Operational Description
Privaris, Inc.

The plusID 75, Equipment Under Test (EUT), is a personal handheld biometric security device. A fingerprint sensor is used to capture the user's finger print which is stored in encrypted, on-board memory for later use. Once programmed, the fingerprint sensor is used to take an image which is checked for a match with the stored image in memory. On a successful match, an RF connection is established with a host machine and credentials are sent. The RF transmissions (class B) are sent via a Broadcom 2045 BT radio and antenna system with the software utilizing a Teleca BT stack.

The plusID 75 Security Device has three functions: enrollment, verification, and transmission.

Enrollment

Enrollment is the device activation and issuance process and generally occurs only once. It is what assigns or "marries" the device to its user. During enrollment, numeric representations of the unique features of a fingerprint (i.e. the ridges, valleys and whorls) are encoded and securely stored on the device. The actual fingerprint is not stored on the device. The fingerprint features are encoded and securely stored so that the device will function only for its authorized user. Also during enrollment, the user's credentials (e.g. a facility entrance code, a password, or personal identity document) are encrypted and transferred to the plusID 90 via a USB connection.

Verification

After the initial enrollment process, each time a finger is swiped over the finger print sensor on the plusID 90, the device will attempt to match that print's features to an originally enrolled fingerprint. This is the verification, or matching, process. A match is indicated by a green light and means that the user has been verified as the authorized owner of the device. If a user attempts to verify a non-enrolled finger, a match will not be found and access to the specified resource will not be granted. Failed verification attempts are indicated by a red light.

Transmission

Upon verification, which is the matching of a live finger to the template of an enrolled finger, the plusID 75 wirelessly transmits the user's credentials that were stored during enrollment (e.g. a facility entrance code, a password, or personal identity documents). The transmission is verification of the user's identity. The credentials are transferred typically as an encrypted data stream, depending on the application. Only the authorized user's finger can trigger the release of their credentials, and only the user's credentials are transferred - the stored fingerprint is never transferred and never released from the device.

The plusID 75 Security Device can store and transmit any number of user credentials including digital certificates. It supports both bluetooth and passive RFID wireless communication protocols for data transmission.