Verifone VX680B Bluetooth™ Technical Document

Elavon offers the Verifone VX680B terminal to our Bank Partners that need cash advance functionality along with EMV processing. This terminal is an all-in-one short-range wireless solution with integrated chip reader, PIN pad and printer. Elavon offers SSL/TLS IP/Ethernet communication on the VX680B terminal solution (enhanced TLS functionality – TLS 1.2 – is targeted for mid-Q4 2015). Analog dial and WI-FI communication methods are not supported.

Security Overview

TheVX680B uses secure, encrypted Bluetooth v2.1 + Enhanced Data Rate (EDR) protocol technology, and operates in Bluetooth Security Mode 4 (described below). The terminal is a Class 1 Bluetooth device that provides a secure connection to a communication base (up to 300 feet).

SECURITY MODE 4

- Bluetooth Security Mode 4 is a service level enforced security mode in which security procedures are initiated after the physical layer is fully established but before the logical channels are fully established. Security requirements for services protected under Security Mode 4 on the VX680B are authenticated link key required and derived from a secret key that is unique to an individual unit and housed within the device during manufacturing.
- The derived authenticated link key is generated as a result of the Bluetooth v2.1 featured Secure Simple Pairing (SSP) without Passkey entry "Just Works" method, which streamlines the pairing process and enhances security. In utilizing the SSP pairing method, the VX680B terminal will prompt and require the user to confirm steps in the pairing process.

SECURE PAIRING PROCESSING (SPP)

The pairing process is necessary before the VX680B terminal and communication base can securely exchange information back and forth.

- Via the VX680B terminal communication administrative menu, a user manually initiates the search for and selects the communication base and securely establishes the derived authenticated Bluetooth link key.
- The communication base is not discoverable by default. A button at the back of the unit, which when pressed, will set the communication base in discoverable mode until the secure pairing process is completed, after which the communication base will no longer be discoverable.
- The terminal is at no time searchable by foreign Bluetooth capable devices either during or after the secure pairing process is completed. The communication base may be discoverable by foreign Bluetooth capable devices during the secure pairing process but no sensitive data is accessible because none is stored on the communication base.
- The newly established derived authenticated Bluetooth link key is stored in VX680B terminal and communication base Flash memory. The derived key is encrypted and cannot be reused as it is unique upon every new pairing sequence execution.

CONFIDENTIALITY

In addition to the Security Mode 4, the VX680B and its supported Bluetooth technology provides a separate confidentiality service to prevent eavesdropping attempts on the data being exchanged between terminal and the communication base.

- Once the secure pairing process is completed all transaction data traffic is encrypted using the standard Bluetooth encryption procedures (based on a stream cipher, E0).
- Additionally all transaction data traffic between the VX680B terminal and the communication base is encrypted using a 128-bit encryption key.

Your
Payment Solutions
Team

DATA AT REST (DATA STORED ON THE TERMINAL)

Data at Rest is encrypted and only stored on the VX680B terminal. It is limited to the minimal content required for subsequent transaction processing (i.e. Voids) and end-of-day settlement transmission to the Elavon host, as well as printing local receipts and reports. Data is stored only on the terminal and not the communication base. There is no clear card data stored on the terminal and all card data is truncated when printed. The Data at Rest is restricted to the local terminal memory with no external data storage or media transfer capability.

The VX680B terminal has built in tamper-resistant security modules that provide layers of device hardware security that protects against physical intrusion and access to internal data or encrypted keys. If there is an intrusion attempt to the unit, it displays a "Tamper" message and be rendered inoperable.

DATA IN TRANSIT

- Local - As previously detailed in this document, data exchange between the VX680B terminal and the communication base is encrypted and secure. Elavon supports PAN encryption.
- External - The communication base manages all transaction processing data exchange between the Elavon host via SSL encrypted IP/Ethernet protocol. TLS 1.2 support is in development for mid-Q4 2015.

PCI COMPLIANCE

The Verifone VX680B terminal solution is PCI 3.0 complaint. Certification validation can be found here. The part number for the VX680 models within the PCI site that apply to those terminals currently deployed by Elavon is: M268-70X-XX-XXn-3. The applicable part number is:

Model: VX680 Bluetooth
Part Number: M268-783-C4-USA-3

Communication Support

Elavon only offers SSL/TLS IP/Ethernet communication on the VX680B terminal solution. Both DHCP (default setting) and Static IP configuration options are supported.

- DHCP (Dynamic Host Configuration Protocol) is utilized to automatically assign a unique address to a device.
- A Static IP address can also be manually configured if required. Special terminal support procedures and handling must be predefined during the terminal boarding and setup process in order to implement this option.

Bluetooth Signal Strength

The achieved Bluetooth signal strength and range is dependent on the specific physical environment in which the terminal and communication base are utilized and what objects may be in proximity with the two devices.

It's important to take into consideration the different types of potential signal quality and range condition that may come into play when implementing the VX680B terminal, such as:

- Physical objects – Physical structures are some of the most common causes of interference. For example, thick walls, pillars, etc. are difficult for a signal to pass through due to their density.
- Radio frequency interference – Wireless technologies such as 802.11b/g use a radio frequency range of 2.4GHz and are found in many devices including cordless phone and microwaves. This can cause "noise" and weaken signal strength.
- Electrical interference – Electrical interference comes from devices such as computers, fans, lighting fixtures or any other motorized devices. The impact that electrical interference has on signal strength depends on the proximity of the electrical device to the terminal and communication base.

General FAQs

Does the terminal need to be returned to the communication base to complete a transaction?
No. The transaction and end-of-day settlement communication processing happens wirelessly via the secure encrypted Bluetooth link that is pre-established during secure pairing process between the terminal and the communication base.

How many terminals can connect to one communication base?
Up to five terminals can be paired with and communicate to one communication base. Only one terminal can communicate with the base at a time.

Can multiple communication bases be utilized in a single location?
Yes. Per standard implementation support, each communication base requires its own individual Ethernet port and cable in order to communicate out of the location to the Elavon host for transaction processing.

Is there a charging only base option available? Yes.

How long does it take to fully charge the battery?
The average range is 4-6 hours for a fully charged battery. The battery consistently charges while on the base. Elavon recommends terminals be fully charged before initial use.

How many transactions can I process on the terminal before I need to recharge the battery?
Up to 950 transactions can be processed on a fully charged battery. The actual number of transactions can vary based on the following:

- The number of receipt copies printed which is the biggest consumption of power
- The size and format of receipts and reports
- The transaction frequency and duration
- The average distance between the terminal and the communication base
- The time the payment application takes to go into sleep mode
- The time the terminal stays off its base
- The age of the battery