pivCLASS®

FIPS- 201 Reader Operation and Output Selections

APPLICATION NOTE

6090- 905, F.0
February 2014

© 2006-2014 HID Global Corporation/ASSA ABLOY AB. All rights reserved.
# Contents

1 Overview ........................................................................................................................................... 4

2 CHUID Definition ............................................................................................................................ 4

3 FASC-N and FIPS-201 Overview .................................................................................................... 5

   3.1 TIG-SCEPACS FASC-N Example ......................................................................................... 5

4 FIPS-201 PIV Application Processing ........................................................................................... 8

   4.1 Data Access 8

   4.2 General Data Formatting ..................................................................................................... 8

      4.2.1 General Reader Message Construction ...................................................................... 9

5 GUID for PIV, PIV-I and CIV ........................................................................................................ 9

6 User Feedback ............................................................................................................................ 9

7 Legacy Nomenclature ................................................................................................................... 9

8 Example Output Options ............................................................................................................. 10

   8.1 40 Bit BCD Output (LSB) ................................................................................................. 10

   8.2 40 Bit BCD Output (Reverse or MSB) ............................................................................. 10

   8.3 64 Bit BCD Output (LSB) ............................................................................................... 10

   8.4 64 Bit BCD Output (Reverse, or MSB) - Supported by PAM ........................................ 11

   8.5 75 Bit Output - Supported by PAM ................................................................................. 11

   8.6 128 Bit BCD Output (LSB) ........................................................................................... 11

   8.7 128 Bit BCD Output (Reverse, or MSB) - Supported by PAM ......................................... 12

   8.8 200 Bit Output - Supported by PAM ............................................................................. 12

   8.9 128 Bit UUID Output - Supported by PAM ...................................................................... 13
Trademarks
HID GLOBAL, HID, the HID logo and pivCLASS are the trademarks or registered trademarks of HID Global Corporation, or its licensors, in the U.S. and other countries.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Description</th>
<th>Document Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/27/14</td>
<td>B. Fontana, B. Dulude, B. Stiller</td>
<td>Updating 128bit MSB, remove HMAC, clarification on MSB, LSB, BCD – App Note now supports pivCLASS only</td>
<td>F.0</td>
</tr>
<tr>
<td>8/10/09</td>
<td>TMP</td>
<td>Modify document per ENG specification. Update examples w/ BCD and R-BCD nomenclature. General Cleanup</td>
<td>E.0</td>
</tr>
</tbody>
</table>

Contacts

<table>
<thead>
<tr>
<th>North America</th>
<th>Asia Pacific</th>
<th>Europe, Middle East &amp; Africa</th>
</tr>
</thead>
<tbody>
<tr>
<td>15370 Barranca Parkway</td>
<td>19/F 625 King’s Road</td>
<td>Phoenix Road</td>
</tr>
<tr>
<td>Irvine, CA 92618</td>
<td>North Point, Island East</td>
<td>Haverhill, Suffolk CB9 7AE</td>
</tr>
<tr>
<td>USA</td>
<td>Hong Kong</td>
<td>England</td>
</tr>
<tr>
<td>Phone: 800 237 7769</td>
<td>Phone: 852 3160 9800</td>
<td>Phone: +44 1440 714 850</td>
</tr>
<tr>
<td>Fax: 949 732 2120</td>
<td>Fax: 852 3160 4809</td>
<td>Fax: +44 1440 714 840</td>
</tr>
</tbody>
</table>

Support: [support.hidglobal.com](mailto:support.hidglobal.com)

Acronym List

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCD</td>
<td>Binary Coded Data</td>
</tr>
<tr>
<td>CHUID</td>
<td>Card Holder Unique ID</td>
</tr>
<tr>
<td>FASC-N</td>
<td>Federal Agency Smart Credential – Number</td>
</tr>
<tr>
<td>PAM</td>
<td>pivCLASS Authentication Module</td>
</tr>
<tr>
<td>PIV</td>
<td>Personal Identity Verification</td>
</tr>
</tbody>
</table>
1 Overview

This document outlines the FIPS-201 PIV output options available with the pivCLASS FIPS-201 readers. pivCLASS FIPS-201 readers comply with the FIPS-201 2.1 Interoperability Standard and PACS 2.2 Implementation Guidelines. pivCLASS FIPS-201 readers are available in either low or medium assurance levels. Also described are pivCLASS FIPS-201 reader operation and definitions of the FIPS-201 data container.

For format output ordering information, refer to the pivCLASS How to Order Guide at www.hidglobal.com.

2 CHUID Definition

Agency and technology independent, U.S. Presidential directive HSPD-12 defines a common data model for Personal Identity Verification (PIV). Table 1 shows the Card Holder Unique ID (CHUID) data model.

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

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Max Bytes</th>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Length</td>
<td>2</td>
<td>EE</td>
<td>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.</td>
</tr>
<tr>
<td>FASC-N</td>
<td>25</td>
<td>30</td>
<td>Mandatory TLV record – Federal Agency Smart Credential Number</td>
</tr>
<tr>
<td>Agency Code</td>
<td>4</td>
<td>31</td>
<td>Optional TLV record – Recommended when the SP 800-87 code for the government agency issuing the credential contains alpha characters.</td>
</tr>
<tr>
<td>Organizational ID</td>
<td>4</td>
<td>32</td>
<td>Optional TLV record – Recommended when the SP 800-87 code for the FASC-N OI field contains alpha characters.</td>
</tr>
<tr>
<td>DUNS</td>
<td>9</td>
<td>33</td>
<td>Optional TLV record – Recommended when the FASC-N agency code = 9999. D&amp;B DUNS number for non-Federal FASC-N issuer.</td>
</tr>
</tbody>
</table>
| GUID               | 16        | 34  | Mandatory TLV record - Shall include 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                |           |     | 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.

In Technical Implementation Guidance – Smart Card Enabled Physical Access Control Systems (TIG SCEPACS) Version 2.3, dated December 20, 2005, the FASC-N Number Format is defined as an eventual, compatible replacement for the SEIWG-012 credential number. At the time of that writing, the FIPS 201 data model was not complete.

The FIPS-201 application is intended to be manufacturer/technology agnostic. The only requirement is the credential must be compatible with all four parts of the ISO-14443 specification. The Application Processing chapter provides specifics on various way 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

Table 2 - Definition of FASC-N Contents

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

The following table defines the packed BCD 4-Bit decimal format with odd parity calculated over the preceding BCD cluster.  

The following provides HID TIG SCEPACS BCD definitions.

**BCD coding is “least significant bit first and parity bit last”**

- 7 = 1110  
  This means the LSB is the first to be sent from the reader

**Reverse BCD coding is the opposite of this coding**

- 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

<table>
<thead>
<tr>
<th>b0</th>
<th>b1</th>
<th>b2</th>
<th>b3</th>
<th>Parity</th>
<th>Corresponding character</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Start Sentinel</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Field Separator</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>End Sentinel</td>
</tr>
</tbody>
</table>

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). 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

```
11010 00001 00001 11001 01000 10110 00001 00001 00001 10000 10110
00011 10110 00001 10110 10000 10110 10000 10000 10000 10000 10000
10011 00000 10000 10000 10000 01000 01000 01000 01000 01000 01000
10011 11111 10101
```

Example: FASC-N parsed by Character

```
11010 00001 00001 11001 01000 10110 00001 00001 00001 10000 10110
SS 0 0 3 2 FS 0 0 0 1 FS
00001 10011 01000 00100 00100 01011 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-14443, Type A credentials and pivCLASS FIPS-201 readers implement the card activation process as detailed in Figure 1 of the specification, part 4. ISO-14443, 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 and serial (when available) output ports. For data lengths not ending on a byte boundary, serial data output is left-padded with zeros. 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

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

5 GUID for PIV, PIV-I and CIV

PIV-I and CIV credentials are issued by non-Federal or commercial agencies. Because 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 4412.

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 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 read 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 list shows 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 HTOG 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 http://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 0001-0001-1001 1000 0111 0110 0101 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

1-00010100111101-00000000000001-111100010010000110-1001100101111000100111-1

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 0011 1100 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

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

Translated Card Data

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

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