

Operational Description Pirvaris, Inc.

The BPID, Model LFLR1, 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, an RF connection is established with a host machine and credentials are sent. The RF transmissions are IEEE 802.15.4 compliant, using a DSSS transceiver with O-QPSK modulation. Typically a short (100 microsecond) packet is sent every 30 milliseconds, but at times the device can send packets nearly continuously. This was forced in the “test mode” that was used for these tests.

The BPIDTM 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 BPIDTM 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 BPIDTM device.

Verification

After the initial enrollment process, each time a finger is placed on the BPIDTM 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 BPIDTM 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 BPIDTM Security Device can store and transmit any number of user credentials including digital certificates. It supports both 802.15.4 and passive RFID wireless communication protocols for data transmission.

A special set of firmware was loaded into the EUT to allow it to be placed in a test mode, broadcasting at the transmit channel, power, and packet type indicated in each test section. High, mid, and low bands were evaluated 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 802.15.4 test set monitored the EUT indicating a successful connection.