V-Flex™ Fingerprint Reader

November 10, 2004

1. Introduction

The intent of this document is to describe the specifications, operation, and physical attributes of the V-Flex fingerprint reader, Model Number V-FLEX, A, manufactured by Bioscrypt, Inc. The device specifications, installation specifications, and connections are provided in detail for system architects and engineers designing access control and other systems utilizing the V-Flex reader.

2. Description

The V-Flex reader shall provide a 1:1 fingerprint verification that is initialized by a Wiegand input sequence as provided by an external Wiegand reader, such as a keypad or proximity card reader. The V-Flex is designed to add biometrics to retrofit applications that have an existing Wiegand-based access control system in place. It is also designed for applications where a card technology other than HID is desired. The V-Flex shall prevent unauthorized access via loaned, lost or stolen proximity cards (or PINs) by requiring that the fingerprint of the person seeking entry match the identity of the cardholder.

3. Mechanical Specifications

3.1. Dimensions

The V-Flex reader shall measure 5.32” x 2.75” x 2.52” (135 x 70 x 64 mm) and shall arrive disassembled. The V-Flex shall be comprised of:

A. A wall plate that mounts directly to the wall or a single-gang box mounted in the wall.
B. The body that mounts to the wall plate.

A 1:1 scale diagram of this wall plate with dimensions is provided in *Figure 1: V-Flex Wall Mounting Plate*.

3.2. Material

The V-Flex reader shall be made of Polylac PA-765A, a high flow grade, flame retardant material to a UL94 V-0 standard. This material shall be used for the case body and the wall mounting plate and shall be an ABS plastic. The “finger mask” that surrounds the fingerprint sensor itself shall be a carbon fiber conductive plastic.

3.3. Fingerprint Sensor

The V-Flex reader shall incorporate the Authentec, Inc. sensor model AF-S2. The AF-S2 sensor shall be manufactured of silicon and shall be capacitive-based. The sensor surface area shall measure 24 x 24 x 3.5 mm. The sensor shall additionally incorporate Authentec’s TruePrint technology, which utilizes a patented radio frequency (RF) imaging technique that allows the sensor to generate an image of the shape of the live layer of skin that is buried beneath the surface of the finger. For more information on this imaging technology, please visit http://www.authentec.com.

3.4. Color

The V-Flex case shall have a charcoal gray body (ABS Grey – Pantone 426C). Furthermore, the color used in the “bioscrypt” text shall be Pantone 423C.

3.5. Weight

The V-Flex shall weigh 6.6 ounces (packaged weight for shipping shall be 1 pound).

3.6. Mounting

The wall mounting plate shall be designed to mount to a single gang electrical box using 2 #6-32 screws in the centerline holes, or to mount directly into a door mullion, wall anchor, wood or sheet metal using #4 flat head screws (thread diameter of <0.125 inch and a head diameter of <0.250 inch) in the 4 outer holes.

The access hole in the wall for wiring should be less than 1.5” wide so that the wall plate will cover it. It should also be less than 1.5” tall if mounting onto dry wall so that there is enough material to hold the anchor. The recommended size is 1” x 1.125” to match the opening in the wall mounting plate.

The V-Flex body case shall have two tabs that slide into slots on the wall plate. The body shall be secured to the wall plate by a single #4-40 inch screw.

3.7. Mounting Position

The V-Flex should be mounted on the wall or structure to be in compliance with all American Disabilities Act (ADA), local and federal laws as they apply to the installation. The reader should also be mounted at a height that is comfortable to use. In general, the reader should be mounted such that the height of the sensor (top of the device) is between 48 and 54 inches from the ground. Should the reader be installed below this mounting height (i.e., on a turnstile), installation of a wedge piece shall be required between the mounting surface and the V-Flex wall mounting plate. Please contact Bioscrypt Technical Support for further information.

Furthermore, the reader shall require free space above the reader such that the user has room to place their finger on the sensor. Roughly, 2-3 inches (or more) of free space is recommended depending on if there is any obstruction interfering with the view of the V-Flex. The reader should also be provided with free space (roughly 3-4 inches recommended) below the device for convenient access to the bottom RJ11 RS-232 port (see *Section 7.3: RS-232 RJ11 Port* for further details).

The V-Flex shall require an external Wiegand reader to initiate the biometric authentication. It is suggested that this external device be placed in close proximity to the V-Flex to make it simple for the user to first present their card or input their PIN and then quickly place their finger on the sensor for authentication. Please refer to *Section 8.3: External Wiegand Reader* for further information.

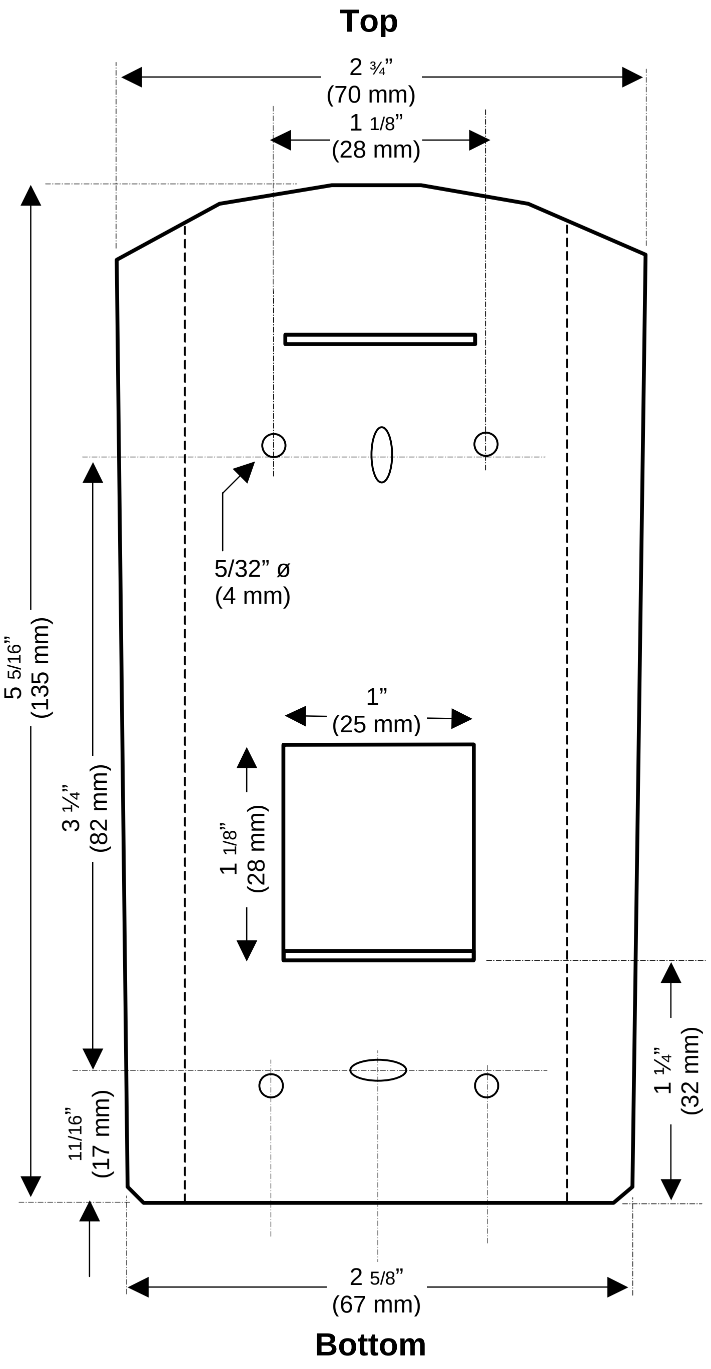

Figure 1: V-Flex Wall Mounting Plate

4. Certifications and Approvals

The V-Flex has been tested for compliance with all applicable international standards and shall have the following approvals: FCC, CE, CSA, UL294, cUL. These approvals shall be printed on the labeling located on the rear panel of the reader.

4.1. FCC Information to Users

The V-Flex shall comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

4.2. CE Information to Users

The V-Flex shall have the CE mark, for compliance with CISPR22, EN 55022 and EN 50082-1 requirements.

4.3. UL and cUL Information to Users

The V-Flex shall comply with the Standard for Access Control System Units for UL294 and with CSA C22.2 No. 205 for the cUL Mark.

5. Environmental Specifications

The V-Flex shall be manufactured for indoor use, and if placed outdoors must be installed within a complete Bioscrypt certified enclosure to protect the reader against direct contact with the elements, including rain, sun, snow, or excessive moisture. Failure to place V-Flex readers installed outdoors within such an enclosure will void the warranty.

5.1. Bioscrypt Enclosure

The Bioscrypt certified enclosure shall be required for outdoor installations and shall optionally include a heater that shall trigger on when temperatures reach below 24° C (75° F). For further information on the Bioscrypt certified enclosure, including power requirements and schematics, please contact Bioscrypt Technical Support.

5.2. Temperature

The electronics and mechanical parts that make up the V-Flex reader shall be rated to operate in a temperature range of 0° C to 60° C (32° F to 140° F). However, the extremes of this temperature range will not be a comfortable operating range for users of the system. The temperature range for the environment in which the reader will be installed should be limited to 10° C to 50° C (50° F to 120° F). Additionally, the reader should not be placed in direct sunlight or in uncontrolled environments (indoors or out).

5.3. Humidity

The V-Flex reader shall be rated to operate within a humidity range of 0% to 95% non-condensing.

5.4. Vibration

The environment in which the V-Flex shall be installed should not subject the reader to vibration.

6. Electrical Specifications

6.1. Pigtail Connections

The V-Flex reader shall include a 15-pin DB15M connector for external connections to power and other devices. A 15-conductor color-coded pigtail cable shall be provided with each V-Flex reader to facilitate connecting the reader to other wiring. The remainder of this document assumes you are using the pigtail cable provided to make connections. *Appendix A: Pigtail Cable Connections* lists the connections available through the pigtail. Also, see *Section 7: Communications* and *Section 8: Connections to External Equipment*. For additional instructions on installing the V-Flex reader, please refer to the *Veri-Series Installation Manual* which shall be provided within the software CD received with the reader.

6.2. Power Requirements

The V-Flex reader shall operate on DC power between 9 and 24 volts, however, operation at 12 VDC is recommended. The V-Flex shall consume approximately a maximum of 5 watts of power:

- At 12 VDC the device shall have an inrush current of 1 amp for 10mS and shall require continuous current up to 400 mA during operation.

The V-Flex reader shall require an isolated power supply (not provided with reader). This power supply may be optionally purchased from Bioscrypt. The power supply should be:

- Isolated from other equipment including card reader power, lock power, Access Control System power and other interference-causing or non-Bioscrypt electro-mechanical devices (i.e., power supply should be dedicated to the V-Flex reader(s)).
- Regulated and filtered.
- Protected by means of an uninterruptible power supply (UPS) or battery backup.
- A UL-Listed Class II power supply at 12 VDC, 500 mA continuous.

Additionally, the power supply should **NOT** be:

- Connected to any device that may put transients on the power supply line or cause the power supply to behave improperly. If transients are an issue in the installation, a transient voltage suppression device is also recommended.

If power is to be distributed to various V-Flex readers over some distance, then it is important to take into consideration the resistance of the cable used for power distribution. Since the reader shall require significant power levels, the cable should be of appropriate gauge (18AWG or better is recommended). Pin 11 should be connected to Power GND and Pin 13 should be connected to +12 VDC power input.

6.3. Grounding

The V-Flex reader shall have various grounding requirements:

- Power GND (Pin 11): the return for the input power supply. Pin 11 shall be connected to the negative on the power supply. Refer to *Section 6.2: Power Requirements* for further details.
- Wiegand GND (Pin 6): the reference ground for the Wiegand Data 0 and Data 1 interface. Pin 6 shall be connected to both GND on the external Wiegand reader and on the reader port of the Access Control System. Refer to *Section 8.3: External Wiegand Reader* and *Section 8.4: Access Control System* for further details.

- Signal GND (Pin 12): the reference for serial communications. Pin 12 shall be connected to the GND on the serial port or RS-485/RS-232 converter (dependent on communications protocol selected). Refer to *Section 7: Communications* for further details.
- Safety GND (Pin 15): protects the V-Flex (sensor and internal electronics) from electro-static discharge (ESD) by providing a safe discharge path to an earth ground. Refer to *Section 8.2: Earth Ground* and *Section 9.4: Fingerprint Placement: Lock, Drop & Hold* for further details.

7. Communications

The V-Flex shall include support for RS-232 and RS-485 serial communications. This is primarily intended for use with a PC running the VeriAdmin software, which allows for template management (enrollments, deletions, editions, distribution) and reader configuration. If RS-232 and RS-485 communications are desired for use with an application other than the VeriAdmin software, the BIO-SDK (Bioscrypt Software Development Kit) shall be required to integrate V-Flex support into a custom application. Refer to *Section 11: VeriAdmin Management Software* for further details on the software features.

The V-Flex shall provide three serial communications ports:

- RS-485 accessible through the pigtail (DB15)
- RS-232 accessible through the pigtail (DB15)
- RS-232 accessible through the bottom RJ11 port

Only two of the three ports may be activated at a time. By default, the V-Flex shall be configured for Port Mode 1 (Host RS-485 DB15 / Aux RS-232 RJ11), which activates the RS-485 port accessible from the pigtail and the RS-232 port accessible from the bottom RJ11 port.

7.1. RS-485 DB15 Port

The V-Flex reader shall support RS-485 serial communications protocol accessible from the DB15 port. This shall be the default configuration for the reader. For RS-485 protocol support, an external converter must be utilized. Bioscrypt has tested and qualified the B&B Electronics 485TBLED RS-485/RS-232 converter for use with the V-Flex reader (must be purchased separately). The B&B Electronics converter connects directly to both the Host PC and to the V-Flex reader. This converter shall support “sense data,” also referred to as "send data". This is necessary since the V-Flex reader shall utilize a half-duplex (2-wire) RS-485 signal with no RTS/CTS control on the RS-232 line.

The RS-485 communications protocol should be chosen if a network of more than one V-Flex reader is being installed or if a single reader is being installed more than 150 feet from the PC or other host. The maximum cable distance for a RS-485 network is 4,000 feet (1200 meters), over which no more than 31 V-Flex readers can be added. To extend these limitations, contact Bioscrypt Technical Support. No end-of-line termination is required at a baud rate of 9600. For RS-485 communications, the V-Flex readers must be connected as follows:

- ❑ Use Category 5 rated cable (shielded is recommended). This cable should be dedicated to the RS-485 network connection between the B&B Electronics 485TBLED converter and the V-Flex readers and should not be used for any other purpose.
- ❑ Use Pin 7 [RS-485 (-)], Pin 8 [RS-485 (+)] and Pin 12 [Signal GND].
- ❑ The B&B Electronics 485TBLED converter shall require 12VDC/100mA power from an external supply.
- ❑ Connect the B&B Electronics 485TBLED converter to the PC's DB9 COM Port using a DB25-to-DB9 cable.
- ❑ Connect the V-Flex readers in a daisy-chain configuration (i.e., Converter → Reader 1 → Reader 2 → Reader 3, etc.). Do NOT use a star or other multi-drop configurations.

For a wiring diagram and more specific instructions please refer to the *Configuration for Veri-Series Fingerprint Readers and RS-485/RS-232 Converter* application note.

7.2. RS-232 DB15 Port

The V-Flex reader shall support RS-232 serial communications protocol accessible through the DB15 port. The V-Flex shall require configuration by means of an active port (RS-485 DB15 or RS-232 RJ11) to activate the RS-232 DB15 port by selecting a Port Mode of 0 (Host RS-232 DB15 / Aux RS-232 RJ11) or 2 (Host RS-232 DB15 / Aux RS-485 DB15). Note that if Port Mode 2 is selected, the bottom RJ11 RS-232 port shall be de-activated. The RS-232 protocol does not run on a differential pair of wires like the RS-485 protocol, and shall therefore be less immune to EMI and other noise sources. The tradeoff for RS-232 shall be speed versus distance. RS-232 communications distances are dependent on the baud rate (bps). For example, at 9600 baud, a distance of

150 feet is possible using shielded cable, but at 57600 baud, a maximum of 20 feet is recommended.

RS-232 communications protocol should be chosen only if a single reader is being installed less than 150 feet from the PC or Host device. For RS-232 DB15 communications, the V-Flex readers must be connected as follows:

- Use Category 5 rated cable (shielded is recommended). This cable should be dedicated to the RS-232 connection between the V-Flex reader and the PC or host device.
- Use a female DB9 connector.
- Connect Pin 9 (RS-232 Tx) to the DB9 Pin 2.
- Connect Pin 10 (RS-232 Rx) to the DB9 Pin 3.
- Connect Pin 12 (Signal GND) to the DB9 Pin 5.

7.3. RS-232 RJ11 Port

The V-Flex reader shall provide a RS-232 RJ11 port on the bottom of the device for convenient access. This shall be the default configuration for the reader. This RJ11 port is implemented as a 6p6c (6-position, 6-conductor) jack. This port shall be physically protected by means of a pin-in-hex security screw. Additional security shall be provided through a password protection feature, which may be activated through the VeriAdmin software.

Additionally, an RJ11-to-DB9 programming cable shall be provided with each V-Flex reader. This cable shall be a 6-foot, 6p6c straight-thru cable with an RJ11-to-DB9 adaptor. This cable should be used to configure the reader and may optionally be used for template management and other functions desired via a local connection.

The RS-232 protocol does not run on a differential pair of wires like the RS-485 protocol, and shall therefore be less immune to EMI and other noise sources. The tradeoff for RS-232 shall be speed versus distance. RS-232 communications distances are dependent on the baud rate (bps). For example, at 9600 baud, a distance of 150 feet is possible using shielded cable, but at 57600 baud, a maximum of 20 feet is recommended. By default, this port will be configured for 57600 baud.

To create your own RJ11-to-DB9 cable the following is required:

- Use Category 5 rated cable (shielded is recommended). This cable should be dedicated to the RS-232 connection between the V-Flex reader and the PC or host device.
- Use a female DB9 connector.
- Use a 6p6c RJ11 jack.
- Orient the jack so that the 6 gold pins are facing upward and the jack (or clip) is facing the user. Pin 1 would be on the far left and Pin 6 would be on the far right.
- Connect the RJ11 Pin 1 (RS-232 Tx) to the DB9 Pin 2.
- Connect the RJ11 Pin 2 (RS-232 Rx) to the DB9 Pin 3.
- Connect the RJ11 Pin 5 (Signal GND) to the DB9 Pin 5.

8. Connections to External Equipment

8.1. Power

The V-Flex reader shall require an isolated power supply (not provided with reader). This power supply may be optionally purchased from Bioscrypt. Two conductors shall be required for this connection (Pins 11 & 13). Since the reader requires significant power levels (see *Section 6.2: Power Requirements*), the cable should be of appropriate gauge (18 AWG or better is recommended).

8.2. Earth Ground

The V-Flex reader shall require a homerun connection to Earth Ground using Pin 15. This connection shall help to protect the V-Flex (sensor and internal electronics) from electro-static discharge (ESD) by providing a safe discharge path to an earth ground. Pin 15 must be connected to a proper earth ground such as a cold-water copper pipe or building ground. The connection chosen for Earth Ground should measure less than 4 ohms resistance when measured against a known local Earth Ground. DO NOT CONNECT PIN 15 TO POWER GROUND. At a minimum, this connection should be made with a low-resistance, single-conductor cable (14 – 18 AWG is recommended). Internally, Pin 15 is connected to the finger mask (conductive plastic surrounding the fingerprint sensor) and should be used in conjunction with the Ridge-Lock. Refer to *Section 9.4: Fingerprint Placement: Lock, Drop & Hold* for further details.

If no such connection is provided, Bioscrypt will consider that the reader was not properly installed and may consider the warranty void.

8.3. External Wiegand Reader

The V-Flex reader shall support Wiegand protocol for the required input connection from an external Wiegand reader (such as a Wiegand keypad or proximity reader). **This connection is required by the V-Flex reader in order to initiate a biometric authentication - the V-Flex shall not function solely as a biometric reader.**

To support a given external Wiegand reader, it is important that the external Wiegand reader meet the following requirements:

- Wiegand data is sent on output as a standard binary representation (i.e., hex and other data interpretations are not supported)
- Wiegand data is sent in a Wiegand format supported by the V-Flex*
- 5 VDC Wiegand is supported (i.e. Data 0 and Data 1 lines should rest at 5 VDC when idle as opposed to 12 VDC)
- Data 0 and Data 1 lines should fall to below 700 - 500 mV to indicate a bit

*The V-Flex reader by default shall have the Wiegand input activated for a Standard 26-bit Wiegand format. The reader shall support other Wiegand formats. Refer to *Appendix B: Wiegand Protocol* for further information.

The V-Flex shall **NOT** directly support the following external reader technologies and shall instead require that a Wiegand converter or interface be installed between the two devices:

- Bar code
- Magnetic stripe
- F/2F

Please contact Bioscrypt Technical Support for further information on these technologies or to check compatibility between your selected external reader and the V-Flex.

For Wiegand input, the V-Flex reader shall require a direct (e.g., homerun) connection from the external Wiegand reader with an 18 – 22 AWG cable using the following three conductors:

- Wiegand In Data 0 (Pin 2) connected to the Wiegand reader Data 0
- Wiegand In Data 1 (Pin 4) connected to the Wiegand reader Data 1
- Wiegand GND (Pin 6) connected to the Wiegand reader Power GND**

**Wiegand GND (Pin 6) should be commoned to both Power GND on the external Wiegand reader and the Access Control System reader Power GND if Wiegand output is also used (refer to *Section 8.4: Access Control System*). Pin 6 acts as the reference ground for the Wiegand Data 0 and Data 1 interface.

8.4. Access Control System

The V-Flex reader shall support Wiegand protocol output for connection to an Access Control System (ACS). This system may provide advanced access control features such as audit trails, user-defined access scheduling, anti-passback, etc.

An 18 – 22 AWG cable should be used for this connection. At 18 AWG, a distance of 500 feet is possible. For Wiegand output the V-Flex reader shall require a homerun connection to the ACS using the following three conductors:

❑ Wiegand Out Data 0 (Pin 1) connected to the ACS Data 0
❑ Wiegand Out Data 1 (Pin 3) connected to the ACS Data 1
❑ Wiegand GND (Pin 6) connected to the ACS reader power GND (0 VDC)**

The V-Flex reader shall by default have the Wiegand output activated for Standard 26-bit Wiegand format. The reader shall support other formats. Refer to *Appendix B: Wiegand Protocol* for further information.

**Wiegand GND (Pin 6) should be commoned to both Power GND on the external Wiegand reader and Access Control System reader Power GND. Pin 6 acts as the reference ground for the Wiegand Data 0 and Data 1 interface.

8.5. Line Trigger

The V-Flex reader shall include a Line Trigger, a low-level signal that is triggered following a successful verification. By default, this line shall be inactive and must manually be activated through use of the VeriAdmin management software provided with the reader. When the Line Trigger is activated, the user must also specify the duration (in seconds) the trigger should be set high. This source output is an open-drain drive capable of 50 mA with a maximum voltage drop of 1 VDC from a 5 VDC source. This drop is load-dependent.

8.6. PC or other Host Device

The V-Flex reader shall support RS-232 and RS-485 serial communications protocols for connection to a PC or other host device. Each V-Flex reader shall include a VeriAdmin software CD. This software allows for reader configuration and template management. For more information on the VeriAdmin software functionality please refer to *Section 11: VeriAdmin Management Software*. If connecting to a PC, it should have the following characteristics:

- ❑ Operating System: Windows 98, ME, NT4.0, 2000, or XP (not compatible with Windows 95)
- ❑ 486-compatible
- ❑ 16 MB RAM
- ❑ 30 MB Disk space
- ❑ DB9 Serial communications port (do not support USB ports)

For more information on the RS-232 and RS-485 connections please refer to *Section 7: Communications*.

Although the V-Flex reader does not have built-in Ethernet support, it may be connected to a Lantronix UDS-10 Serial Device Server for this purpose. For more information on this connection please refer to the application note *Configuration for Veri-Series Fingerprint Readers and Lantronix UDS-10 Serial Device Server*.

9. Operation

The V-Flex reader shall be designed to integrate easily into most access control systems. To function, a fingerprint must be enrolled on the reader and this can be done through the VeriAdmin software included with the reader. Once a fingerprint is enrolled, authentication may be performed any number of times. After authentication, the original Wiegand string, as provided by the external Wiegand input (i.e., proximity card or PIN) and which contains the user ID number associated with the fingerprint template, shall be sent to the Access Control System or other host equipment for appropriate action.

9.1. Fingerprint Template Capacity

The V-Flex shall include support for up to 4000 fingerprint templates within its internal memory. By default, the V-Flex may only retrieve templates from its own internal memory. When placed in an advanced polling mode, the V-Flex reader may additionally retrieve templates from a PC or other host device. For this advanced polling mode functionality, the Bio-SDK (Software Development Kit) will be necessary to create custom software incorporating this feature.

9.2. Memory

The V-Flex reader shall utilize non-volatile flash memory to store all templates and data configurations and shall therefore not lose any templates or configuration information if the reader is powered down.

9.3. User Interface

The V-Flex shall have a common user interface. A green LED on the front of the reader shall indicate that power is on. A bi-color LED on the top of the reader shall display green, red, or amber (green and red together). The top LED may display in an off, solid or blinking (flashing) state. The color and state of the top LED may also be customized through the use of the VeriAdmin software. By default, the color and state of the top LED shall have particular meanings as shown in Table 1: V-Flex LED Feedback.

Top LED Indicator	Meaning
Off	Reader is Idle
Solid Red	Invalid Input (i.e., Card, PIN, etc.) Biometric Authentication Failed
Solid Amber	Place Finger on Sensor
Solid Green	Biometric Authentication Accepted Enrollment Fingerprint Image Captured
Flashing Red	Present Card to be Deleted
Flashing Amber	Present Card to be Enrolled

Table 1: V-Flex LED Feedback

9.4. Fingerprint Placement: Lock, Drop & Hold

A Ridge-Lock shall be provided as part of the fingerprint sensor mask as a fingerprint placement guide and a means to discharge ESD. To properly place the finger on the sensor, the user should slide their finger across this Ridge-Lock, parallel to the sensor. Once the Ridge-Lock locks into place under the first joint, the user should then lower the finger evenly onto the sensor and apply moderate pressure. The user should hold the finger on the sensor until the top LED turns off and returns a green LED. A Macromedia Flash animation depicting proper fingerprint placement using the Ridge-Lock may be viewed online at http://www.bioscrypt.com > Support > Enrollment Tips. This information is also available for download as a PDF file.

The Ridge-Lock is designed as a guide to help the user to properly and consistently position their finger on the sensor so as to fully capture the fingerprint core, the unique information-rich area of the fingerprint. When used properly during enrollment and authentication, the Ridge-Lock shall help to reduce false rejections.

As the end user's first point of contact with the reader, the Ridge-Lock is also designed as means of discharging ESD through the Earth Ground connection, which is manufactured using a carbon fiber conductive plastic. This shall help to protect the sensor from damage by ESD. This requires that the reader have a proper connection to Earth Ground. For more information on this connection please refer to *Section 6.3: Grounding* and *Section 8.2: Earth Ground*.

9.5. Enrollment

Enrollment is the process of adding users to the fingerprint reader system. The V-Flex shall provide one-touch enrollment through either of the following methods:

- ❑ At a PC running the VeriAdmin software. The Enrollment PC should be located in close proximity to a V-Flex reader. When initiated through the software, the template that is created through the enrollment process may be stored either on the PC or the reader itself. When saved to the PC, the fingerprint template shall not be usable on the V-Flex reader for authentication until the template is transferred to the reader's internal memory (unless the reader is in advanced polling mode – see *Section 9.1: Fingerprint Template Capacity* for further details).
- ❑ At the reader locally through the use of an Enrollment Command Card. Command Cards must first be enrolled through the use of the VeriAdmin software. Once an Enrollment Command Card has been created using the software, it may then be used to locally activate an enrollment mode directly at the reader without the use of the software. When initiated through a Command Card, the template that is created during the enrollment process is stored locally on the reader

itself. For more information on the Command Card process, please refer to the *Veri-Series Operations Manual*.

When enrollment is initiated, the reader shall display a solid amber LED to indicate to the user to place a finger on the sensor. When the fingerprint is captured, the LED shall turn off. Once the processing is completed, the LED shall turn red or green depending on the result. The reader shall also produce an audible tone when enrollment is successful.

We suggest that enrollments be performed through the method using the VeriAdmin software instead of using the Command Cards. When the VeriAdmin software is used for enrollments, the software shall provide feedback regarding the image capture which allows the enrollment administrator to validate that the fingerprint core was fully captured and properly centered in the field of view. Additionally, quality and content scores shall be returned rating the enrollment; however, the image capture should act as the ultimate deciding factor in accepting the enrollment. This typically tends to yield a higher quality database of fingerprint templates, helping to reduce false rejections.

When a template is stored on the reader after enrollment is complete, the template shall reside on the reader until deleted, and the user shall be able to authenticate on this particular reader as long as the template is resident.

During the enrollment process, the V-Flex reader shall not be available for access control functions. This, however, shall not affect other readers on the network (if any). In many circumstances, it is recommended that an additional reader be designated for use as an Enrollment Station.

9.6. Fingerprint Template Format

During the enrollment process, the V-Flex shall create a fingerprint template roughly 348 bytes and shall be compatible with other Bioscrypt authentication devices (i.e. V-Prox, V-Smart, V-Smart iCLASS, V-Station, V-Station Prox, V-Station MIFARE, V-Station iCLASS). This template is smaller in size than identification templates and may not be converted to identification templates for use on a searching device (i.e., V-Pass or V-Station Search).

9.7. Template Distribution

Once a fingerprint template has been enrolled, it may be distributed to other V-Flex readers using the VeriAdmin software. This distribution may occur over a RS-485 network, or templates may be downloaded to a laptop and then the laptop may be used to upload the templates locally to each of the remaining readers via the bottom RJ11 RS-232 port.

9.8. Authentication

Authentication is the process of providing the V-Flex with an ID number representing one or more templates stored on the reader, presenting a candidate fingerprint to the sensor, and getting a result of pass, fail, or invalid ID. The V-Flex reader shall be based on a digital signal processor (DSP) that utilizes a fingerprint sensor to capture an image of the presented finger. The authentication process on the V-Flex is as follows:

- The user presents provides an input to the external Wiegand reader (i.e. proximity card or numeric PIN)
- The V-Flex shall extract the Wiegand sequence from the external Wiegand reader and store the information in a buffer
- The V-Flex shall pull up the template(s) corresponding to the Wiegand ID and return an amber LED signaling the user to place their finger on the sensor to proceed with the verification process. If the Wiegand ID provided by the user does not correspond to a validly enrolled template, the reader shall return a red LED indicating failure
- The user will present their finger to the sensor
- The V-Flex sensor shall capture the fingerprint
- The V-Flex DSP shall perform a 1:1 verification between the captured image and the stored template
- The V-Flex shall return a red or green LED indicating failure or pass
- On a pass, the V-Flex shall then release the Wiegand sequence from buffer to output to an Access Control System and/or activate the Line Trigger (depending on the reader's configuration).

Due to the nature of the 1:1 (one-to-one) algorithm utilized by the V-Flex, the Wiegand input provided by the external Wiegand reader shall be required in order to initiate the biometric authentication.

9.9. Granting Access

When used in conjunction with an Access Control System (ACS), physical access shall not be granted by the V-Flex directly. The V-Flex reader shall simply send a Wiegand data signal to the ACS. That system is responsible for logging and making the decision to release door locks, etc.

When the Line Trigger feature is used, any user fingerprint template stored on the reader shall have the ability to perform a biometric authentication and access the V-Flex reader. The V-Flex reader itself does not support advanced access control features (such as audit trails, user-defined access scheduling, anti-passback, request to exit buttons, etc.). For these features, an ACS shall be required.

9.10. Biometric Authentication

By default, the V-Flex reader shall require that users present a candidate fingerprint for authentication. However, biometric authentication may be globally disabled on the V-Flex reader. In this mode, the reader will act simply as Wiegand reader and output a Wiegand string after a valid Wiegand ID has been presented.

10. Estimated Performance

Bioscrypt works to continuously improve the performance of the core fingerprint authentication technology while also improving the usability and flexibility of the system. We have developed a database of real-world fingerprint images and use these images to test the algorithm used by the V-Flex. This database has increased in size to the point where today we perform 1,000,000 comparisons to generate the following statistics.

10.1. Performance Terminology

Biometric systems typically state performance in terms of False Rejection Rates (FRR) and False Acceptance Rates (FAR).

The FRR is the expected rate at which the system would incorrectly reject (fail) the correct fingerprint – this assumes that the ID number is provided correctly from an external Wiegand input.

The FAR is the expected rate at which the system would incorrectly accept (pass) the wrong fingerprint.

10.2. Authentication Algorithm

The authentication algorithm allows for two different performance-tuning parameters: Global Security Threshold and individual Template Security Threshold. Table 2: Security Threshold Error Rates lists the FRR and FAR values for various security levels. The V-Flex shall use the lower of either the Global

Security or individual Template Security Threshold when performing the authentication.

Security Threshold	FRR	FAR
Very High (1)	1/100	1/20,000
High (2)	1/200	1/5000
Medium (3)	1/1000	1/1000
Low (4)	1/5000	1/200
Very Low (5)	1/10,000	1/100
None (0)*	0	1
Password Only (6)**	0	1

Table 2: Security Threshold Error Rates

The V-Flex by default shall be configured to a Medium Global and Template Security Threshold. This threshold level is referred to as the Equal Error Rate (EER) or the point at which the FRR is equal to the FAR. As shown above, the EER for the V-Flex is 1/1000.

*The None Template Security Threshold level shall be applicable only to individual fingerprint template files and may not be applied as a global reader setting. When a level of None is selected for an individual fingerprint template, the reader shall not initiate a biometric authentication and shall instead accept any user that presents an input (i.e. card or PIN) corresponding to an enrolled fingerprint template. There shall be two options for this setting: a finger is required, but any finger shall be accepted (the default setting), or no finger shall be required.

**The Password Only Template Security Threshold is not applicable on a V-Flex reader and is instead intended for a V-Station reader. Note that the V-Flex shall not require a finger to be presented for biometric authentication for any fingerprint templates with a Template Security Threshold level of Password Only. For more information on this setting please contact Technical Support.

11. VeriAdmin Management Software

Each V-Flex reader shall include a CD-ROM containing the VeriAdmin PC software. The VeriAdmin software supports Windows 98/NT4.0/ME/2000/XP. It is not tested under other Windows-compatible or non-Windows-based operating systems.

The VeriAdmin Management Software may be used to perform the following functions:

- ❑ Manage a network of V-Flex readers
- ❑ Enroll new user fingerprint templates
- ❑ Edit existing user fingerprint templates
- ❑ Delete user fingerprint templates
- ❑ Distribute the user templates from the V-Flex reader or PC to other Bioscrypt readers in the installation
- ❑ Create Command Cards – proximity cards or PINs with the privilege to enroll or delete other user users locally at the reader (without necessity of software)
- ❑ Adjust the parameters (communications, biometrics, Wiegand, line trigger, etc.) of an individual reader or all readers connected on a network
- ❑ Configure the operation of the V-Flex top LED
- ❑ Perform firmware updates

For further details on the VeriAdmin software and its operation, please refer to the *Veri-Series Operations Manual* (installed on the PC at the time of software installation).

12. Appendix A – Pigtail Cable Connections

The following table represents the color codes and signal descriptions used in the pigtail cable for the V-Flex reader. This pigtail cable is interchangeable and may be used with the V-Flex and V-Pass fingerprint readers.

Pin #	Signal Description	Original Cable (Gray Jacket)	New Cable (Blue Jacket)
1	Wiegand Out Data 0	Red/Black	Green
2	Wiegand In Data 0	Green/Black	Green/White
3	Wiegand Out Data 1	Orange	White
4	Wiegand In Data 1	Orange/Black	White/Black
5	Line Trigger	Green	Gray
6	Wiegand GND	Red	Black/White
7	RS-485 (-)	Blue/Black	Blue/Black
8	RS-485 (+)	White	Blue
9	RS-232 TX	Black/White	Violet
10	RS-232 Rx	Red/White	Violet/White
11	Power GND	Black	Black
12	Signal GND	Green/White	Black/Red
13	Power Input (9-24VDC)	Blue/White	Red
14	Reserved	Blue	Red/White
15	Safety GND	White/Black	Green/Yellow

Table 3: 15-Conductor Pigtail Cable Connections

13. Appendix B – Wiegand Protocol

The Wiegand protocol has become a standard means of communicating user identification numbers between access control front-end products, such as a card reader or keypad, and the access control system interface to that front-end. Some manufacturers have modified the original standard format for their own use, but often still support the original standard.

The V-Flex reader shall support a variety of formats; however, the factory default is the Standard 26-bit format as described below. Note that the format selected shall be used for both Wiegand input (extracting sequence from external Wiegand reader) and Wiegand output (releasing sequence to Access Control System). The V-Flex shall not support the use of a different format for input than output.

13.1. Standard 26-bit Format

The Wiegand protocol is described completely in a document available from the Security Industry Association (SIA) as *Access Control 26-bit Wiegand Reader Interface Standard*. Without going into the detail provided in that document, the Wiegand communication format can be summarized as providing a series of binary bits (0 or 1) that are interpreted as two (2) data fields: site code and identification number. Proprietary and customized formats are prevalent and can contain extended data ranges or additional data fields, but the standard format is 26-bit.

The 26-bit format is generally diagrammed as follows:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
P_E	S	S	S	S	S	S	S	S	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	P_O
	E	E	E	E	E	E	E	E	E	E	E	E	O	O	O	O	O	O	O	O	O	O	O	O	

Where P represents a parity bit, S represents a bit from the Site Code (also referred to as a Facility Code), N is a bit from the ID Number (also referred to as Card ID), E represents bit positions that are used for Even parity calculations, and O represents bit positions that are used for Odd parity calculations. The facility code is 8 bits and supports values from 000 to 255. The ID number is 16 bits and supports values from 00000 to 65535.

In the case of a V-Flex the ID number assigned to each fingerprint template should be identical to the proximity Card ID or keypad PIN number.

13.2. Other Supported Formats

The V-Flex shall support the following Pre-Defined Wiegand formats:

- Standard 26-bit
- Apollo 44-bit
- Northern 34-bit
- Northern 34-bit (no parity)
- Andover 37-bit*
- Generic 64-bit*
- Ademco 34-bit
- HID Corporate 1000 35-bit
- HID 37-bit
- Wiegand 4002 40-bit*
- Generic 34-bit*

If the external Wiegand reader and the Access Control System are configured for a Wiegand format other than the default of Standard 26-bit, then the software shall be required to select the supported format.

Only one format may be selected and configured into the reader at a time (i.e. the V-Flex reader shall not support both Standard 26-bit cards and Northern 34-bit cards at the same time).

*This format is available as a Custom Pre-Defined Format and must be manually uploaded to the reader. Please refer to section *13.3: Custom Pre-Defined Formats*. Contact Bioscrypt Technical Support to confirm compatibility with your reader.

13.3. Custom Pre-Defined Formats

The V-Flex reader shall support the use of a Custom Wiegand Format. A slot on the Pre-Defined Wiegand Formats drop-down list shall be allocated to a Custom Wiegand Format. A Custom Wiegand Format file shall be required and must be uploaded onto the V-Flex reader. This file may be created only by the Bioscrypt Engineering Department after thorough tests are completed involving all necessary equipment (i.e. cards, Access Control System, etc.) to be utilized at the site. Please contact Bioscrypt Technical Support to see if the Wiegand format used by your external Wiegand reader and Access Control System is available as a custom Wiegand format.

13.4. Pass-Thru Formats

If the format you prefer to use is not available as a Pre-defined or Custom format, the V-Flex reader shall support a Pass-Thru mode. In this mode, critical information about the format is provided to the V-Flex reader, which shall allow the V-Flex reader to correctly extract the sequence and interpret the ID sent by the external Wiegand reader. To support your proprietary Wiegand format in a Pass-Thru mode, the following is required:

- Wiegand data is interpreted as a standard binary representation (i.e. hex and other data interpretations are not supported)
- A contiguous series of bits for the ID number
- The sequence must be non-encrypted
- The Total number of bits in the format is 64 or fewer
- The bit stream provides the bits in order from Most Significant Bit (MSB) to Least Significant Bit (LSB)

The V-Flex reader shall be unable to correctly interpret the ID number if the conditions above are not met. If your Wiegand format meets these requirements, then the following information is required to configure this format into the V-Flex reader in Pass-Thru mode:

- Total Number of Bits in the format
- Start bit position of the ID number data in the format (note: Bioscrypt considers the first bit position as 0)
- Length of the ID number data in the format (number of card id bits)

13.5.Pre-Defined vs. Pass-Thru Functionality

Advanced Wiegand functionality shall be available for use on a V-Flex when a Pre-Defined or Custom format is used that shall not be available for Pass-Thru formats. Since Bioscrypt has intimate knowledge of Pre-defined and Custom formats (including site code start and length, parity bit start and length, parity bit calculation, etc.), the following features are available for Pre-Defined and Custom formats:

- Alt Site Code: an alternate site code may be activated and selected. This code shall override the site code on all proximity cards used in conjunction with an external Wiegand reader connected to the V-Flex. When this option is not selected, the site code provided by the card shall be passed through to the Access Control System on successful authentications. If a site code is not provided by the external Wiegand reader (as when using a keypad), the Alt Site Code parameter shall allow you to configure a site code into the V-Flex if one is expected by the Access Control System.
- Fail ID Code: a failure code may be activated and selected. This code shall supersede the ID portion of the Wiegand string for all failed authentications that occur at the reader. When this option is not

selected, a Wiegand sequence shall not be sent to the Access Control System on failures.

- Fail Site Code: a failure code may be activated and selected. This code shall supersede the site or facility code portion of the Wiegand string for all failed authentications that occur at the reader. When this option is not selected, a Wiegand sequence shall not be sent to the Access Control System on biometric failures.
- On Fail Send Inverse Parity: when activated, a failed authentication shall result in the Wiegand sequence being sent to the Access Control System with the parity bits inversed to indicate failure. This option should not be selected unless the Access Control System performs parity bit calculation and supports this feature.

13.6.Extended ID

The V-Flex reader shall support Wiegand formats, which allocate up to 64 bits for the Card ID. Because Bioscrypt fingerprint templates by default use only up to a 32-bit ID, any Wiegand Formats which allocate more than 32 bits to the ID number shall require the V-Flex to be in a special Extended ID mode, which adds an Extended ID field to the fingerprint template. This field actually uses the Employee ID field (not shown in VeriAdmin) and the Password field (not available on a V-Flex).

For Extended ID support, the V-Flex shall require firmware version 7.30 or greater with a VeriAdmin software version of 5.30 or greater. Also, a Custom Wiegand Format file or Pass-Thru Format shall be required to support Extended IDs. For more information on this feature, please contact Bioscrypt Technical Support.

13.7.Duress Signals

The V-Flex reader shall support a Duress Finger Mode which offers users a way to indicate a duress situation (such as being forced to open a door) by authenticating with a specially designated “duress finger”. An individual fingerprint template may be specified as such by selecting the “Make Duress Finger” option during enrollment. One Wiegand ID may be used for both duress and non-duress finger templates. When a successful authentication occurs with such a template, the reader shall send the Wiegand sequence to the access control panel in reverse bit order. The Access Control System can then respond with the appropriate action (alerting security personnel, sounding alarms, etc.). To fully support this feature, the Access Control System must also support reverse-bit Wiegand sequence duress signals.

Technical Support Contact Information:

Bioscrypt
5805 Sepulveda Blvd., Suite 750
Van Nuys, CA 91411
USA
Hours: 530A – 500P
Direct: 818-304-7180
Toll-Free: 866-304-7180
Fax: 818-304-7187
E-mail: support@bioscrypt.com
Web: http://www.bioscrypt.com

Disclaimer

The information in this document has been carefully checked for accuracy and is presumed to be reliable. Bioscrypt, Inc. and its writers assume no responsibility for inaccuracies and reserve the right to modify and revise this document without notice.

It is always our goal at Bioscrypt, Inc. to supply accurate and reliable documentation. If you discover a discrepancy in this document, please e-mail your comments to support@bioscrypt.com or contact Bioscrypt Technical Support at the telephone numbers listed above.

Bioscrypt accepts no liability for the misuse of third-party hardware mentioned in this document. In no case shall Bioscrypt be liable for damage to a reader resulting from the misuse of such hardware.

Version Number: 3
Date: November 10, 2004

Corporate & Canadian Office
5450 Explorer Drive, Suite 500
Mississauga, ON, Canada L4W 5M1
T 905 624 7700
F 905 624 7742
www.bioscrypt.com

U.S. Office
5805 Sepulveda Blvd., Suite 750
Van Nuys, CA 91411
T 818 304 7150
F 818 461-0843

U.K. Office
35 Jackson Court, Hazlemere
High Wycombe, Buckinghamshire
England HP15 7TZ
T +44 (0) 1494 814 404
F +44 (0) 1494 815 513

Document# 430-00139-02