pivCLASS®

FIPS-201 Reader Operation and Output Selections Application Note

6090-905, Rev. F.1

April 2020

Copyright

Trademarks

Revision history

Date	Description	Revision
April 2020	Updates to the following sections: ■ *Section 1 Overview*. ■ *Section 2 CHUID definition*. ■ *Section 4.2 General data formatting* ■ *Section 5 GUID for PIV, PIV-I, and CIV*. ■ *Section 8.9 128 Bit UUID Output - Supported by PAM*.	F.1

Contacts

For additional offices around the world, see **www.hidglobal.com/contact/corporate-offices**.

Americas and Corporate	Asia Pacific
611 Center Ridge Drive Austin, TX 78753 USA Phone: +1 866 607 7339 Fax: +1 949 732 2120	19/F 625 King's Road North Point, Island East Hong Kong Phone: +852 3160 9833 Fax: +852 3160 4809
Europe, Middle East and Africa (EMEA)	**Brazil**
3 Cae Gwyrdd Green Meadow Springs Cardiff CF15 7AB United Kingdom Phone: +44 (0) 2920 528 500	Condomínio Business Center Av. Ermano Marchetti, 1435 Galpão A2 - CEP 05038-001 Lapa - São Paulo / SP Brazil Phone: +55 11 5514-7100

HID Global Technical Support: **www.hidglobal.com/support**.

Contents

This page is intentionally left blank.

1 Overview

This document outlines the definitions of the FIPS-201 data container and the output options available with pivCLASS FIPS-201 readers. pivCLASS readers comply with, and are GSA APL certified per FIPS-201-2, with support of Little to Very High assurance levels. Support of Little assurance level is supported directly in the reader. Support of higher assurance levels requires use of the pivCLASS Solution, described at:

https://www.hidglobal.com/solutions/pivclass-government-access-control-solutions

2 CHUID definition

Agency and technology independent U.S. Presidential directive HSPD-12, and the resulting FIPS-201 Standard, defines a common data model for Personal Identity Verification (PIV). The following table shows the Card Holder Unique ID (CHUID) data model.

Table 1 - Description of the Card Holder Unique ID (CHUID)

Data Element	Max. Bytes	Tag	Description
Buffer Length	2	EE	Mandatory TLV record. Exists when a TLV record, in addition to the FASC-N, exists in the CHUID for contact File System and contact-less smart cards.
FASC-N	25	30	Mandatory TLV record. Federal Agency Smart Credential Number.
Agency Code	4	31	Optional TLV record. Recommended when the SP 800-87 code for the government agency issuing the credential contains alpha characters.
Organizational ID	4	32	Optional TLV record. Recommended when the SP 800-87 code for the FASC-N OI field contains alpha characters.
DUNS	9	33	Optional TLV record. Recommended when the FASC-N agency code = 9999. D&B DUNS number for non-Federal FASC-N issuer.
GUID	16	34	Mandatory TLV record. Includes a UUID (see Section SP 800-73-3 Section 3.3), an issuer assigned IPv6 address3, or be coded as all zeroes (0x00). **Note:** FIPS 201-2 now mandates that PIV use this field and that it will be a UUID. IPv6 and 0x00 are no longer valid. May want to note this for transitional purposes.
Expiration Date	8	35	Mandatory TLV record. Card expiration date, YYYYMMDD
RFU	2	38 - 3C	Reserved for future use.
Authentication Key Map	512	3D	Optional TLV record. May exist for high assurance profile applications.
Asymmetric Signature	2816	3E	Mandatory TLV record. Issuer defined algorithm, public key and signature.
LRC	1	FE	Optional TLV record. Longitudinal Redundancy Code.

3 FASC-N and FIPS-201 overview

The FASC-N is a BCD (Binary Coded Data) credential number definition that maintains transparent interoperability with the SEIWG-012 credential number, but redefines the use of the SEIWG-012 SSN and reserved fields.

Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (TIG-SCEPACS) Version 2.3, dated December 20, 2005, defines the FASC-N Number Format as an eventual, compatible replacement for the SEIWG-012 credential number.

The FIPS-201 application is intended to be manufacturer/technology agnostic. The only requirement is that the credential must be compatible with all four parts of the *ISO/IEC 14443* specification. The Application Processing chapter provides specifics on the various ways of accessing the application data. The following tables define information contained in the FASC-N and the length of the BCD digits.

Note: Some of the reader formats are emulated by the pivCLASS Authentication Module (PAM). Those output formats are identified below.

3.1 TIG-SCEPACS FASC-N Example

SS AGENCY CODE + FS SYSTEM CODE + FS CREDENTIAL NUMBER + FS CS + FS ICI + FS PI + OC + OI + POA + ES + LRC

Table 2 - Definition of FASC-N contents

Field name	Length (BCD Digits)	Field Description
AGENCY CODE	4	Identifies the government agency issuing the credential
SYSTEM CODE	4	Identifies the system the card is enrolled in and is unique for each site
CREDENTIAL NUMBER	6	Encoded by the issuing agency. For a given system no duplicate numbers are active
CS	1	CREDENTIAL SERIES (SERIES CODE) Field is available to reflect major system changes
ICI	1	INDIVIDUAL CREDENTIAL ISSUE (CREDENTIAL CODE) Initially encoded as “1”, will be incremented if a card is replaced due to loss or damage
PI	10	PERSON IDENTIFIER Numeric Code used by the identity source to uniquely identify the token carrier (for example, DoD EDI PN ID)
OC	1	ORGANIZATIONAL CATEGORY 1. Federal Government Agency 2. State Government Agency 3. Commercial Enterprise 4. Foreign Government

Field name	Length (BCD Digits)	Field Description
OI	4	ORGANIZATIONAL IDENTIFIER OC=1 – FIPS 95-2 Agency Code OC=2 – State Code OC=3 – Company Code OC=4 – Numeric Country Code
POA	1	ORGANIZATIONAL CATEGORY 1 – Employee 2 – Civil 3 – Executive Staff 4 – Uniformed Service 5 – Contractor 6 – Organizational Affiliate 7 – Organizational Beneficiary
SS	1	Start Sentinel Leading character which is read first when card is swiped
FS	1	Field Separator
ES	1	End Sentinel
LRC	1	Longitudinal Redundancy Character

Table 3 - Definition of BCD 4-Bit Cluster with Parity, defines the packed BCD 4-Bit decimal format with odd parity calculated over the preceding BCD cluster (the definition is taken from *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.2, July 30, 2004).

The following provides HID TIG-SCEPACS BCD definitions.

- BCD coding is “least significant bit first and parity bit last”. For example, 7 = 1110. This means the LSB is the first to be sent from the reader.
- Reverse BCD coding is the opposite of this coding. For example, 7 = 0111. This means the MSB is the first to be sent from the reader.

Table 3 - Definition of BCD 4-Bit Cluster with Parity

b0	b1	b2	b3	Parity	Corresponding character
0	0	0	0	1	0
1	0	0	0	0	1
0	1	0	0	0	2
1	1	0	0	1	3
0	0	1	0	0	4
1	0	1	0	1	5
0	1	1	0	1	6
1	1	1	0	0	7
0	0	0	1	0	8
1	0	0	1	1	9
1	1	0	1	0	Start Sentinel
1	0	1	1	0	Field Separator
1	1	1	1	1	End Sentinel

Note: Table 3 - Definition of BCD 4-Bit Cluster with Parity, is modified from *ISO 7811/2 Section 9.2.2 Table 2* for providing ease-of-use for the following examples.

The following example shows the 40 character FASC-N credential encoded as a 200-bit string on the physical credential. The parity bit of the LRC is encoded/transmitted last (the least significant bit of the 25th byte). Also shown is the binary data stream, Start Sentinel (left) to LRC (right). BCD refers to this structuring.

Example: FASC-N data stored on the card

110100000100001110010101000**10110**0000100001000011000**10110**0000110011010000010000100011010**10110**0000**10110**1000010110100001000010000100001000010000100011001110011100111001100000100000100001000011001010100**11111**10101

Example: FASC-N parsed by Character

11010	00001	00001	11001	01000	10110	00001	00001	00001	10000	01101
SS	0	0	3	2	FS	0	0	0	1	FS
00001	10011	01000	00100	00100	01101	10110	00001	10110	10000	10110
0	9	2	4	4	6	FS	0	FS	1	FS
10000	10000	10000	01000	01000	01000	11001	11001	11001	11001	10000
1	1	1	2	2	2	3	3	3	3	1
10000	01000	01000	11001	01000	11111	10101				
1	2	2	3	2	ES	5				

Decoded FASC-N data elements

- AGENCY CODE = 0032
- SYSTEM CODE = 0001
- CREDENTIAL# = 092446
- CS = 0
- ICI = 1
- PI = 1112223333
- OC= 1
- OI=1223
- POA=2
- LRC = 5

4 FIPS-201 PIV Application processing

4.1 Data access

For ISO/IEC 14443, Type A credentials and pivCLASS FIPS-201 readers implement the card activation process as detailed in Figure 1 of ISO/IEC 14443-4.

Note: Type B credentials are deprecated for use with PIV systems.

If the credential supports a baud rate of 424kb/s in both directions, configure the reader to switch to 424kb/s for all communications after anti-collision. If the credential only supports 212kb/s, the reader will switch to 212kb/s.

After card activation, the pivCLASS reader attempts to read, in order, one of the following four applications.

4.2 General data formatting

After reading the application data, the pivCLASS FIPS-201 reader reports the data over the Wiegand, OSDP, and Serial (when available) output ports. For data lengths not ending on a byte boundary, serial data output is left-padded with zeros. *Section 4.2.1 General reader message construction* provides an overview of general message construction. In the default settings, the message is transmitted in BCD format beginning with the credential CSN. Available output options, such as an HMAC signature, are listed as configurations in the HID Global How to Order Guide. The FASC-N message element may undergo further formatting by the pivCLASS reader as shown in *Table 4 - Appended FASC-N fields by message length*.

4.2.1 General reader message construction

Credential CSN + **HMAC Signature** + **FASC-N** + **GUID** + **Card Expiration**

Table 4 - Appended FASC-N fields by message length

Length	Appended Fields
40 Bits	System + Credential (parity automatically removed)
64 Bits	Agency + System + Credential + Series + Issue (parity automatically removed)
75 Bits	Agency + System + Credential + Expiration Date (parity automatically removed)
128 Bits	Agency + System + Credential + Series + Issue + Pers Inden + Org Cat + Org Ind + Pers/Org (parity automatically removed)
200 Bits	Complete FASC-N number (parity included)
128 Bits	PIV-I/CIV GUID (UUID)

5 GUID for PIV, PIV-I, and CIV

PIV-I and CIV credentials are issued by non-Federal or commercial agencies. As there is no central authority responsible for managing a smart numbering system similar to the FASC-N on Federally-issued credentials, the PIV-I and CIV credential standards use the Universally Unique Identifier (UUID), as defined in *RFC 4122, A Universally Unique IDentifier (UUID) URN Namespace*.

HID pivCLASS readers in legacy mode can dynamically determine whether a FIPS 201 credential is a PIV or PIV-I/CIV. If the first 14 digits of the FASC-N are all 9s, then the credential is deemed a PIV-I or CIV, and the reader automatically outputs the 128-bit CHUID GUID element. Otherwise, the credential is assumed to be a PIV credential, and the FASC-N is output. The format of the FASC-N is determined by the reader configuration.

Beginning with FIPS 201-2, PIV cards must also include a GUID container encoded with a UUID that is not all zeroes (0x00).

6 User feedback

After the anti-collision process, if an ISO/IEC 14443 Type A or Type B credential is detected, the pivCLASS FIPS-201 reader will illuminate the LED to a solid amber color. The LEDs remain amber until the reader processes the application. The duration of application processing is dependent upon reading the FIPS-201 card type. Do not remove the card from the RF field of the reader during application processing. Once complete, the reader flashes the LED green, sounds the buzzer for 250ms, and returns the LEDs to the default state. Unsuccessful reads cause the reader to flash the LEDs red and sound the buzzer for 250ms.

7 Legacy Nomenclature

Some legacy pivCLASS FIPS-201 readers and configuration cards may utilize Most or Least Significant Bit (MSB vs LSB) nomenclature in the part and/or part number descriptions. In keeping in-line with FIPS-201 nomenclature, HID has adopted Binary Coded Data (BCD) nomenclature based on data encoding per the FIPS-201 standard.

The following lists the nomenclature compatibility:

- MSB (Most Significant Bit) = Reverse BCD (binary coded data)
- LSB (Least Significant Bit) = BCD (reverse binary coded data)

This nomenclature identifies which bit is first sent from the reader.

8 Example output options

The following examples illustrate output of the pivCLASS FIPS-201 reader and the PAM. The examples provided are derived from sample card data and represent the resulting Serial, Wiegand, and Translated card data sent from the reader. The following examples do not cover every orderable option provided by the pivCLASS FIPS-201 family of readers.

Note: Beginning September 2014, only the 128-bit MSB credential numbering output formats defined in Sections 8.7 and 8.9 below will be authorized for use with PACS. Future revisions of this document will exclude output formats that are not authorized for use in a FICAM. See the FICAM Functional Requirements and Test Cases at: **https://www.idmanagement.gov/**

8.1 40 Bit BCD Output (LSB)

Serial Output

```
00 08 91 E6 A2
```

Decoded Wiegand Data

```
  0     0     0     1     9     8     7     6     5     4
0000  0000  0000  1000-1001  0001  1110  0110  1010  0010
```

Translated Card Data

System Code = 0001, Credential Number = 987654

8.2 40 Bit BCD Output (Reverse or MSB)

Serial Output

```
00 01 98 76 54
```

Decoded Wiegand Data

```
  0     0     0     1     9     8     7     6     5     4
0000  0000  0000  0001-1001  1000  0111  0110  0101  0100
```

Translated Card Data

System Code = 0001, Credential Number = 987654

8.3 64 Bit BCD Output (LSB)

Serial Output

```
8C  28  00  08  91  E6  A2  88
```

Decoded Wiegand Data

```
  1     3     4     1     0     0     0     1     9     8     7     6     5     4     1     1
1000  1100  0010  1000 - 0000  0000  0000  1000 - 1001  0001  1110  0110  1010  0010 - 1000 - 1000
```

Translated Card Data

Agency Code = 1341, System Code = 0001, Credential Number = 987654, Credential Series = 1, Issue Code = 1

8.4 64 Bit BCD Output (Reverse, or MSB) - Supported by PAM

Serial Output

```
13  41  00  01  98  76  54  11
```

Decoded Wiegand Data

```
  1     3     4     1     0     0     0     1     9     8     7     6     5     4     1     1
0001  0011  0100  0001 - 0000  0000  0000  0001 - 1001  1000  0111  0110  1010  0100 - 0001 - 0001
```

Translated Card Data

Agency Code = 1341, System Code = 0001, Credential Number = 987654, Credential Series = 1, Issue Code = 1

8.5 75 Bit Output - Supported by PAM

Serial Output

```
0C  53  D0  00  7C  48  1A  65  B8  97
```

Decoded Wiegand Data

```
1 - 00010100111101 - 00000000000001 - 11110001001000000110 - 100110010110111000100101 1 - 1
```

Translated Card Data

Agency Code = 1341, System Code = 0001, Credential Number = 987654, Exp Date = 20110411

8.6 128 Bit BCD Output (LSB)

Serial Output

```
8C  28  00  08  91  E6  A2  88  84  C2  A6  E1  90  88  C2  88
```

Decoded Wiegand Data

```
  1     3     4     1     0     0     0     1     9     8     7     6     5     4     1     1
1000  1100  0010  1000 - 0000  0000  0000  1000 - 1001  0001  1110  0110  1010  0010 - 1000 - 1000

  1     2     3     4     5     6     7     8     9     0     1     1     3     4     1     1
1000  0100  1100  0010 - 1010  0110  1110  0001  1001  0000 - 1000 - 1000  1100  0010  1000 - 1000
```

Translated Card Data

Agency Code = 1341, System Code = 0001, Credential Number = 987654, CS = 1, ICI = 1, PI = 1234567890, OC = 1, OI = 1341, POA = 1

8.7 128 Bit BCD Output (Reverse, or MSB) - Supported by PAM

Serial Output

```
13  41  00  01  98  76  54  11  12  34  56  78  90  11  34  11
```

Decoded Wiegand Data

```
  1     3     4     1     0     0     0     1     9     8     7     6     5     4     1     1
0001  0011  0100  0001 - 0000  0000  0000  0001 - 1001  1000  0111  0110  0101  0100 - 0001 - 0001

  1     2     3     4     5     6     7     8     9     0     1     1     3     4     1     1
0001  0010  0011  0100 - 0101  0110  0111  1000  1001  0000 - 0001 - 0001  0011  0100  0001 - 0001
```

Translated Card Data

Agency Code = 1341, System Code = 0001, Credential Number = 987654, CS = 1, ICI = 1, PI = 1234567890, OC = 1, OI = 1341, POA = 1

8.8 200 Bit Output - Supported by PAM

Serial Output

```
D4 32 48 58 21 0C 2D 31 71 B5 25 A1 68 5A 08 C9 2A DE 0A 61 84 32 48 43 E2
```

Decoded Wiegand Data

SS		1		3		4		1		D		0		0		0		1	
1101	0	1000	0	1100	1	0010	0	1000	0	1011	0	0000	1	0000	1	0000	1	1000	0
D		9		8		7		6		5		4		D		1		D	
1011	0	1001	1	0001	0	1110	0	0110	1	1010	1	0010	0	1011	0	1000	0	1011	0
1		D		1		2		3		4		5		6		7		8	
1000	0	1011	0	1000	0	0100	0	1100	1	0010	0	1010	1	0110	1	1110	0	0001	0
9		0		1		1		3		4		1		1		F		8	
1001	1	0000	1	1000	0	1000	0	1100	1	0010	0	1000	0	1000	0	1111	1	0001	0

Translated Card Data

Agency Code = 1341, System Code = 0001, Credential Number = 987654, CS = 1, ICI = 1, PI = 1234567890, OC = 1, OI = 1341, POA = 1, LRC = 8

8.9 128 Bit UUID Output - Supported by PAM

Example GUID

```
b8c8bd84 – 20bb – 4026 – 8133 – 613153c02ec1
```

Serial Output

```
B8 C8 BD 84 20 BB 40 26 81 33 61 31 53 C0 2E C1
```

Decoded Wiegand Data

B	8	C	8	B	D	8	4	2	0	B	B	4	0	2	6
1011	1000	1100	1000	1011	1101	1000	0100 –	0010	0000	1011	1011 –	0100	0000	0010	0110
8	1	3	3	6	1	3	1	5	3	C	0	2	E	C	1
1000	0001	0011	0011 –	0110	0001	0011	0001	0101	0011	1100	0000	0010	1110	1100	0001

Translated Card Data

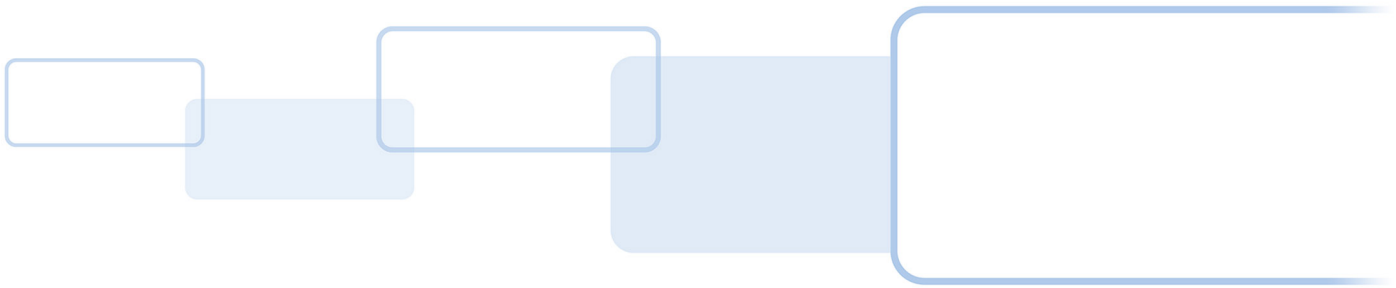
Agency Code = 1341, System Code = 0001, Credential Number = 987654, CS = 1, ICI = 1, PI = 1234567890, OC = 1, OI = 1341, POA = 1

Note: As per *Section 5 GUID for PIV, PIV-I, and CIV*, the UUID output from the pivCLASS reader is a fallback for when the reader determines that the credential is not a PIV. This option is not a standalone option in the reader.

9 Abbreviated terms

Term	Definition
BCD	Binary Coded Data
CHUID	Card Holder Unique ID
CIV	Commercial Identity Verification
FASC-N	Federal Agency Smart Credential - Number
FICAM	Federal Identity, Credential, and Access Management
FIPS-201	Federal Information Processing Standard Publication 201
GSA APL	General Services Administration Approved Products List
GUID (or UUID)	Globally Unique Identifier (or Universally Unique Identifier)
HMAC	Hash-based Message Authentication Code
HSPD-12	Homeland Security Presidential Directive 12
LSB	Least Significant Bit
MSB	Most Significant Bit
OSDP	Open Supervised Device Protocol
PACS	Physical Access Control System
PAM	pivCLASS Authentication Module
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification – Interoperable

This page is intentionally left blank.



hidglobal.com