Sample Operational Description
EMC16647 FCC TCB and IC CB Certification for the BPID
Applicant: Pirvaris, Inc.

The BPID, Model LFBT1, Equipment Under Test (EUT), is a personal handheld biometric security device. A fingerprint sensor is used to capture the users finger print which is stored in 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, a connection is established with a host machine via Bluetooth and credentials are sent.

The BPID™ 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 BPID™ 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 typically encrypted and wirelessly transferred and stored on the BPID™ device.

Verification

After the initial enrollment process, each time a finger is placed on the BPID™ device, 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 BPID™ device 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 BPID™ Security Device can store and transmit any number of user credentials including digital certificates. It supports both Bluetooth™ and RFID wireless communication protocols for data transmission.

The hardware for an RFID interface was included with this model. However, the firmware for this interface was not included and the RFID interface was not functional in the version of the product supplied for testing.

A special set of firmware was loaded into the EUT to allow it to be placed in a slave mode. A Bluetooth test set was used to set the transmit channel, power and packet type to the levels indicated in each test section. Frequency hopping was turned off for the purpose of testing the transceiver at the required channels.

The LED indicators were used to determine that the EUT was successfully placed in slave mode. Then the Bluetooth test set monitored the EUT indicating a successful connection.