Enrolling with PIV and PIV-I Velocity Enrollment Manager





Overview

The Homeland Security Presidential Directive 12 (HSPD-12) called for a common identification standard to be adopted by all Federal Government Agencies. The Person Identity Verification (PIV) credential has been issued to over 8 million Federal employees (almost four million people). The PIV credential is a smart card operating at 13.56 MHz with a specific data module called End-Point. Certain data is available by a "free read", while other personal data requires a personal (secret) PIN (personal identification number) to access (for example the required biometric fingerprint data).

PIV card users can utilize their cards in Physical Access Control Systems (PACS) in a number of ways based on the required level of assurance at the specific locations they are permitted to access. At the lowest level of assurance a "free read" of the Card Holder Unique Identifier (CHUID) data object, and at the highest level of assurance, a multi-factor authentication using Public Key Infrastructure (PKI).

The CHIUD contains a Federal Agency Smart Credential Number (FASC-N), which is used to enroll a user in Velocity, providing a unique credential number for use in the Physical Access Control System (PACS). In a PKI implementation, the FASC-N is used but the certificates on the card (the card certificate in the case of "contactless" CAK and the Person Certificate in the case of contact "PAK") are used to validate the card and user.

For Government contractors, cards are issued with the same card data module, and the same CHUID, however the first three fields of the FASC-N contain only "9's". These cards are called PIV-I (interoperable). Correct implementation of these cards requires the PACS to utilize the Universal Unique Identification (UUID) number rather that the FASCN. PIV-I cards include the PKI certificates that enable the CAK/PAK schema.

Velocity provides the ability to enroll PIV cards on HIRSCH PACS with the appropriate read and MATCH custom settings.

The following pages will assist in establishing the devices and Enrollment Manager Settings to enroll the PIV and PIV-I cards into the Velocity system.

To have the **PIV** read into the Velocity access control system the following setups need to be established.

1. Create the following User Defined Fields in Enrollment Manager.

•	Name Parsing	Text
•	Agency Code	Number
•	System Code Credential Number	Number
•	Credential Series	Number
•	Individual Credential Issue	Number
•	Person Identifier	Number
•	Organizational Category	Number
•	Organization Identifier	Number
•	Person Org Assoc Category	Number
•	Expiration Date	Date

• Locate under Enrollment Manager > Tools > User Defined Fields....

ser Def Ente For I item	ined Fields Additional Ima er the caption and type of ear fields defined to be List types).	ges) ch Use s, you r	er Defined o may optiona	data entry field. ally enter default values I	or the list (Ctrl-Enter to	enter next
Number	r of UDFs: 36	Appl	y			
UDF	Caption	Req	Color	Туре	Default	Tab 🔺
1	Name Parsing		Black	Text	(None)	Genera
2	Agency Code		Black	Number	(None)	Genera
3	System Code		Black	Number	(None)	Genera
4	Credential #		Black	Number	(None)	Genera
5	Credential Series		Black	Number	(None)	Genera
6	Individual Cred Issue		Black	Number	(None)	Genera
- 7	Person Identifier		Black	Number	(None)	Genera
8	Organizational Category		Black	Number	(None)	Genera
9	Organization Identifier		Black	Number	(None)	Genera
10	Person Org Assoc Category		Black	Number	(None)	Genera
11	Expiration Date		Black	Date	(None)	Genera
12	×		Black	I	(None)	Genera
13	Company Name		Red	n List	(List)	Genera 🕳
4		-	D 1		01 Y	•
Help					<u></u> ОК	Cancel

Figure 1 - User Defined Fields

- 2. For PIV the Name field must be Parsed, split between First, Middle and Last Name.
- Properties Enrollment Manager Tools > Preferences
- Change the UDF Name Parsing field to the UDF defined.

sing field	Preferences	×
	General Print Control Defaults Circle Display Print Confirmation Quick Find Default Query Size: 10 Number of items to display in the Quick find displayment is Bancer 5 to 50	
	UDF Name Parsing Perform automatic name parsing for this UDF: UDF 1 - Name Parsing	
	Interval Offset Display Today 17:00 Today (17:00) Today 01:00 Today (17:00) Today 01:00 Today (17:00) Today 23:59 Michight Week 1 1 Week Month 1 1 Month Year 1 1 Year 1 2 2) tooko	
	Help OK Cancel	

Figure 2 Enrollment Manager Preferences

- 3. Establish the device for reading the card and install by USB. The driver for the device must be downloaded from the internet as Velocity does not supply the driver.
 - a. SCR3310 b. SCR3311



Figure 3 -CRSCMCEUSB Card Reader



4. The RUU device may also be used to enroll the PIV card. Be sure to have the correct firmware installed on the device using the Cogent software. This will allow for the addressing TCP/IP and will enable the choice for enrollment on the Device Configuration RUU tab.



5. If an Enrollment Station is being used, the Special Handling needs to be established under Device Configuration. Enrollment Manager > Tools > Device Configuration > Credential Enrollment

[Device Configuration	х
	Credential Enrollment Signature	e <u>C</u> apture <u>S</u> canners PIV <u>R</u> eader RU <u>U</u>
	DIGI*TRAC Credential MATCH	H Enrollment Station
	Serial port:	\\MARYJOGRAPHICPC\COM1 -
	Custom card mapping:	<none> •</none>
	Enable Hex Pass-through:	
	Special Handling:	200-bit FASCN Bypass 👻
	Note: Since the Enrollment Stati typically not used simultaneously A/B switch is used.	on and Signature Capture Devices are , they may share a common serial port if an
	Help	OK Cancel

Figure 5 - Device Configuration Special Handling

Note: The reader used for the enrollment must have the MATCH custom settings as well as the correct firmware for the data to pass correctly into the Enrollment Manager Fields.

6. Select Enrollment Manager Tools > Device Configuration and map the UDF fields to each device used for card reads.



Figure 6 UDF Field Mapping for Enrollment – Click and Drag to UDF Field.

Note: For PIV-I cards, the UDF Field of UUID/GUID is the only field that is necessary to map for credentialing. This field will need to be added to the UDF Fields if both types of cards are being enrolled into Enrollment Manager if previously not added.

Enrollment Manager > Tools > User Defined Fields – be sure to select Unique Text as the UDF type.

- 7. Close and reopen Enrollment Manager. There should now be a scan button
- 8. Select Add Person and select the scan button.

Add New Credential	Assign Credential	Preview Badge	Print Badge
Scan			Undo Apply



Read PIV Card	Type:	FIPS 201 Contact	
		Read locked information (requires)	PIN)
Field Caption	V	alue	
Name			
Employee Affiliation line 1			
Employee Affiliation line 2			
Expiration Date (Printed)			
Agency Card Serial Number			
Issuer Identification			
Agency Code			
System Code			
Credential Number			
Credential Series			
Individual Credential Issue			
Person Identifier			
Organizational Category			
Organization Identifier			
Person Organization Association I	Categori		
			Clear
Jutput Window:			

9. Select the device to read the card if multiple devices are being used.



10. To read all the fields, the card holder will need to enter their PIN to unlock the card. This applies to both PIV and PIV-I card. Once OK is selected, the card will read and the fields will show the data.

[Give it a few seconds, and the data will fill in the fields above, and also the output window.]

Verify Scanner Data		x	
<u>P</u> IV Reader			
Read PIV Card Type	e: FIPS 201 Contact	•	
Field Caption	Value		
Name	GROTHMAN-PELTON, MARY J		
Employee Affiliation line 1			
Employee Affiliation line 2			
Expiration Date (Printed)	06AUG2015		
Agency Card Serial Number	0005963390		
Issuer Identification	7099		
Agency Code	7099		
System Code	1101		
Credential Number	073914		
Credential Series	1		
Individual Credential Issue	1		
Person Identifier	0004656580		
Organizational Category	1		
Organization Identifier	7099		11. Click Accept for the data
Person Organization Association Category	2	· · · ·	
Output Window:		Cļear	to populate the UDF fields in
Line1: Line2: ExpirationDate: 06AUG2015 AgencyCardSerialNo: 0005963390 IssuerID: 7099 Discourt DNA OK			Enrollment Manager.
	Accept	Cancel	

Figure 10 Scanned Data from PIV/TWIC Card



General HR S	martCards Be Careful of Ler	ngth TAB 4 TAB 5	TAB 6 TAB 7 TAB 8 TA	AB 9 TAB 10 Groups			
🌆 ID:	-99	Record La	st Updated: 3/24/2013				
Name: (First, Last)	ame: (First, Last) MARY J GROTHMAN-PELTON						
Name Parsing	Jame Parsing GROTHMAN-PELTON, MA Organizational 1						
Agency Code	7099	Organization Identifie	7099				
System Code 1101		Person Org Assoc 2					
Credential # 073914		Expiration Date	08/06/2015				
Credential Series 1		GUID	000000000000000000000000000000000000000				
Individual Cred Issue	1	User Defined 13		Double-click images			
Person Identifier	0004656580	User Defined 14		to edit			
Add Nev	Add New Credential						
Scan	Scan Undo Apply						

12. Click Apply to download. You are now ready to issue a credential.

For PIV Credentials - 200 bit FASCN

13. Add New Credential

General Function Limits Options Biom	Concatenate FASCN UDFs X
ID: (new)	Select numeric UDFs to concatenate into the FASCN field:
Description: PIV Credential (TWIC) Badge Template: (None) IDF: 2-Card Card Type: 200-bit FASCN	Agency Code Agency Code • System Code System Code • Credential Number Credential # • Credential Series Credential Series • Individual Credential Issue Individual Cred Issue • Person Identifier • • Organizational Category • •
Data: FASCN: 3 Enrollment Station Status. Double click for Diagnostics Help	Organizational Identifier Organization Identifier Person/Organization Association Person Org Assoc Category OK Cancel OK Cancel

Figure 11 - Add New Credential - UDF MATCH

Note: The PIV and PIV-I cards may use IDF 2 for use with just the card presented at the reader. If any other IDF is selected, a PIN will be required. This should never be the secret PIN that the user has to unlock the data on the card.

The 200-bit FASCN will populate the UDF concatenate window. Select the corresponding UDF fields created and click OK. This will produce the FASCN that will be used for the card read.

Card							
Туре:	200-bit FASCN 🔹 🔹						
	·						
Data:	<udf>709911010739141</udf>	UDF					
FACCH		22.45-34					
FASUN:	70991101073914110004	32 digits					
Enrollment S for Diagnos	Enrollment Station Status. Double click						

To locate the UDF concatenate window, select the UDF...button on the Data field.

General Function Limits Options Biometrics				
ID: (new)				
🔳 Link to:	v			
Description:	PIV Credential			
Badge Template:	(None) 🗸 🖾 🗕			
IDF:	2-Card			
Card				
Туре:	200-bit FASCN			
Data:	<udf>709911010739141 (UDF)</udf>			
FASCN:	70991101073914110004(32 digits			
Enrollmer for Diagn	nt Station Status. Double click			

Concatenate FASCN UDFs		X
Select numeric UDFs to concatenate	into the FASCN field:	
Agency Code	Agency Code 🗸	
System Code	System Code 🔹 👻]
Credential Number	Credential # 🔹 👻]
Credential Series	Credential Series 🔹 👻]
Individual Credential Issue	Individual Cred Issue 🔹 👻]
Person Identifier	Person Identifier 🔹 👻	
Organizational Category	Organizational Category 🗾 👻]
Organizational Identifier	Organization Identifier 💦 👻]
Person/Organization Association	Person Org Assoc Category 🚽	
	OK Cancel	

IDENTIVE

Figure 12 UDF button on Credential General Tab

This will supply a 32 digit number in both the Data field and the FASCN field.

Select the Function Tab and assign the appropriate Door Group for this individual.

Figure 13- FASCN Assignment

• All Limits

- Threat Authority and 2 Person Rule may be assigned
- Options
 - Special Needs Access and Passback Executive Override may be assigned
- Click OK and the PIV credential has been issued.
- Verification of download may be seen in the Event Viewer.



For PIV-I Credentials

The UUID/GUID is the unique text that is used for the credential.

Using the contact reader, the card will be read just like the PIV card, with the addition of the UUID.

To read all the data the card holder will also need to enter their PIN number.

NOTE: The PIV-I card has 9999 instead of a Government Agency Code.

Assign a Door Group function and any Limits or Options for this credential.

Verify Scanner Data		Х			
Plv Beader					
		1			
Deed DIV Could					
neau Fiv Calu	Read PIV Land Type: PIPS 201 Contact *				
Read locked information (requires PIN)					
Field Caption	Value	Courd DTM			
Name		Card PIN			
Employee Affiliation line 1					
Employee Affiliation line 2		A STATE OF STATE OF			
Expiration Date (Printed)					
Agency Card Serial Number					
Issuer Identification					
Agency Code	9999				
System Code	9999	Please enter PIN:			
Credential Number	999999	****			
Credential Series	1				
Individual Credential Issue	1				
Person Identifier	0004656580	OK Cancel			
Organizational Category	1				
Organization Identifier	0001				
Person Organization Association Category	12	· · ·			
Output Window:	Output Window:				
Detected: SCM Microsystems Inc. SCR33x USB Smart Card Reader 0 Specified reader found: SCM Microsystems Inc. SCR33x USB Smart Card Reader 0 pivSelectCardApplication: PIV_OK pivSetData: PIV_OK FASC:N parse completed. ED: 03/15/2018					
Help		Accept Cancel			

Figure 14 - PIV-I card with PIN

Personal Information				
General	HR SmartCards Be Carefu	l of Length TAB 4 TAB 5 TAB 6 TAB 7 TAB 8 T 💶		
UDF	Caption	Value 🔺		
20	Agency Code	9999		
21	System Code	9999		
22	Credential ID			
23	Credential Number	999999		
24	Credential Series	1		
25	Individual Cred Issuer	1		
26	Person Identifier	0004656580		
27	Organization Category	1		
28	Organization Identifier	0001		
29	Person Organ Ass Category	2		
30	Expiration Date	3/15/2018		
31	AgencyCode CHUID			
32	Organ Identifier CHUID			
33	DUNS			
34	GUID	9A9A67B2D2DC43F5BBE842220428A82C		

Figure 15 The UUID/ GUID will have numbers and letters.



.Door Properties - PIV

- HID iCLASS reader with 200 bit firmware – using a MATCH2 set with Custom 27-28 - 29
- Entry Reader Setup Tab Special Handling- 200 bit FASCN Bypass
- Present PIV card and access granted.

PIV	Door-M8 DR3 Executive Offices \\XNET.001.0001.001.01.DR03 Properties 🗴
er with – using a Custom	General Entry Reader Relay Input Setup ScramblePad Options Logic Reader Name: M8 DR3 Executive Offices
ıp Tab – 200 bit	MATCH Reader Enable bezel tamper Enable Wiegand Hex Pass-through LED reverse
and	Disable reader above this level: 99 - Level 99 - Disable CCOTZ above this level: 99 - Level 99 -
	Enable ScramblePad Sharing Custom Card Codes: None> Special Handling 200-bit FASCN Bypass
	Help OK Cancel

Figure 16 - Entry Reader Settings

Note: MATCH special settings for the corresponding bit formats

- 64 bits Custom 24,25,or 26
- 75 bits Custom 18, 20 or 21
- 128 bits -Custom 18,20,21,24,25,26,27,28,and 29[PIV only]
- 200 bits -Custom 27,28,or 29

Note: Along with the MATCH custom settings, the firmware on the reader must also correspond to the bit format.



For PIV-I cards

- HID iCLASS with 128 bit firmware and MATCH2 with Custom 27-29
- The PIV-I card uses the FASCN Bypass to allow the UUID to be used
- Along with the Wiegand HEX Pass-through, the card reads the same at the door
- The Door Properties is different, using the Enable Wiegand Hex Pass-Through to enable the UUID/GUID to pass through
- Presented to the reader, the PIV-I card will issue an access grant
- If the reader has the ability to read both formats, then the cards enrolled will read by presenting the card
 - If the Agency Code is all "9s" the reader will pass through the UUID

Door-2-Lab Security Area 1 \\XNET.001.0003.001.01.DR02 Properties 💦 🗙				
General Entry Reader Exit Reader Relay Input				
Setup ScramblePad Options Logic				
	_ []			
Reader Name: 2-Lab Security Area 1	_			
MATCH Reader	ם וו			
Enable bezel tampe				
ED reverse				
L	- 1			
Direkte sonder eksen this level				
Disable reader above this level: 99 - Level 99 -				
Disable CCOTZ above this level: 99 - Level 99				
🕅 Enable ScramblePad Sharing				
Custom Card Codes:				
<none> *</none>				
Special Handling:				
200-bit FASCN Bypass				
Help OK Can	cel			

Velocity Enrollment Manager has

all the ability to read both PIV and PIV-I cards. The trick is to make sure all the corresponding devices are established with the correct formats.

- Enrollment Station
 - MATCH Custom settings
 - Reader firmware
- Device Configuration
 - User Defined Fields to map the data
 - Name Parsing is PIV cards are being read
- Scanning the card
 - PIN needed for name field
- Door Properties
 - Reader settings