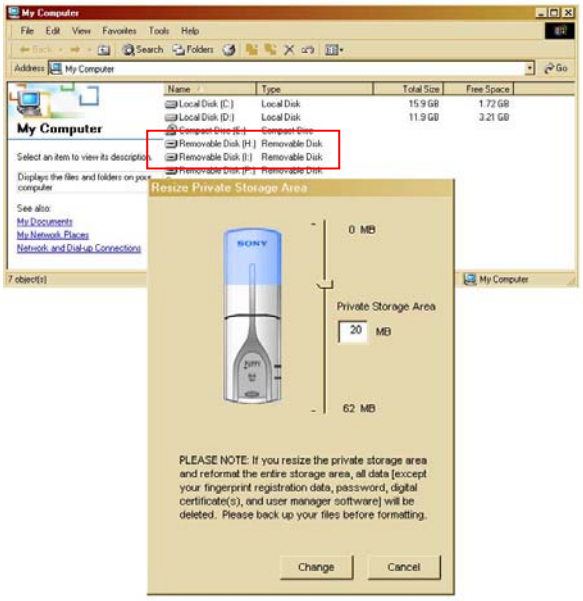
[4] Entrust certificate compatibility expected Q204.

not necessary if the certificates were generated via CAPI while the FIU-810 token was plugged into the host machine.

USB Mass Storage-based secure file storage / transport. In order to promote the highest level of compatibility, all communications with the FIU-810 unit are handled via native USB Mass Storage Class drivers. Therefore, no special driver install is required, and users won't need to carry an extra CD with them when they use it on a new computer. The FIU-810 unit's flash memory is allocated into three specific areas, as defined below.



The FIU-810 device, when plugged into a PC, displays two separate drives. One is the public storage area, which is accessible to any user, and the other is the private storage area, which is accessible only to the owner of the FIU-810 token after a successful authentication attempt. The amount of flash memory allocated to the private storage area is up to the user, and can be managed via an interface within the User Manager software.[5] The FIU-810 device is set at the factory with all memory allocated to the public space. The user (or administrator) must set up the private storage area upon receipt.



The private storage & system areas are encrypted via a 3DES key that is generated when a user is created on the device.[6] Files that are being written to or read from the private drive are decrypted on the fly by the FIU-810 hardware, after authentication is successful. Files in the system area are decrypted only when necessary, and then only within the security policies of the FIU-810 architecture and settings.

Once the user's fingerprints are enrolled and the private area has been set up, the partition can be accessed on non-Windows-based computers. Because the FIU-810 token handles fingerprint authentication in hardware and uses standard USB Mass Storage drivers, files stored in the

[5] Note that 2 MB must be maintained in the public storage area for the 'User Manager' software. Therefore, the maximum size of the Private Storage area is 60 MB.
[6] A new 3DES key is generated each time a new user is created. This key is stored in EEPROM.

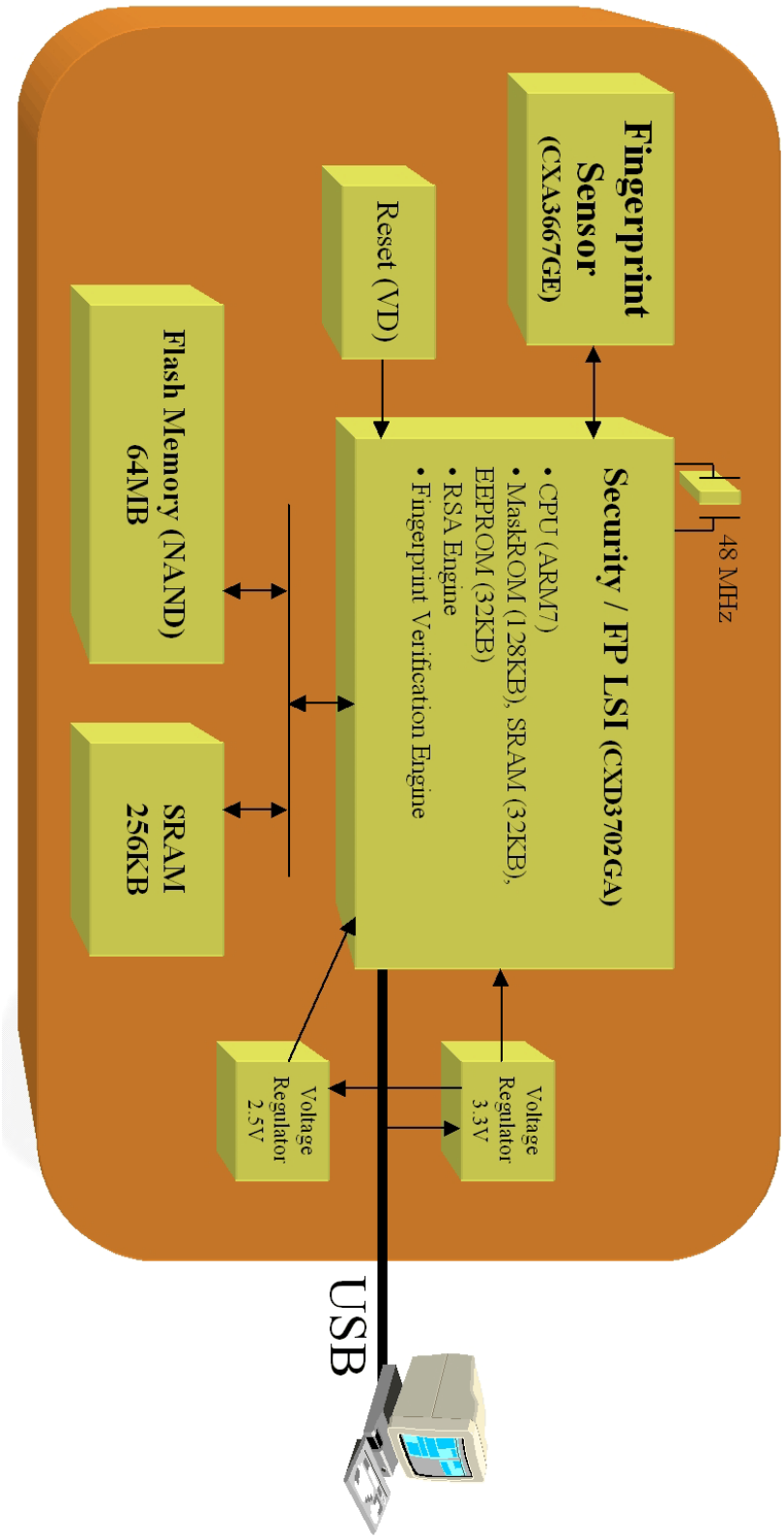
token's private area can be accessed on a Mac OS X or Linux-based PC using those systems' built-in drivers.[7]

On any machine, after a private storage area has been set and the device plugged in, the orange LED on the FIU-810 device will flash, signaling to the user that the FIU-810 unit is waiting for a finger to be placed on the reader so that it can unlock the private area. Once a finger is placed on the device, the unit will attempt to match it with the templates stored on-board, and if matched, the private storage area will be unlocked, looking to most machines as if a floppy disk had been inserted into an empty drive.

When the FIU-810 unit is unplugged from a machine, the private storage area is automatically locked. The private storage area can also be locked and unlocked manually via the User Manager application.

[7] Fingerprint management and private storage area allocation are only accessible via 'User Manager' on a Windows-based PC, however.

FIU-810 Puppy® Fingerprint Identity Token -- Block Diagram



Additional white papers describing the FIU-810 hardware and compatible software packages will be available at www.sony.com/puppy .