bioscrypt

V-Station™

Operator’s Manual

Version 7.50

Table of Contents

1. Introduction

This document describes how to operate a V-Station with firmware version 7.50 from the keypad at the unit without using the PC administration software. All of the menus and how they link together are described along with general principles of how to navigate the menu tree. This document assumes a basic understanding of how other Bioscrypt products are operated and administered.

2. Navigation

There are three primary ways a user or administrator can interact with a V-Station: navigating menus, entering data and initiating actions. The results of specific actions are described in more detail in the various menu sections, beginning with Section 5. This section describes how navigating the menus and entering data are accomplished.

There are two main groups of buttons on the V-Station, numeric and navigational. Any button with a number on it fits in the first group and the rest belong in the second group.

2.1 Numeric Buttons

The first group of buttons is used only to enter information. When a screen that does not require user input is displayed, these buttons have no effect. There are several input screens that require the user to distinguish one choice out of two or three. Some of these do not require the user to hit ENTER (called "hot keys"). All other input screens require pressing ENTER after keying in data. If a screen does not change after you key in data, press ENTER.

2.2 Navigational Buttons

Above the numeric keys is a row of three navigational keys. From left to right, they are ▽, ▲ and △. The other navigational keys are where the "*" and "#" keys would be on a phone. They correspond to CLEAR and ENTER, respectively. The ▲ key and ENTER key serve the same function, described below. Placing the ▲ key between the arrow keys makes navigation a little simpler.

Within any menu, going between entries is simply a matter of using the △ and ▽ buttons. When the beginning or end of a menu is reached, scrolling does not wrap around. An icon in the upper right corner will indicate which direction of navigation is valid. When you get to the last entry in a menu, the icon is an up arrow. At the first entry, it is a down arrow and for all other entries, an icon with arrows pointing both up and down will appear.

Unlike firmware version 7.00, versions 7.10 and after show up to four menu items at a time. The item that is currently selected is indicated two ways. The text is highlighted with a black bar and an arrow appears at the beginning of the line.

After using the ▲ and ▼ keys to get to the menu desired, the ENTER key or the ● key will select it. At that point, either a user entry screen will appear or another set of menus will appear. To back out of a menu selection, simply use the CLEAR button, much as you would use the “Back” button in a web browser. CLEAR also acts as a backspace key in a user entry menu. When all of the characters in a user entry menu have been erased, CLEAR reverts back to acting like “Back.”

For security purposes, there is a global inactivity timeout. If you access the menu system and remain idle for a long period of time (60 seconds), the unit will revert back to the splash screen. Before this happens, a blinking box with an “x” inside will appear for ten seconds in the bottom right of the LCD.

3. User Interface

Once users are enrolled, using the V-Station to verify them is a simple procedure. On the searching model (A-S), users simply put their finger on the sensor. After detecting a finger, the unit will display “Remove finger, Searching database” and display the result on the LCD as well as flash the LED appropriately. With all models (A-S included), users can simply enter their ID on the keypad or initiate the proper Wiegand input, wait for the screen to say “Place Finger” (the top LED will turn amber) and place their finger. The LCD should then say either “Accepted” (top LED will turn green) or “Rejected” (top LED turns red). If accepted, the verification actions specified by the administrator will be executed. If rejected, the unit returns to its idle state.

V-Station models A-P, A-G and A-H can all initiate verifications by waving the appropriate card in front of the reader. There are some cases where the unit will indicate success immediately without the need to present a finger. See section 5.8 for details. There are various other modes that may vary this behavior slightly. Firmware versions 7.30 and above allow passwords, multiple fingers and duress modes. All of these are discussed in more detail below.

4. Administrator Mode

A wide array of administrative tasks can be taken care of directly on the V-Station via the keypad. Here, we describe how to access the administrative menus.

In order to enter administrator mode, a template with administrative privileges needs to be verified. If no such template exists, all users will be allowed into the administrative menus. V-Stations will be in such a state when shipped. The administrator will need to access the unit and enroll herself or himself as an administrator. This process is described in detail in the section describing the enrollment process.

When the unit is idle, it will display a splash screen with the date and time across the bottom. Pushing a numeric key will make that numeral appear as the first digit of the ID to be entered on a screen with the title "Enter Verify ID." To access the administrative menus from here, first make sure the ID reads "000" on this screen before pressing ENTER. If no administrator currently exists, the message "WARNING: No AdminID" will appear. Otherwise, the screen should display "Enter Admin ID." If you push the ENTER key when the splash screen is displayed, the unit will think you have entered no ID number and will display "Invalid ID" before returning to the splash screen.

If the unit discovers that the ID entered corresponds to a template with administrative privileges, it will show "Place Finger" and wait for a fingerprint. Otherwise, the unit will display the message "Rejected" and return to the splash screen. If a finger is detected and the verification is successful, the screen will show a series of menus. For full administrators, four entries will appear, "Template Admin," "Comm. Admin," "Security Admin," and "System Admin." For administrators with only enroller privileges (Admin level 1), two will appear, "Enroll (Add) User" and "Verify User" from the Template Admin menu.

5. Template Admin Menu

There will be either eight or nine options in this menu, Enroll (Add) User, Enroll (Add) Prox, Edit User, Delete User, Delete Prox Card, Delete Smart Card, Delete All Users, Verify User and Bypass Next Verify. Delete Smart Card appears only if your V-Station is an A-G (MIFARE) or A-H (iCLASS) model. This section describes each selection.

5.1 Enroll (Add) User

After selecting "Enroll (Add) User," the screen will show "Enter Enroll ID." The user may have any ID from 1 to 4,294,967,294. Entering an ID outside this range will result in an error and will return the user to the initial administrative menu. If an ID that is already in use is entered, the screen will display "User ID In Use, Are You Sure?" and "1) Acpt. 2) Rjct." on the bottom line. The default is to accept and if no input is detected, the unit will continue. If the ID is rejected, the unit will display "Rejected" and return to the top of the Template Admin Menu.

If the unit is currently using extended IDs, it will show "Enter Extended ID" after a valid ID is entered and accepted. Any value that is valid for the Wiegand format in use can be entered. Extended IDs have the added restriction that each ID/Extended ID pair must be unique. After a valid ID or ID/Extended ID pair is entered, the unit will show "Place Finger," indicating that the finger to be enrolled be placed on the sensor.

Quality and Content

When the finger is placed and the unit has processed the image, the Quality and Content scores will be displayed with stars. A choice to accept, reject or retry is also displayed. The quality score refers to image quality. Factored into this score are things like signal-to-noise ratio and contrast. When the image is good, more information can be extracted from it. Content refers to how unique an image is. The majority of the features that make a fingerprint unique are in the middle of the tip joint of a finger, where the ridges swirl around. If one were to take the edges of a finger, the ridges are very similar from person to person and do not convey much information, resulting in a lower Content score.

If the scores shown for these values are satisfactory, press 1 to accept. More stars represent higher quality and content, so a large number of stars is desirable. Scores of one or two stars should only be accepted in extreme cases. The values will range from one to five stars. Rejecting will take you back to the Template Admin menu. Retrying will return you to the "Place Finger" screen. A complete discussion of Quality and Content can be found in the *Veri-Series Operations Manual*.

Finger selection

The unit will then ask which finger to associate with the template, what security level to set it to and what administrative level to set it to. When the screen asks "Finger (0..9)," the user may enter a value between 0 and 9. The user may also decide not to make this association and hit ENTER. Looking at both hands, palms down, the numbering is from left to right. For instance, the left ring finger is finger 1, while the right middle finger is finger 7.

Duress Finger

The unit will now ask if the template being enrolled should be a duress template. When the screen asks "Duress Template? (0), (0) No (1) Yes," enter 1 to make the template a duress template or 0 for a normal template. Successful verifications of duress templates will result in bit-reversed Wiegand output. In order for this feature to take effect, the unit must be set to duress mode. If the unit is not in duress mode, a normal Wiegand string will be sent after a successful verification. A complete discussion of duress mode and templates can be found in the *Veri-Series Operations Manual.*

Access Schedule

If the unit has access schedules enabled, it will now ask which schedule to assign the template. The screen will show "Access Sched(0)," allowing values from 0 to 63. Schedules 59 through 62 are reserved for future use and should not be used. Schedule 0 will deny access for the template while access schedules are enabled on the unit. Schedule 63 will grant access. The user defines all other schedules. A complete discussion of access schedules can be found in the *Veri-Series Operations Manual.*

WARNING: the unit will look up all schedules. Undefined schedules should not be used. Unused schedules should be explicitly set to no access.

Security Level

The security level (screen shows “Security (0..6)”) must be between 0 and 6. A value of 0 means there is no security. Any finger will pass on templates with a 0 security setting. There is also an option to not even require a finger for templates set to security level 0. The values 1 to 5 are related to the likelihood of a false acceptance. Consequently, a larger security number (higher likelihood of false acceptance) relates to a lower security setting, with the exception of 0. So, by choosing 1 (“Very High”), the likelihood of false acceptance is minimized. If a user is having trouble at this security level, it could be lowered to any value from 2 (“High”) to 5 (“Very Low”) as the administrator sees fit. Though the chance of a false acceptance is higher at these values, it will be easier for the legitimate user to pass (see Section 7.3 for details on how this is affected by the unit’s global security level). The default value is 3 (“Medium”) and can be selected by pressing the ENTER key immediately upon entering this screen. Unlike administration levels (see below), it is possible to assign different security levels to templates that have the same ID.

Security level 6 indicates that the unit should bypass biometric verifications for the template, but require a password. Such templates must be used on V-Stations since there is no mechanism for entering a password for other products. A complete discussion of the Security Level can be found in the *Veri-Series Operations Manual*.

Security Level is also not an option on searching units (A-S model). The thresholds for acceptance are inherently assumed by the searching algorithm.

Administration Levels

There are three levels of administration, to be set when the screen shows “Admin (0..2).” Level 0 corresponds to an ordinary user. They may verify, but are not allowed to access any administrative functions. Level 1 corresponds to an enroller. These templates are allowed to add users to the system and verify existing users. However, they can only add users with no administrative privileges (Admin Level 0) and can not access any other administrative functions. Level 2 administrators have full access to the entire unit. The default value is 0 and administrators can select this value by pressing the ENTER key immediately upon entering this screen. Administrators of level 1 can only enroll ordinary users.

If an administrator is enrolling a template to an ID that has already been assigned on the unit, the new template will be assigned with the ID entered and the lowest available index. When adding a template in this manner, the administration level of all templates with the same ID must be the same. Typically, an ID is associated with a person whose administrative privileges do not change. Any attempt to enroll a template to an ID with a different administration level than the current templates associated with that ID will result in the message "Admin mismatch" being displayed and the unit returning to "Enroll (Add) User."

Password

The unit will now ask for a password to be assigned to the template (screen shows "Enter PW"), but only if the Wiegand format in use does not use extended IDs. For this release, the use of passwords and extended ID Wiegand formats are mutually exclusive. Any value from 0 to 4,294,967,295 can be entered and will be placed in the password field of the template (0 is default). If a unit has password mode enabled, verification actions will only take place after a password is entered. A template with a password of 0, however, will not require a password. It is up to the administrator to ensure that templates have non-zero passwords if this level of protection is desired.

Password mode is available on searching units (A-S model). However, only 1-to-1 verifications will ask for it. Successful searches (1-to-many) will not require a password to initiate verification actions.

Saving to Smartcard

For V-Station models A-G (MIFARE) and A-H (iCLASS) only, the next screen will ask where to save the template, showing the text "Store Template To 1)Unit or 2) Smartcard." The default is to store the template to the unit. If this is chosen, the unit will store the template, showing "Stored" and proceed to the Alternate Fingers screen. If the template is to be stored onto a smartcard, the unit will prompt the user with "Enter Key." If the key entered does not match the one on the unit, "Invalid Key" will be displayed and the unit will return to the Template Admin menu. If the key is valid, the unit will prompt the user again, this time with "Present Card." When a card is detected, the unit will inform the user with "Card Detected" and store the template to the smartcard. If any errors occur, a descriptive message will appear on the screen and the user will be returned to the Template Admin menu. Typical messages include "Card Full" and "Invalid Key." Even if the key entered matches the one on the unit, it may not match the one on the smartcard. In order to successfully store a template to a card, it must match both. Upon success, the unit will display "Stored" and proceed to the Alternate Finger screen.

Alternate Fingers

At the end of the enrollment process, the unit will ask to enroll an alternate finger. It is advisable to do so. This way, in the event of an injury (such as a cut or scratch) to one finger, another may be used to gain access. The procedure is identical to initial enrollment except that it starts at the "Place Finger" screen.

5.2 Enroll (Add) Prox

After selecting "Enroll (Add) Prox," the screen will show "Swipe Card" on the first line and "External Reader" on the second. Since the A-P model has an internal prox card reader, the second line will not be shown for that model. If a prox card is successfully detected, the screen will show "Card ID is" on the first line, the value read from the prox card on the second line and "1)Acc 2)Rej 3)Retry" on the third line. Accepting takes you to the "Place Finger" screen of the regular enroll process. Rejecting takes you back to the Template Admin menu. Retrying returns you to the "Swipe Card" screen.

5.3 Edit User

After selecting "Edit User," the screen will show "Enter Edit ID." When an ID is entered, the screen will show "Enter Template Index." After the index is entered, the unit will look for a valid template with that ID-Index pair. If one is found, the template can be edited. The screen sequence is identical to the enrollment procedure, from "Enter Finger" to "Enter Password." If the ID-Index pair is not found on the unit, the screen will show "Invalid ID" and return to the top of the Template Admin menu.

5.4 Delete User

After selecting "Delete User," the screen will show "Delete Template ID." The screen will then show "Enter Template Index" after an ID has been entered. An index is not required here; if the administrator pushes ENTER with no data, the template with the lowest index value will be selected. If the ID-Index pair corresponds to a valid template, the screen will show "Deleted." If the ID-Index pair does not correspond to a valid template, the screen will show "Deletion Failed." In both cases, the screen will ask for another template to be deleted. Either the process can be repeated or CLEAR can be used to back out to the Template Admin menu.

5.5 Delete Prox Card

After selecting "Delete Prox Card," the screen will show the same "Swipe Card" screen that the Enroll (Add) Prox menu item begins with. If a Wiegand string is successfully read to the unit, it will prompt the user with "Delete All Instances of" followed by the ID of the Wiegand string and "1)Acc 2)Rej 3)Retry." Accepting will attempt to delete all templates with the associated ID. If successful, the unit will display "Deleted"; otherwise, "Delete Failed" will be displayed. Rejecting will take you back to the Template Admin menu. Retrying will return you to the "Swipe Card" screen.

5.6 Delete Smart Card

After selecting "Delete Smart Card," the unit will display "Enter Key," the same as when enrolling or storing to a smart card. If the key entered does not match the one stored on the unit, "Invalid Key" will be displayed. Otherwise, it will display "Present Card" and reply with either "Card Detected" or "Card Not Found," whichever is appropriate. If a card is found, the next screen will display "Del All Fingrprnts" followed by "1) Yes 2) No." Cards with no templates will result in the unit displaying "Card Empty" and returning to the Template Admin menu. Selecting "No" will also return the user to the Template Admin menu. If the user selects "Yes," the unit will display "Present Card" followed by either "Card Detected" or "Card Not Found." If the card is found, the unit will attempt to delete all templates and Wiegand strings from the card. The unit will display "Deleted" or "Delete Failed," whichever is appropriate and return to the Template Admin menu. If at any time in the process, the ESI fails to respond, the unit will display "ESI Not Responding" and return to the Template Admin menu.

5.7 Delete All Users

After selecting "Delete All Users," the unit will display "Are You Sure?" Press 1 to accept or 2 to reject. If 1 is selected, the unit will attempt to delete all the templates and display "Deleted" upon success or "Delete Failed" otherwise. If 2 is selected, the screen will display "Rejected." In all cases, the unit will return to the Template Admin menu.

5.8 Verify User

After selecting "Verify User," the unit will display "Enter Verify ID." If a valid ID is entered, the unit will display "Place Finger." When the verification completes, the result will be shown on the LCD. If the unit is in default mode, verification actions will be initiated. The various modes and their effect on the verification process are discussed below. If an invalid ID is entered, an error will be displayed and the unit will return to the "Enter Verify ID" screen.

Two modes of operation enhance security for verifications. These are passwords and access schedules. If password mode is turned on, the unit will show "Enter PW." If the password entered matches the value stored in the template, the screen will show "Accepted" and return to the "Enter Verify ID" screen. In addition to passwords, access schedules can be enabled and disabled. Each template has a schedule associated with it. If access schedules are turned on, the unit will check the schedule specified in the template (the actual schedules are stored on the unit). If the user is not allowed at the moment, the screen will show "User Not Scheduled" and return to the "Enter Verify ID" screen.

There is also a mode where the unit requires multiple fingers to successfully verify before showing "Accepted." The "Verify User" menu option ignores this mode.

Two modes of unit operation can disable biometric verification, the global biometric mode and the biometric schedule. The global mode ignores the time. The schedule allows the unit to turn the mode on and off at specific times. If a unit either has the global biometric mode disabled or is not currently scheduled to require biometrics, it will simply check if the ID entered is associated with an enrolled template. If so, the unit will display "Accepted" without requiring a finger.

Two values of template security level also allow a user to bypass biometrics. If a template's security level is set to 0, no biometrics will be performed. However, it may require a finger to be presented anyway, in which case, it will display "Place Finger."

When a finger is placed, the screen will show “Accepted” and will return to the “Enter Verify ID” screen. If no finger is required, the screen will show “Accepted” without the “Place Finger” screen and return to the “Enter Verify Screen.” The setting that determines whether or not a finger is required is not accessible from the menu system in this version of firmware and must be set via VeriAdmin. Security level 6 also allows a user to bypass biometrics. However, this mode requires a password, regardless of what the unit's password mode is set to. When the unit is presented with a template of security level 6, it will prompt the user with “Enter PW.” If the value entered matches what is stored in the template, the screen will show “Accepted” and return to the “Enter Verify ID” screen.

There is also Custom Verification Entry mode, which does not affect security in terms of verification actions, but puts extra information in the Transaction Log. See Section 8.6 for details.

5.9 Bypass Next Verify

After selecting “Bypass Next Verify,” the unit will immediately display “Next Ver BYPASSED!” This allows the very next verification (however it is initiated) to bypass access schedules, which need to be carefully distinguished from biometric schedules.

6. Comm. Admin Menu

There are four options in this menu, Ethernet Options, Serial Comm., Wiegand Admin and Verify Actions. Ethernet Options contains three items. Serial Comm. contains five items that each performs a specific task. The Wiegand Admin menu's tasks are nested slightly deeper. And Verify Actions has three settings.

6.1 Ethernet Options

Within this menu are three submenus, “IP Address,” “Show IP Address,” and “Drop TCP Connection.”

IP Address
After selecting “IP Address,” the unit will display “Set IP Address” followed by the current IP Address in dotted decimal notation. The desired IP can be entered in the same notation. If a valid address is entered, the screen shows “Stored” and returns to the “Set IP Address” screen, displaying the address just entered.

Show IP Address
After selecting “Show IP Address,” the unit will display “Show IP Address” followed by the current IP Address. The advantage to using this selection rather than the “IP Address” menu item above is that this one will display the IP address assigned to the unit. After a few seconds of displaying the IP address, the unit returns to the “Ethernet Options” menu.

Drop TCP Connection
After selecting "Drop TCP Connection," the unit will ask, "Are You Sure?, 1) Acpt. 2) Rjct." Rejecting will cause the unit to display "Rejected" and return to the Ethernet Options menu. Accepting will force the unit to attempt to drop all open TCP connections. The unit will display "TCP Conn. Dropped" upon success and "TCP Drop Failed" upon failure. In either case, it will return to the Ethernet Options menu.

6.2 Serial Comm. (baud rate, protocol, password protection, net ID)

Within this menu are three menus, "Host Port Baud Rate," "Host Port Protocol," and "Change Net ID." Each of these menu items is described below. For firmware version 7.20, the Aux port baud rate is set to 57,600 and can not be changed.

Host Port Baud Rate
After selecting "Host Port Baud Rate," the unit will display "Enter Baud Rate" followed by the current baud rate. When a baud rate is entered, the unit first checks to see if it is valid. If it is, the baud rate is changed and a confirmation message appears. Supported baud rates are 57,600, 38,400, 19,200 and 9,600.

Host Port Protocol
After selecting "Host Port Protocol," the unit will show "Enter Protocol" and the current protocol. Select 1 for RS-232 and 2 for RS-485. Unlike many of the menus that present "Accept" and "Reject" as options, the user must hit ENTER after making a selection in this menu. After selection, "Stored" should appear on the screen, confirming that the desired protocol has been selected.

Change Net ID
After selecting "Change Net ID," the unit will display "Enter Net ID" followed by the current net ID. Any number valued 0 to 65,534 is a valid net ID. After entering the net ID, the unit checks that the value entered is in range. If it is, it sets the unit's ID, displays the "Stored" confirmation message and returns to the "Enter Net ID" screen.

6.3 Wiegand Admin (predefined formats, options, enable)

This menu has 3 submenus, "Defined Settings," "Other Settings," and "Disp Wiegand Format." The first two have submenus, with "Defined Settings" containing "Defined Formats" and "Defined Options," while "Other Settings" has "Wiegand Input" and "Wiegand Output." Each of these and the menus beneath them are described here. "Disp Wiegand Format" has no submenus, but is also described below.

Defined Settings: Defined Formats
In this menu is each of the seven defined formats that can be found in the "Unit Parameters" dialog box of VeriAdmin. Selecting any one of these menu items will set the Wiegand format to the one specified. Defined formats currently supported are the industry standard 26-bit format, Apollo's 44-bit format, Northern's 34-bit format (with

and without parity), Ademco's 34-bit format and HID's Corporate 1000 format (35-bit) and their 37-bit format. If the format is successfully set, a confirmation message appears.

Defined Settings: Defined Options
Three options are currently supported, each with a menu item here, "Failstring," "Alternate Sitecode" and "Invert Parity." The first will show "Set Fail Str(0:off)"; and the second will show "Set Alt Site(0:off)." Both will show the current setting, 0 for disabled or 1 for enabled. If enable is selected, the next screen will ask the user to enter a numeric string to use as the value for the particular feature. The ranges for both are 0 to 4,294,967,295. Parity inversion is a simple toggle. The screen following the selection of this menu item will display the current setting. Enter 1 to change it.

The "Failstring" option is used when it is desirable to output a Wiegand string even when verification fails. If this is initiated, the string stored as the "Failstring" in memory will be substituted for the ID field in the Wiegand string.

"Alternate Sitecode" is generally recommended only for searching devices. If this feature is enabled, the Wiegand string that is output will have the stored sitecode inserted.

"Invert Parity" is also only used when the verification fails. If changing the ID in the Wiegand string produces undesirable side effects, inverting the parity is another way to communicate a failed verification to a device connected to the V-Station's Wiegand output.

For both the Failstring and Alternate Sitecode, numeric entries from the keypad will allow 32-bit numbers (up to 4,294,967,295). This differs from VeriAdmin. Using numbers that exceed the limits of the current Wiegand format will result in unpredictable behavior.

Other Settings: Wiegand Input, Wiegand Output
After selecting one of these menu items, the screen will display "Toggle Input Enable" for "Wiegand Input" or "Toggle Output Enable" for "Wiegand Output." The current status of input (enabled or disabled) will also be displayed. Press 1 to toggle. CLEAR will exit the menu with no change.

From the V-Station menu system, enabling Wiegand output means that the unit will always send a Wiegand string upon successful verification, regardless of how it was initiated. In VeriAdmin, there is an option to send the Wiegand string only if the verification was initiated by a Wiegand device. That option is not currently available from LCD menus.

Disp Wiegand Format
After selecting "Disp Wiegand Format," the unit will display the name associated with the current Wiegand format. If the format is either the pass-through format or auxiliary format, "Pass Through," or "Auxiliary Format" will be displayed, respectively. The

format will be displayed for a short time and the screen will subsequently return to the Wiegand Admin menu.

6.4 Verify Actions (Host Port, Aux Port and GPIO)

This menu has 3 submenus, "Set Host Port," "Set Aux Port" and "Set GPIO." After selecting one of these menu items, the screen will display "1) Enable 2) Disable" and whether the particular output port is enabled or disabled. For all three ports, "Accepted" will be shown if a valid value is selected. "Rejected" will be displayed if an invalid value is entered. The lone exception is if GPIO is enabled. In this case, the screen will prompt the user to set the duration for the GPIO line with "Duration (s,1-30)" followed by the current setting. If the value entered by the user is in range, "Accepted" will be displayed. Otherwise, "Rejected" will be displayed. For both accepted and rejected settings in all three menus, the unit will return to the "1) Enable 2) Disable" screen, confirming the user's choice.

From the V-Station menu system, enabling the host or aux port will send the ID in the outgoing packet. When using VeriAdmin, there is the option to not send the ID. This is not currently available from LCD menus. Specific implementation details can be found in the *Serial Command Interface* and *DLL Manual* documents that come with the SDK. Also note that VeriAdmin refers to GPIO as "Line Trigger" in its Verification Action Response dialog. The menu system's "GPIO" refers to exactly the same thing as VeriAdmin's "Line Trigger" and changes to one will be reflected in the other.

7. Security Admin

7.1 Biometric

When this menu is selected, the screen will display "(1)On (2)Off." The administrator simply selects whether biometrics are to be turned on or off. If turned off, the unit will still check incoming ID's to see if they correspond to valid templates. However, it will not require that a finger be presented to initiate verification actions.

7.2 Aux Port Disable/Aux Port Enable

Depending on the current state of the aux port, either "Aux Port Disable" or "Aux Port Enable" will appear in the Security Admin menu. If enabled, the menu will show the disable option. If disabled, the menu will show the enable option.

If "Aux Port Enable" was initially shown, the unit will display "Enter PW" and wait for user input. Upon receiving input, the unit will check the value entered against the stored password. If the two match, the port will be re-enabled. Otherwise, an error message will appear.

If "Aux Port Disable" was initially shown, the unit will display "Enter PW" and wait for user input. Any number valued 1 to 4,294,967,294 is a valid password. If the value 0 is entered, the aux port subsequently can not be enabled with a password as described above. The only way to enable it is through either the host port or via Ethernet.

7.3 Set Global Security

When this menu is selected, the screen will display "Security (1..5) (3)." If the administrator wishes to change the setting, it should be entered here. Otherwise, hitting ENTER will leave the setting at its current value. As with the security setting for templates, the global security setting is directly related to likelihood of false acceptance. When verifying a template, the unit takes the higher setting between the template and the global security and adjusts the threshold for verification accordingly. This way, if many users are having problems verifying successfully, the entire system can be set to a higher security setting (lower security level) without the requirement of editing each template individually. NOTE: Currently, hitting CLEAR will not back the unit out of this screen.

7.4 Duress Mode

When "Duress Mode" is selected, the screen will show "1)On 2)Off." Entering a 1 or 2, then pressing ENTER will turn duress mode on and off, respectively. Entering any other value will result in "Rejected" being displayed and not affect duress mode on the unit. After the duress mode has been set, the unit will return to the Security Admin menu.

In duress mode, when a duress template has successfully verified, the Wiegand output string is bit-reversed (other actions may be made possible in the future). If the mode is turned on, but the verified template is not a duress template, verification actions will proceed normally.

7.5 Access Schedule

When "Access Schedule" is selected, the screen will show "Acces Sched En (1)." Entering a 0 will turn off access schedules. Entering a 1 will enable access schedules. Turning access schedules on is the default. This selection is a hot key, so pressing ENTER is not required. Selecting a number other than 0 or 1 will have no effect. After the unit receives the choice, it will either display "Stored," if it was successful in setting the parameter, or "Storage Failed," if it was not.

7.6 Multi-finger Options

When "Multi-finger Opts" is selected, a submenu with two entries will appear, "Fingers" and "Timeout." After selecting "Fingers," the screen will show "Set Num Fingers" and the user can either require a single finger by entering 1 and pressing ENTER or two fingers by entering 2 and pressing ENTER. After selecting "Timeout," the screen will show "Set Timeout(1-30)" and the user can set the timeout. Neither of these entry screens is a hot key and 0 is not a valid value. If 0 is entered or anything larger than 2 for "Fingers" and 30 for "Timeout" is entered, the unit will show "Invalid Value" and return to the "Multi-finger Opts" submenu. If the settings could not be stored, "Storage Failed" will be displayed. Otherwise, the unit will have saved the new settings and show "Stored."

When the number of fingers is set to 2, the unit will require two successful biometric comparisons before verification actions are taken. The two comparisons can have any combination of input sources and can even mix identifications (1-to-many) with verifications (1-to-1) on searching units. After the first successful comparison, the green LED will flash quickly before the unit returns to waiting for input. If the next successful comparison takes place within the timeout specified, verification actions will be initiated. The two users can not have the same template ID. The only time an action will be taken after a single successful comparison is when it is initiated from either serial port or Ethernet. In this case, a reply will be sent on that port, but no other actions will be taken.

7.7 PW Mode

When "PW Mode" is selected, the screen will show "Mode (0 Off, 1 On)." The mode can then be set by selecting 0 for disable or 1 for enable, followed by ENTER. When password mode is on, the unit will query, upon successful verification, the user for the value in the password field of the template. Verification actions will only be initiated after it is confirmed that the value entered matches that in the template. If the password stored in the template is 0, the unit will not ask for a password no matter what is stored for this setting.

8. System Admin

The remaining miscellaneous administrative functionality resides here. There are six menu items, "Contrast Control," "Set Time/Date," "Transaction Log," "Erase Verify Queue," "Set Factory Defaults" and "Change CVE Mode."

8.1 Contrast Control

Upon selecting "Contrast Control," the screen will respond by displaying "Enter Contrast" on the first line, "25 <- Contrast <- 65" on the second line and wait for administrator input. After getting input from the administrator, the unit checks the value to make sure it is in range (25 to 65). If not, an error message is shown. Otherwise, the contrast on the screen is adjusted and a confirmation message appears. The default value is 40. Values near this default generally look best, though ambient lighting conditions should be taken into account.

8.2 Set Time/Date

This menu has two submenus, "Set Time" and "Set Date." When "Set Time" is selected, the screen shows "Enter Time" followed by the time format and the current time, then waits for input. If the input is valid, the time is set and a confirmation message appears. Otherwise, an error message will appear. Setting the date with the "Set Date" menu is identical except that it shows “Enter Date” followed by the date format and current date. Invalid values are anything that is out of range (e.g. entering 15 for the month or 98 for the hour). Entering values out of range will result in the screen showing “Rejected.”

8.3 Transaction Log

This menu has two submenus: “Erase Log (All)” and “Erase Log (Read).” Both will prompt the administrator with the message “Are You Sure?” If the administrator rejects erasure, a message will appear and the screen will return to the Transaction Log menu. If the administrator accepts erasure, the entries in the Transaction Log will be erased. “Erase Log (All)” completely erases the entire transaction log. “Erase Log (Read)” only erases the entries of the transaction log that have been marked as read.

The transaction log is stored in flash and contains much more information than the verification queue and holds many more events. Additional information includes, but is not limited to, timestamps, deletion events and source ports. A complete discussion about the transaction log can be found in the *Veri-Series Operations Manual*.

8.4 Erase Verify Queue

When “Erase Verify Queue” is selected, the unit will flush all the entries from the verification queue and display “Erased.”

The verification queue is an 8-entry queue of the most recent events involving enrollment or verification. Due to its size and limited information, it is intended for polling applications to discover what is in the queue quickly, before an overrun occurs. Developers wishing to use the verification queue will need to obtain the SDK and refer to the *Serial Command Interface* and *DLL Manual* documents included with it.

8.5 Set Factory Defaults

This menu has three submenus, “Reset Parameters,” “Set RS-232 Defaults” and “Set RS-485 Defaults.” Selecting “Reset Parameters” will set many of the parameters of the unit to factory defaults. In addition to resetting the serial ports as described below, parameters such as Wiegand format and net ID are returned to the values that were set when the unit was shipped. Selecting “Set RS-232 Defaults” will reset RS-232 communications settings. These settings are 57,600 for both the host and aux port baud rates, RS-232 for the host port protocol and enabling the aux port with no password protection. Selecting “Set RS-485 Defaults” will reset RS-485 communications settings. These settings are 9,600 baud for the host port, 57,600 baud for the aux port, RS-485 for the host port protocol and enabling the aux port with no password protection. After selecting any of these, the screen will show “Factory Defaults Set” and return to the menu selected by “Set Factory Defaults.” If the user sees any other message, there is something very wrong with the unit and Bioscrypt tech support should be contacted.

8.6 Change CVE Mode

This menu affects Custom Verification Entry mode (CVE) and has no submenus. When it is selected, the unit immediately displays “Mode On (1) Off (0)” on the top line and displays the current status of the mode (0 for disabled, 1 for enabled) on the second line. The user can then enter the desired value (0 to disable or 1 to enable), after which the unit will display “Stored.” If any other value is selected, the unit will display “Invalid Value.”

When CVE mode is turned off, verification will not be affected. The normal set of menus is displayed and the verification actions currently set on the device will be triggered.

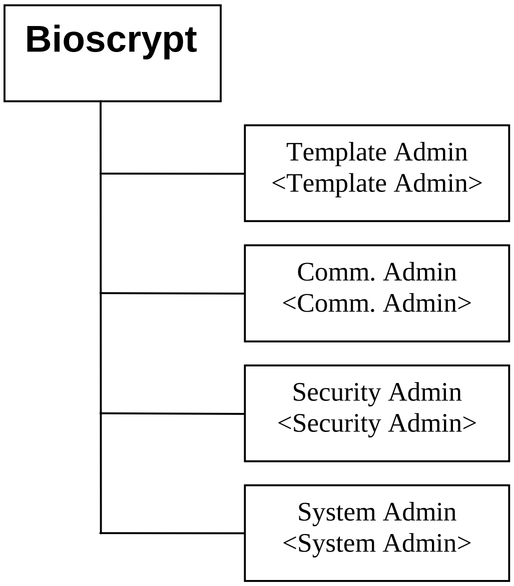
When CVE mode is turned on, two things happen that are different from a normal verification. First, the **line trigger** and **Wiegand** outputs are suspended momentarily. All other verification actions, however, proceed as normal. Second, the unit requests one additional piece of information from the user. Just before “Accepted” would be displayed in the normal verification process, the unit will query “Enter Entry Code.” Valid values for this code range from 0 to 249. Values 250-255 are reserved for the unit to report various occurrences. When the code is entered, the line trigger will then fire. The value entered by the user will also be written to the Transaction Log under the “Code” column. If a timeout occurs while waiting for user input, the number 255 will be written to the Transaction Log. At this point, the unit should display “Accepted” on the LCD screen regardless of whether there was a timeout or not.

Though the line trigger and GPO0 use the same hardware, CVE mode only affects actions specified to “Line Trigger,” found in the “Misc” tab of the Unit Parameters dialog in VeriAdmin. Any actions specified in the “General Purpose I/O” tab of the Unit Parameters dialog will not be affected.

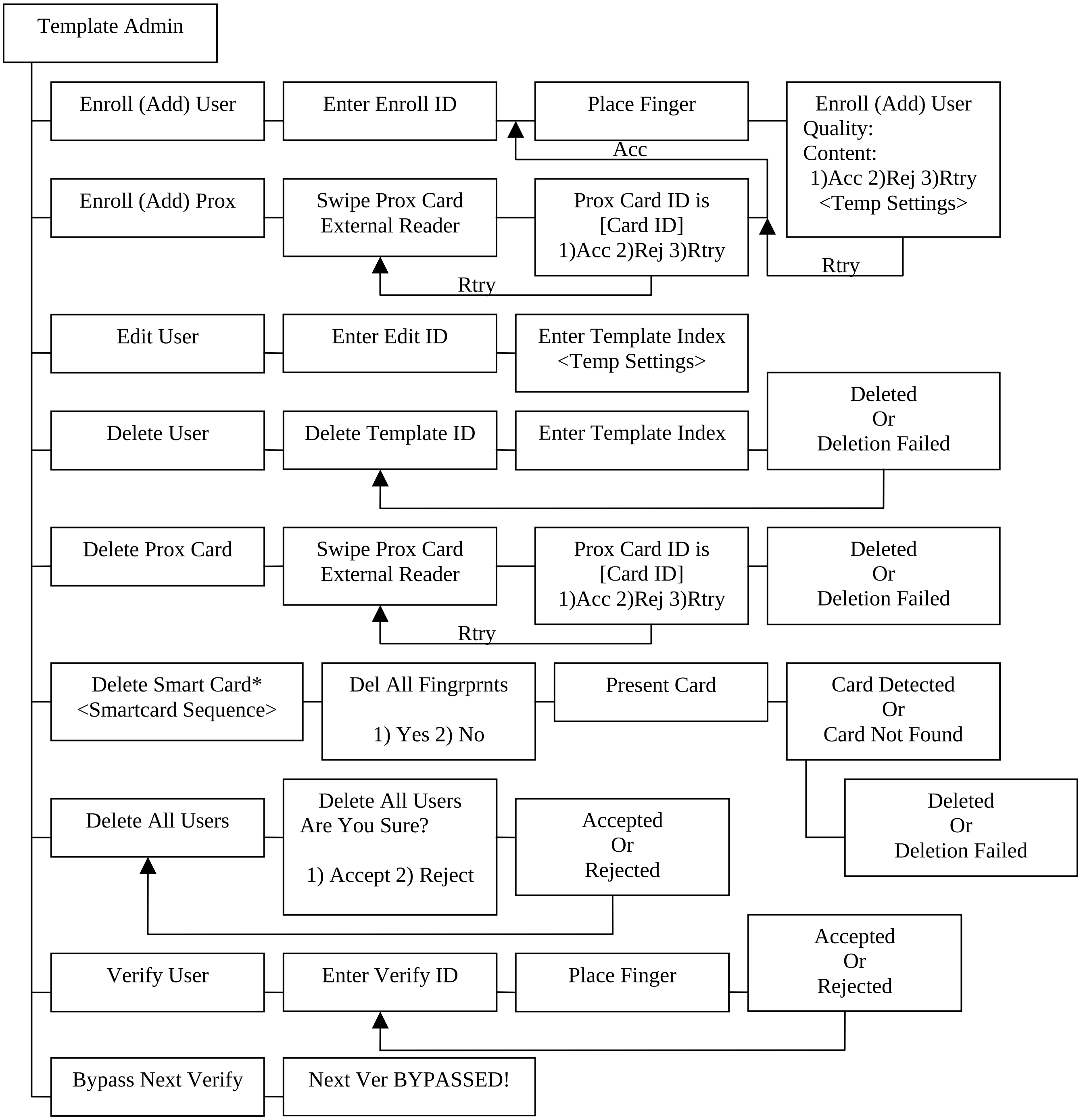
9. Menu Tree

The following diagrams show the entire menu structure in schematic form. Menus progress from left to right. Where applicable, screens that jump back multiple screens are indicated. When menus are fully described, the text displayed is shown and angle brackets (<>) surround the title of the section that describes the menu that results when that item is selected or valid data is entered.

9.1 Initial Administrative Menu

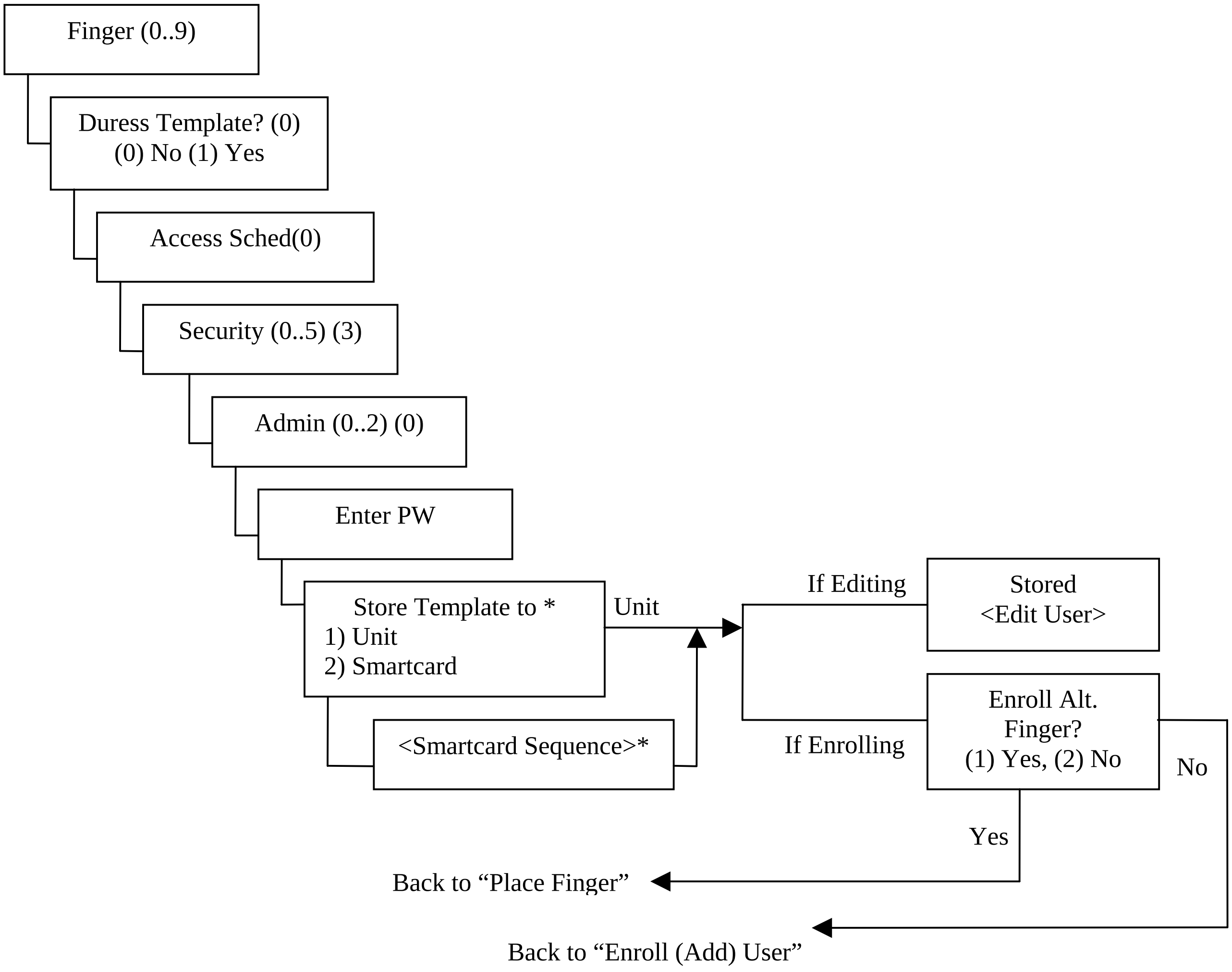


9.2 Template Admin Menu



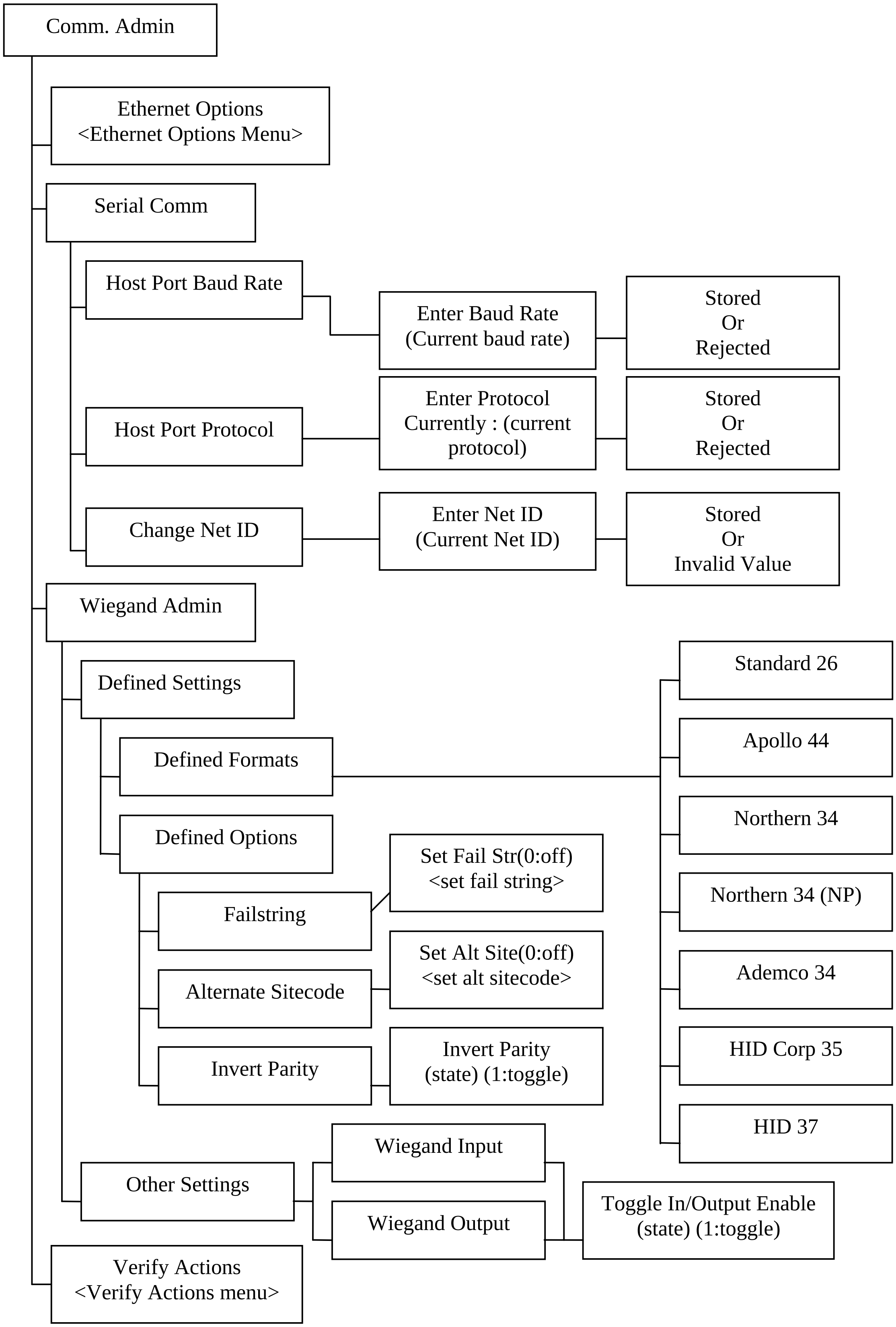
* Menu available only on V-Station models A-G (MIFARE) and A-H (iCLASS)

9.3 Template Settings Sequence

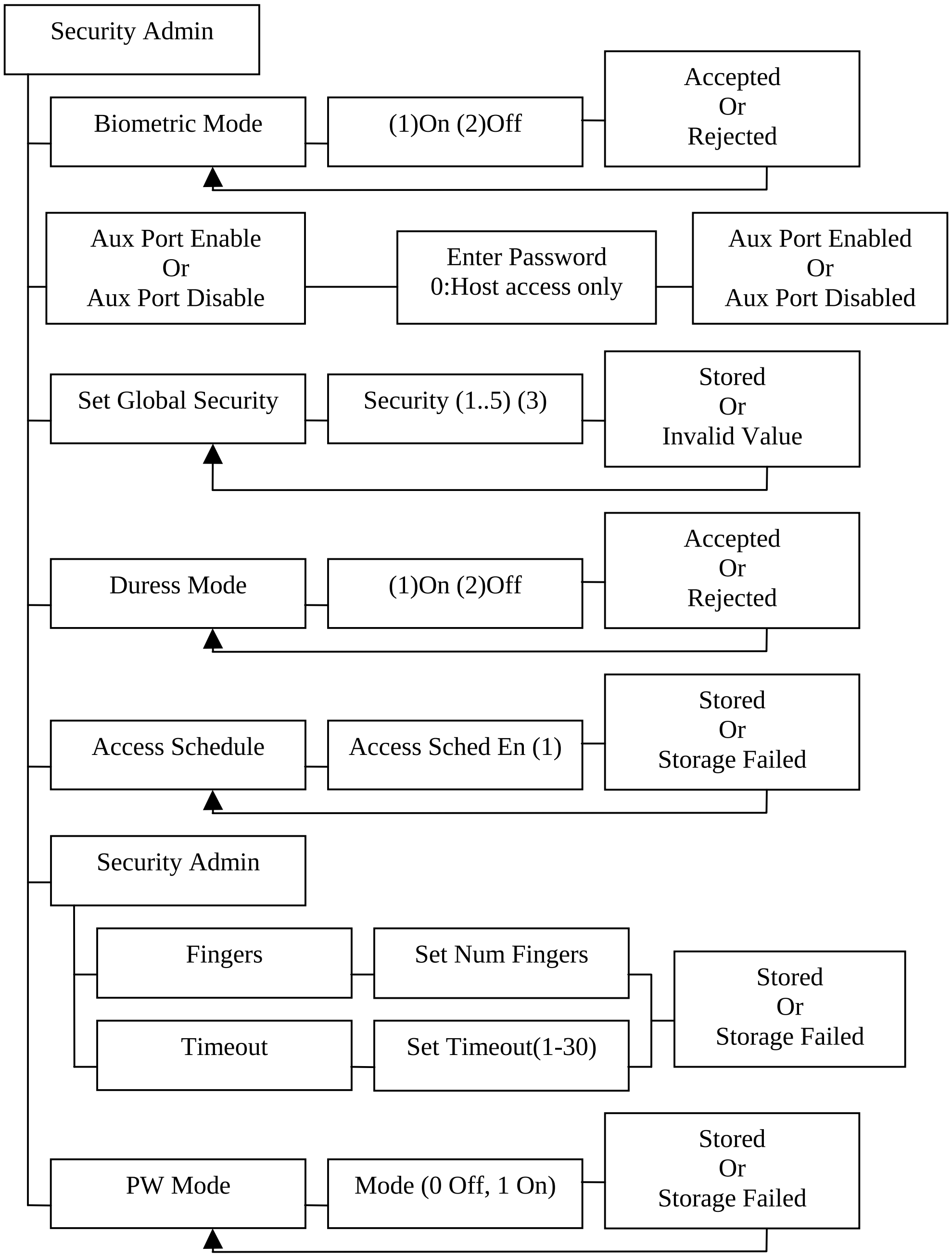


* Menu shown only on V-Station models A-G (MIFARE) and A-H (iCLASS)

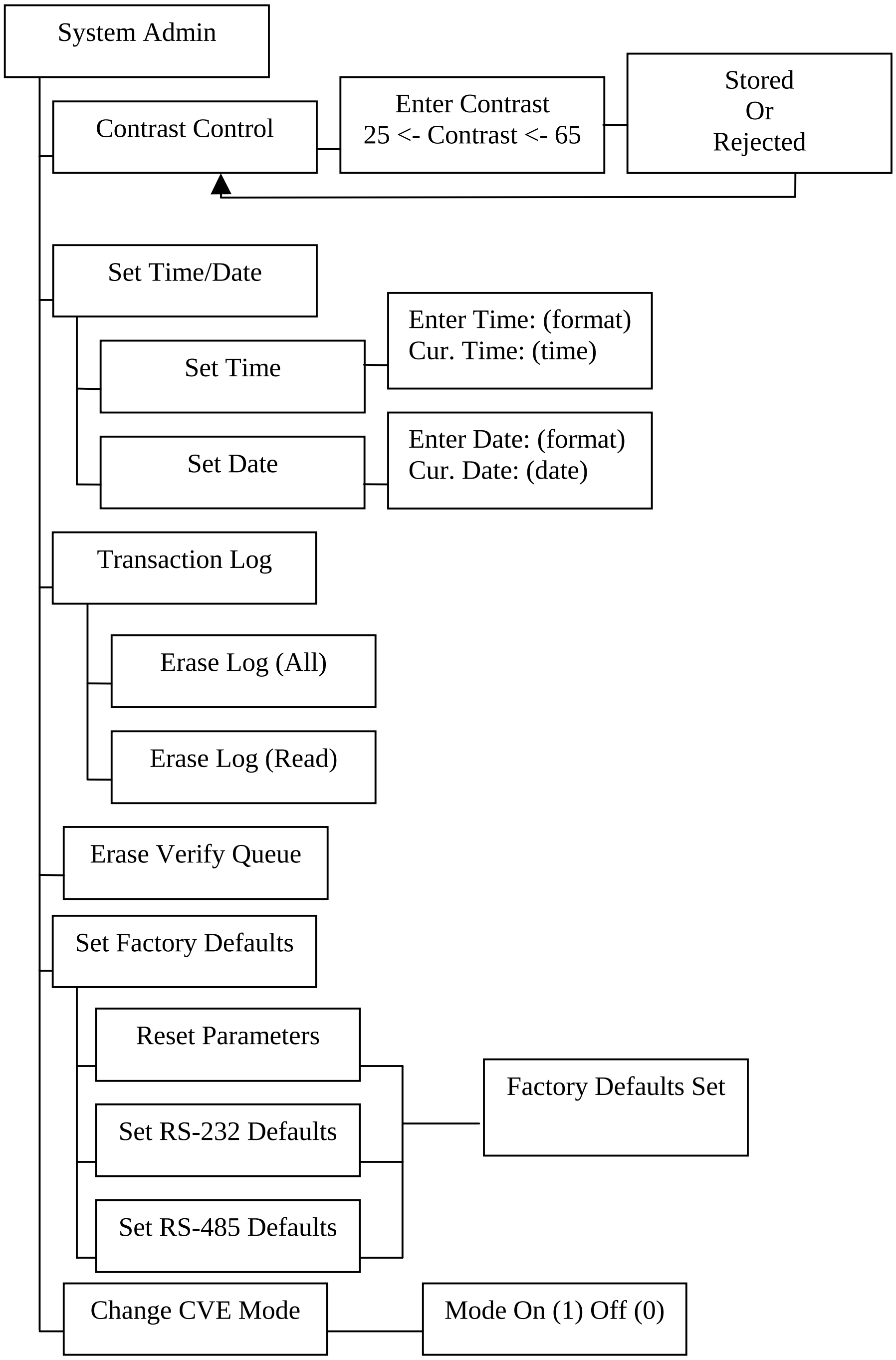
9.4 Comm. Admin Menu



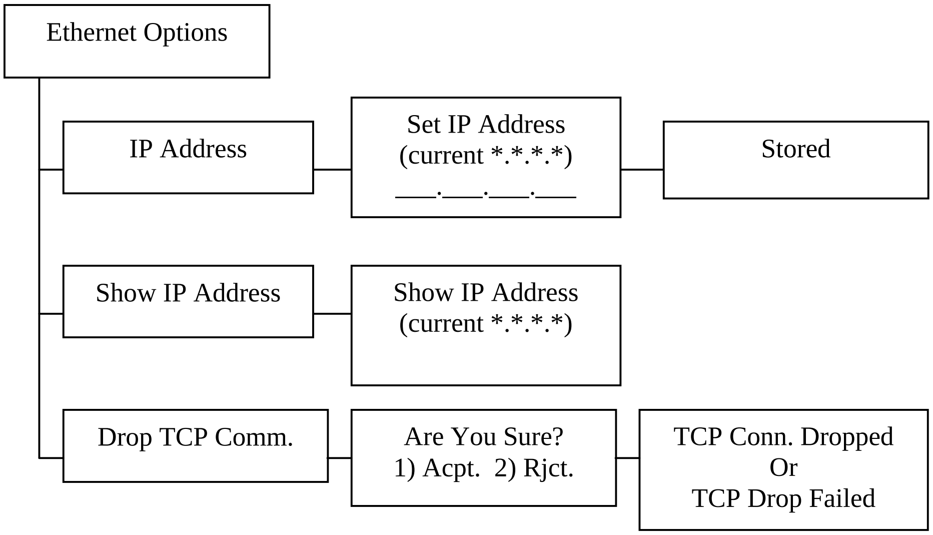
9.5 Security Admin Menu



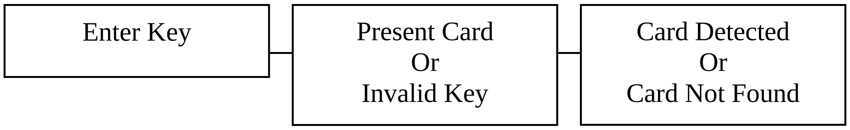
9.6 System Admin Menu



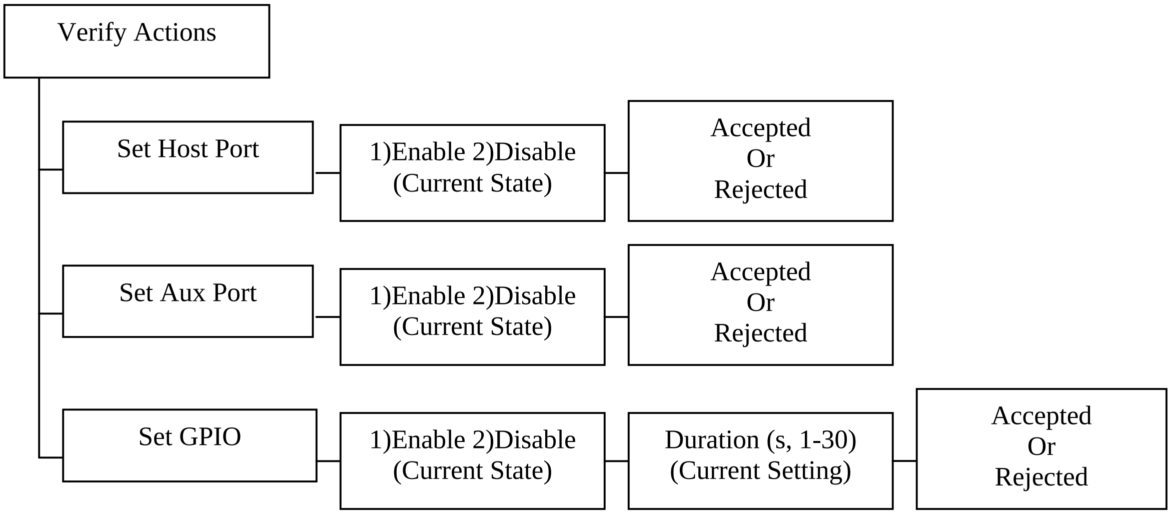
9.7 Ethernet Options Menu



9.8 Smart Card Sequence



9.9 Verify Actions Menu



10 Bioscrypt Contact Information

Technical Support Contact Information:

Telephone:	866.304.7180 (toll free) 818.304.7180 (direct)
Fax:	818.304.7187
Email:	support@bioscrypt.com
Web:	http://www.bioscrypt.com
Hours:	5:30A – 5:00P PST (Monday – Friday)
Address:	Bioscrypt Inc Technical Support Dept 5805 Sepulveda Blvd, Suite 750 Van Nuys, CA, 91411

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