

**FRTC Section 4 Backend
Registration and Data Model
Companion Paper**

FRTC VERSION 1.4.2 Rev A



FIPS 201 EVALUATION PROGRAM

March 31, 2021

Version 1.0

Office of Government-wide Policy
Office of Technology Strategy
Identity Management Division
Washington, DC 20405

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	2/12/2021	Initial draft for comment	Public
Initial Release	1.0	3/31/2021	Initial publication	Public

Table of Contents

Table of Contents	3
1. Background	4
2. Objectives	4
3. Test Cases and Changes	5
3.1 Test Case 4.01.01	5
3.2 Test Case 4.01.02	5
3.2 Test Case 4.01.03	5
3.2 Test Case 4.01.04	5
4. Data Model	6
References	9

1. Background

Section 4 of the FIPS 201 Evaluation Program Physical Access Control Systems (PACS) Functional Requirements Test Cases (FRTC) focus on a system's ability to provision and deprovision card and user data from an external source (also known as 'backend registration'). The current set of test cases are categorized as design analysis and simply require applicants to attest to the ability to perform these actions. As PACS become more Enterprise oriented (ePACS), many agencies are beginning to see a benefit in automated provision provided data from their Identity Management Systems (IDMS) and Card Management Systems (CMS). It is the intent of the Data Model to define the potential data set presented to a PACS or ePACS and ensure Approved Product List (APL) systems are able to appropriately handle the data set and conduct backend registration processes.

2. Objectives

The data model in conjunction with the requirements in [FRTC] Section 4 are intended to ensure an APL system is capable of appropriately handling the data set. It is the intent that a PACS should be able to perform provisioning, deprovisioning, and modifications of both user and card data as part of identity life cycle management. The existing data set is intended to be larger than any given system is expected to support due to the varying requirements across multiple PACS solutions. Additional [FRTC] requirements for Section 4, as well as the accompanying data model were developed to facilitate the following goals:

1. Define a super-set of data elements APL systems may require for successful registration. Each PACS will be able to use a subset of this model required for registration and consider the remaining elements as optional.
2. Verify systems can appropriately handle more data than may be minimally required for registration
3. Ensure backend registration of user and card data is processed similar to individual enrollment data
4. Ensure updates between the IDMS/CMS and PACS are handled appropriately to facilitate lifecycle operations
5. Ensure provisioning and deprovisioning workflows occurs as designed

While the initial data set will be used for design analysis, the FIPS 201 Evaluation Program will create testing artifacts for FRTC Section 4 test cases in a future update. Data element definition table is displayed for clarity and not a requirement for a specific type of interface (xml, soap, etc).

3. Test Cases and Changes

The following test cases are associated with the back end enrollment functionality

4.01.01	TC-23-001	The E-PACS shall accept automated provisioning using APL data model from a source it trusts and that complies with the security requirements described in the detailed guidance of PIA-8 [PIV in ePACS].
4.01.02	TC-23-002	The E-PACS shall accept automated deprovisioning from a source it trusts and that complies with the security requirements described in PIA-3.5 and PIA-3.6 [PIV in ePACS].
4.01.03	TC-23-003	The E-PACS shall accept automated record modifications (e.g., certificates) using APL data model from a source it trusts and that complies with the security requirements described in the detailed guidance of PIA-8 [PIV in ePACS].
4.01.04	TC-23-004	The E-PACS shall support a secure channel (e.g., mutual-authentication over TLS) for all transactions with the trusted source.

3.1 Test Case 4.01.01

This test case was updated to reflect the requirement of a system to use the data model as a data set.

3.2 Test Case 4.01.02

No change

3.2 Test Case 4.01.03

This test case was added to ensure data life cycle maintenance, encompassing updates to card and user data.

3.2 Test Case 4.01.04

This test case was added to ensure the system complies with secure transmission procedures. Card and user data should be considered Personally Identifiable Information (PII) and appropriate safeguards need to be placed around transmission per [SP 800-53].

4. Data Model

#	Data	Structure	Length	Reference	Data Tag
Biographic Identity Data					
A1.0	FASC-N/PI Person Identifier	string	10	SP800-73	PI
A1.1	FASC-N/OI Organization Identifier	string	4	SP800-87	OrgID
A1.2	Card Holder UUID	number	16	SP800-73	PersonUUID
A1.3	Subject's first name	string	50	FIPS 201-2 <Secondary Identifier>	FirstName
A1.4	Subject's middle name	string	50	FIPS 201-2 <Secondary Identifier>	MiddleName
A1.5	Subject's last name	string	50	FIPS 201-2 <Primary Identifier>	LastName
A1.6	Suffix to subject's name	string	10	FIPS 201-2 <Primary Identifier>	Suffix
A1.7	Height	string	6	CJIS-EBTS (FII) or (F' II")	Height
A1.8	Weight	string	6	CJIS-EBTS (xxxLBS)	Weight
A1.9	Place of Birth	string	50		POB
A1.10	Citizenship - Nationality	string	3	ISO 3166-1 country code	Nationality
A1.11	Hair Color	string	3	CJIS-EBTS p38	HairColor
A1.12	Gender	string	1	CJIS-EBTS p37	Gender
A1.13	Eye Color	string	3	CJIS-EBTS p37	EyeColor
A1.13	Race	string	1	CJIS-EBTS p39	Race
A1.14	Subject's date of birth	string		Date format TBA	DOB
A1.15	Agency, Dept or Organization Affiliation	string	50	FIPS 201/Zone 10F	OrgAffiliation
A1.16	Affiliation Class	string	50	FIPS201/ Zone 15F, 18F	AffiliationClass
A1.17	Affiliation	string	50	FIPS 201/Zone 8F (Employee, Contractor, Detailee, Private Sector, State/Local/Tribal)	Affiliation
A1.18	FASC-N/OC Organizational Category	string	1	TIG SCEPACS v2.2	OrgCategory
A1.19	FASC-N/POA Person Organization Association Category	string	1	TIG SCEPACS v2.2	OrgPOA
A1.20	CHUID/Organizational Identifier	string	4	800-87	OrgSubID
#	Data	Structure	Length	Reference	Data Tag
#					
A.2.0	Federal Emergency Response Official indicator	string	4	FIPS 201/Zone 12F	FERO

A.2.1	Law Enforcement Official (LEO) indicator	string	3		IndicatorLEO
A.2.2	Weapon Bearer Indicator	string	10		WeaponBearerIndicator
A.2.3	Weapons Registration Number	string	10		WeaponsRegistrationNumber
#	Data	Structure	Length	Reference	Data Tag
			#		
A.3.0	Portrait image - JPEG	B64	SP 800-76-compliant	INCITS 385	PortraitJPG
A.3.1	Portrait image – JPEG2000	B64	SP 800-76-compliant	INCITS 386	PortraitJPG2000
A.3.2	PIV Fingerprint Template 1	B64		INCITS-378 / CBEFF / SP800-76	CardFPTemplate1
A.3.3	PIV Template metadata 2	B64		INCITS-378 / CBEFF / SP800-76	CardFPmetadata1
A.3.4	PIV Fingerprint Template 2	B64		INCITS-378 / CBEFF / SP800-76	CardFPTemplate2
A.3.5	PIV Template metadata 2	B64		INCITS-378 / CBEFF / SP800-76	CardFPmetadata2
#	Data	Structure	Length	Reference	Data Tag
			#		
A.4.0	Credential Issue Date	string	8	FIPS 201 /Zone 13F	CardIssueDate
A.4.1	CHUID/Expiration Date	string	8	SP800-73	CardExpirationDate
A.4.2	CHUID/GUID	number	16	SP800-73	CardUUID
A.4.3	FASC-N	string	25	TIG SCEPACS v2.2/Includes AC-SC-CN-CS-ICI-PI-OC-OI-POA	CardFASCN
A.4.4	FASC-N/AC Agency Code	string	4	TIG SCEPACS v2.2	IssuerAgency
A.4.5	FASC-N/SC System Code	string	4	TIG SCEPACS v2.2	SystemCode
A.4.6	FASC-N/CN Credential Number	string	6	TIG SCEPACS v2.2	CredentialNumber
A.4.7	FASC-N/CS Credential Sceries	string	1	TIG SCEPACS v2.2	CredentialSeries
A.4.8	FASC-N/ICI Individual Credential Issue	string	1	TIG SCEPACS v2.2	CredentialICI
A.4.9	Printed Name	string	150	FIPS-201/Zone 2F	CardPrintedName
A.4.10	Card Expiration Date	string		Zone 14F	CardExpirationDate
A.4.11	Card Identification Number	string		FIPS 201/Zone 1B	CIN
A.4.12	Issuer Identification Number	string	6	FIPS 201/Zone 2B	IIN
A.4.13	Signature	B64		FIPS 201/Zone 3F	CardSignature
A.4.14	CHUID/Content Signer Cert	B64		SP800-73/Extract from Issuer Asymmetric Signature field	ContentSigner

A.4.15	Signed CHUID	B64		Base 64-encoded SHA-256 hash of the CHUID	ContentSignerHash
A.4.16	Secure Messaging Certificate Signer	B64		SP800-73	SMCertSigner
A.4.17	Credential Status	string	1	e.g., Active, Revoked	CredStatus
A.4.18	Card Capability Container	B64	287	SP 800-73-4	CCC
A.4.19	Security Object	B64	1336	SP 800-73-4	SecObject
#	Data	Structure	Length	Reference	Data Tag
PIV Public Key Infrastructure (PKI)					
A.5.0	PIV Authentication Cert	B64		X.509	PAK
A.5.1	Card Authentication Cert	B64		X.509	CAK
A.5.2	Email address (from X509 SAN)	string	50	RFC-822 email. May be >1	SANRFC822

References

- [FIPS 201] Personal Identity Verification (PIV) of Federal Employees and Contractors, Federal Information Processing Standard 201-2, August 2013, or as amended
<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf>
- [FRTC] FIPS 201 Evaluation Program Functional Requirements and Test Cases, August 2018
<https://www.idmanagement.gov/pacs-frtc-v1-3-3/>
- [PIV in ePACS] Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS), March 2014, or as amended
<https://playbooks.idmanagement.gov/assets/pacs/PIV-in-EPACS-v3.pdf>
- [SP800-53] Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Revision 5, September 2020, as amended
<https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
- [SP800-73] Interfaces for Personal Identity Verification, NIST Special Publication 800-73-4, May 2015, or as amended
<https://csrc.nist.gov/publications/detail/sp/800-73/4/final>