

PIV INFORMATION AND TROUBLESHOOTING STEPS– **Must Read**

Rev F.

GENERAL INFORMATION:

1) PIV cards are government issued cards. There are different types.

- FIPS – Federal Information Processing Standard
- TWIC – Transportation worker identification credential
- FRAC – First Responder Authentication Credential
- CAC - Department of Defense

2) Before selecting a reader, you must know some information in regard to your government issued card. You should know the format and some of the internal information such as the agency code and site code.

3) The CA3000 has a few PIV formats built in. The most common format is the 75 bit format PIV format (PIV MSB).

4) Unlike standard hid prox readers and prox cards, you must select the correct PIV reader to match your specific PIV format. If the PIV Cards are a 75 bit format, you must purchase a PIV reader that is programmed to output a 75 bit format.

TROUBLESHOOTING STEPS FOR PIV READERS AND CARDS:

- 1) You must verify the reader is a PIV reader. As of mid 2011, all Exceed readers are PIV compatible.
- 2) As of January 2011, the two controllers that support PIV are the Accelerator and the SuperTwo. The SuperTwo requires the PIV feature to be purchased and the security key must have it enabled.
- 3) It is very important to have the correct firmware in the panels. If the updated firmware is not downloaded to the panel, you might get erroneous errors such as “Badge Violate Unauthorized” or “Badge Violate Facility”. Below is the correct firmware information.

<u>Panel</u>	<u>CA3000 version</u>	<u>Firmware version</u>
Accelerator	V2.6.19x	A10518
Accelerator	V2.7.19	A40020 (Do not use this on previous versions)
Accelerator	V2.7.26	A40028 (Do not use this on previous versions)
Accelerator	V2.8.x	A40028
SuperTwo	V2.8.x	S2 40045

Notes: You must purchase licensing for PIV support on a SuperTwo.

- The default firmware in the accelerator board will have a number similar to A1Axxx. Do not use this. You must do a firmware download with the above firmware versions.
- If you are using a SuperTwo, you need to contact Continental Technical Support for an updated firmware image.

4) You must verify the PIV reader acknowledges the PIV card when it's presented to it. You must hold the card against the reader for at least 10 seconds. The PIV reader will beep if it acknowledges the card. If the reader doesn't acknowledge the card, the reader might not be the correct type.

5) PIV cards are very secure and contain a lot of data. The data transferred between the reader and card is much greater than a standard prox card. This is why the authentication process takes much longer than a standard prox card.

6) If the PIV card is acknowledged by the PIV reader, you should hear a quick beep. If this occurs, you should see an alert display on the CA3000. If no alert displays on the CA3000, you must verify the PIV badge format in the CA3000 matches the format of your PIV readers (ex. 75 bit, 200 bit).

7) If you purchased a 75 bit Exceed-ID PIV reader, you should select the "PIV MSB" format in the CA3000 software. This is the 75 bit PIV format.

8) The parity information for the "PIV MSB" format is incorrect in CA3000 version 2.7.19 and earlier. Change the parity bits as follows:

Offset	Length
--------	--------

Even	0,	38
Odd	38,	37

Note: Without this parity change, you might experience some badges not working.

9) If you do not know the agency code, site code or other fields in the PIV card, you can modify the badge format temporarily to see the information on the screen.

Procedure to determine data in the PIV card and display it:

Modify the badge ID bits in the correct format (75 or 200). To determine the agency code, you swap the badge Id bits with the Agency code bits. When you swipe the PIV badge, you will get a “Badge Violate Void” alert with a badge number. The badge number is actually your agency code. You can use this method of swapping format bits, to determine the values in different fields of the PIV card (ex. Agency code, site code...).

10) If no alert displays on the CA3000 when you swipe the badge, verify you have the correct firmware in the panel as per the previous step. As a test, you can modify your parity bits to all zero to eliminate parity checking. Do not leave it at zeros indefinitely. With the parity bits set to zeros, swipe the badge. If data displays, this verifies you have a problem with the parity.

	Offset	Length
Even	0,	0
Odd	0,	0

11) You will get a “Badge Violate Unauthorized” if the agency code is not correct in personnel. If you do not know the agency code, refer to step 9 above to determine it.

12) If you have a dual technology card, you could get 2 beeps. One for the 125 KHZ read and one for the 13 megahertz read.

13) If you are unable to get a read using the PIV formats in the CA3000, there is another test you can perform. PIV cards output a unique ID. Some unique ID's are 40 bits, 48 bits and 56 bits. You can create a 40 bit format in the CA3000. Configure it for Non-ABA. Present the PIV card to the reader. If you get a read, this is the unique ID. If the 40 bit format doesn't work, repeat these steps for the 48 and 56 bit format. If you can read the Unique ID, this will verify the reader is acknowledging the card and sending data.

14) If all else fails, create a new database and reconfigure it. After creating a new database, re-test it.