



9292 Jeronimo Road
Irvine, CA 92618-1905



FIPS201 Reader Output Selections

Application Note

6090-905, D.0



Version History

Date	Author	Description	Version
6/12/08	LJH	Corrected errors in 40, 64, and 128 bit outputs	D
8/25/06	NDC	Corrected errors in 75 and 200 bit output	C
6/27/06	LJH	Modified Example (adding Expiration Date) and added Wiegand 75 MSB. Removed disclaimer.	B
1/18/06	JB and NDC	Corrected errors in 128 bit outputs	A.2
8/09/05	JMB	Updated HMAC Flow Chart	A.1
1/06/05	LJH	Re-formatted and re-issued	A.0

Contacts

North America

9292 Jeronimo Road
Irvine, CA 92618-1905
USA

Phone: (800) 237-7769
Support: 1-800-237-7339
Fax: (949) 598-1690
Email: tech@hidglobal.com

Asia Pacific

19/F 625 King's Road
North Point, Island East
Hong Kong

Phone: 852 3160 9802
Support: 852 3160 9833
Fax: 852 3160 4809
Email: asiasupport@hidglobal.com

Europe, Middle East and Africa

Phoenix Road
Haverhill, Suffolk CB9 7AE
England

Main: +44 (0) 1440 714 850
Support: +44 (0) 1440 711 822
Fax: +44 (0) 1440 714 840
Email: eusupport@hidglobal.com

Contents

1	Overview	4
2	FASC-N	4
3	FIPS201 Low Assurance Output Options.....	5
4	40 Bit FASC-N (MSB or LSB)	6
5	64 Bit FASC-N (MSB or LSB)	6
6	75 Bit FASC-N (MSB or LSB)	6
7	128 Bit FASC-N (MSB or LSB)	7
8	200 Bit FASC-N	7
9	FIPS201 Medium Assurance Output Options	8
10	32 Bit HMAC + 40 (MSB or LSB) Bit FASC-N	9
11	32 Bit HMAC + 64 (MSB or LSB) Bit FASC-N	9
12	32 Bit HMAC + 128 (MSB or LSB only) Bit FASC-N.....	10
13	32 Bit HMAC + 200 Bit FASC-N.....	10
14	80 bit Combined 48 Bit FASC-N + 32 Bit HMAC	11



1 Overview

This document outlines the output options that are available with the HID Global **iCLASS** FIPS201 readers. These FIPS201 readers comply with the FIPS201 2.1 Interoperability standard and PACS 2.2 Implementation guidelines. The FIPS201 readers are available in either Low or Medium Assurance levels.

For ordering information, refer to the HTOG (How to order guide) at <http://www.hidglobal.com>.

2 FASC-N

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. (e.g. DoD EDI PN ID)
OC	1	ORGANIZATIONAL CATEGORY 1 - Federal Government Agency 2 - State Government Agency 3 - Commercial Enterprise 4 - Foreign Government
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



Field name	Length (BCD digits)	Field description
		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

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

3 FIPS201 Low Assurance Output Options

- 40 Bits System + Credential
- 64 Bits Agency + System + Credential + Series + Issue
- 75 Bits Agency + System + Credential + Expiration Date
- 128 Bits Agency + System + Credential + Series + Issue + Pers Inden + Org Cat + Org Ind + Pers/Org
- 200 Bits Complete FASC-N number

Example:

Agency	1111	Pers. Ident.	6666666666
System	2222	Org Cat	7
Credential	333333	Org Ident	8888
Series	4	Pers/Org	9
Issue	5	LRC	6
		Expiration Date	12312010

3.1 Card Data (Hex)

3019D421085908422D9CE739CD896AD9AD6B5AD6B5ADE084214FED

Note: Optional Tag buffer (EE 02 04 1E), not transmitted.



4 40 Bit FASC-N (MSB or LSB)

System + Credential

4.1 LSB

0100010001000100110011001100110011001100

4.2 MSB

0010001000100010001100110011001100110011

5 64 Bit FASC-N (MSB or LSB)

Agency + System + Credential + Series + Issue

5.1 LSB

1000100010001000010001000100010011001100110011001100110000101010

5.2 MSB

000100010001000100100010001000110011001100110011001101000101

6 75 Bit FASC-N (MSB or LSB)

6.1 MSB

Agency + System + Credential + Expiration Date

1111222233333320101231

Even Parity (first 37 bits) + 00010001010111 + 00100010101110 +
01010001011000010101 + 1001100101011100001101111 + Odd Parity

100010001010111001000101011100101000101100001010110011001010111000011
011110

7 128 Bit FASC-N (MSB or LSB)

Agency + System + Credential + Series + Issue + Pers Inden + Org Cat + Org Ind + Pers/Org

7.1 LSB

```
1000100010001000010001000100010011001100110011001100110000101010
01100110011001100110011001100110011001100110111000010001000100011001
```

7.2 MSB

```
0001000100010001001000100010001000110011001100110011001101000101
0110011001100110011001100110011001100110011110001000100010001001
```

8 200 Bit FASC-N

8.1 Complete FASC-N number

```
3019D421085908422D9CE739CD896AD9AD6B5AD6B5ADE084214FED
110101000010000100001000010110010000100001000010001011011001110011100
111001110011100110110001001011010101100110101101011010110101101011
0101101011010110101101111000001000010000100001010011111101101
```

8.2 FASC-N parsed by Character

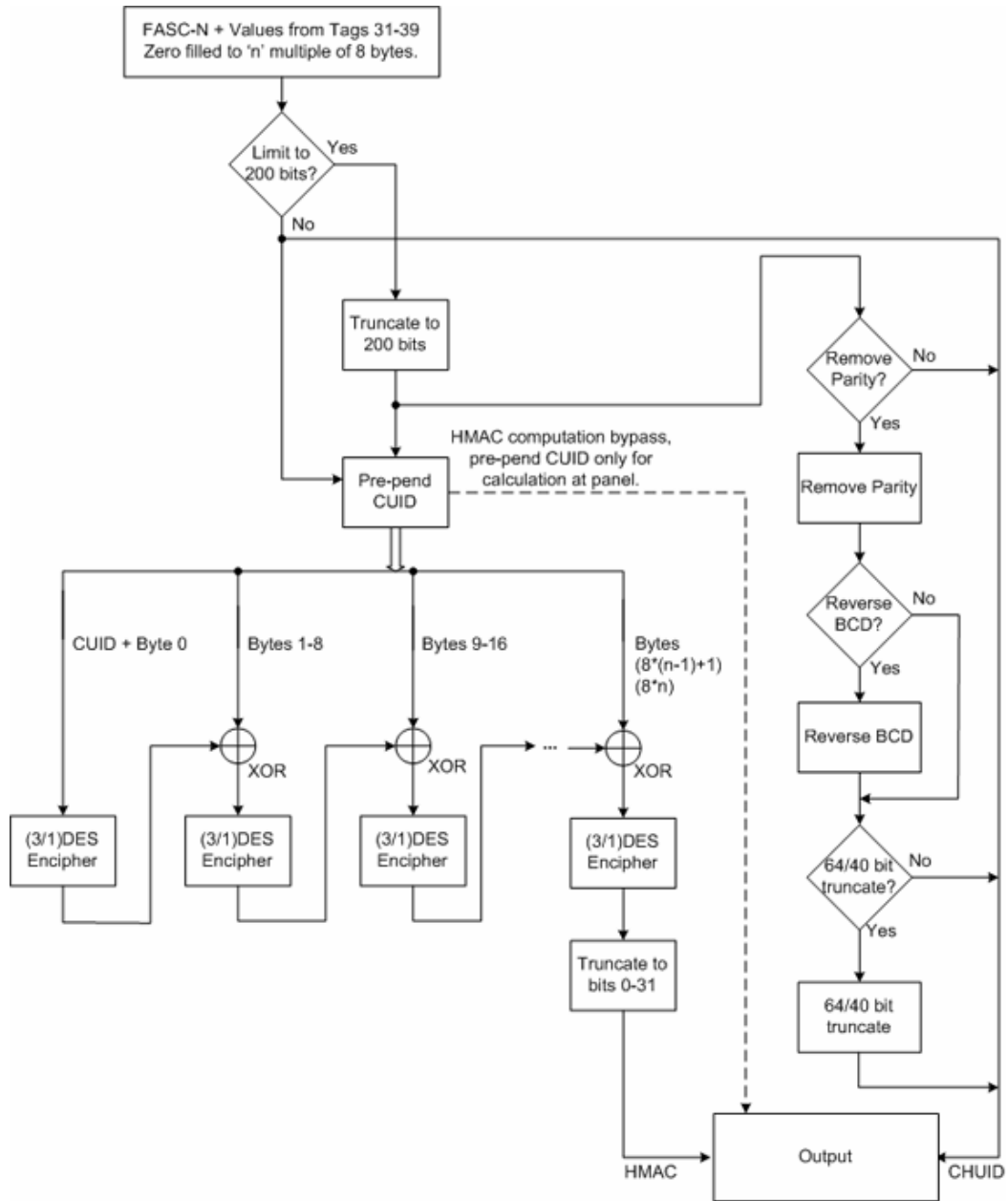
<u>11010</u>	<u>10000</u>	<u>10000</u>	<u>10000</u>	<u>10000</u>	<u>10110</u>	<u>01000</u>	<u>01000</u>	<u>01000</u>	<u>01000</u>	<u>10110</u>
SS	1	1	1	1	FS	2	2	2	2	FS
<u>11001</u>	<u>11001</u>	<u>11001</u>	<u>11001</u>	<u>11001</u>	<u>11001</u>	<u>10110</u>	<u>00100</u>	<u>10110</u>	<u>10101</u>	<u>10110</u>
3	3	3	3	3	3	FS	4	FS	5	FS
<u>01101</u>	<u>01101</u>	<u>01101</u>	<u>01101</u>	<u>01101</u>	<u>01101</u>	<u>01101</u>	<u>01101</u>	<u>01101</u>	<u>01101</u>	<u>01110</u>
6	6	6	6	6	6	6	6	6	6	7
<u>10000</u>	<u>10000</u>	<u>10000</u>	<u>10000</u>	<u>10000</u>	<u>11111</u>	<u>01101</u>				
8	8	8	8	9	ES	6				



9 FIPS201 Medium Assurance Output Options

Medium Security adds an HMAC signature to the output. The HMAC verifies the integrity of the card (by use of the CSN) and the contents of the FASC-N and Expiration Date, by calculating a 3DES CBC signature using a site secret key. The result is truncated to 32 bits.

9.1 32 Bit HMAC



9.2 HMAC Example

CSN	04 12 41 41 B4 C4 40
FASC-N	D421085908422D9CE739CD896AD9AD6B5AD6B5ADE084214FED
(BCD)	(B1111D2222 D333333D 4D 5D 6666666666 788889 FD)
3DES KEY	00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
HMAC	AD 83 3E 05
32 Bit HMAC	10101101100000110011111000000101

10 32 Bit HMAC + 40 (MSB or LSB) Bit FASC-N

32 Bit HMAC
40 Bit FASC-N
System + Credential

10.1 MSB

10101101100000110011111000000101 (HMAC) +
0010001000100010001100110011001100110011

10.2 LSB

10101101100000110011111000000101 (HMAC) +
0100010001000100110011001100110011001100

11 32 Bit HMAC + 64 (MSB or LSB) Bit FASC-N

32 Bit HMAC
64 Bit FASC-N
Agency + System + Credential + Series + Issue

11.1 MSB

10101101100000110011111000000101 (HMAC) +
000100010001000100100010001000110011001100110011001101000101

11.2 LSB

10101101100000110011111000000101 (HMAC) +
100010001000100001000100010011001100110011001100110000101010

12 32 Bit HMAC + 128 (MSB or LSB only) Bit FASC-N

32 Bit HMAC

128 Bit FASC-N

Agency + System + Credential + Series + Issue + Pers Inden + Org Cat + Org Ind + Pers/Org

12.1 MSB

10101101100000110011111000000101 (HMAC) +
 0001000100010001001000100010001000110011001100110011001101000101
 011001100110011001100110011001100110011001100110011110001000100010001001

12.2 LSB

10101101100000110011111000000101 (HMAC) +
 100010001000100001000100010011001100110011001100110000101010
 011001100110011001100110011001100110011001100110111000010001000100011001

13 32 Bit HMAC + 200 Bit FASC-N

32 Bit HMAC

Complete FASC-N number

3019D421085908422D9CE739CD896AD9AD6B5AD6B5ADE084B5AFED

10101101100000110011111000000101 (HMAC) +
 110101000010000100001000010110010000100001000010001011011001110011100
 111001110011100110110001001011010101101100110101101011010110101101011
 0101101011010110101101111000001000010000100001010011111101101

14 80 bit Combined 48 Bit FASC-N + 32 Bit HMAC

FASC-N (Agency + System + Credential Number) + HMAC

Modified FASC-N (HMAC replaces PI)

Example

101000011011010001000001000010011001100101010000

10101101100000110011111000000101 HMAC

CUID (CSN) + CHUID

This output provides you the ability to calculate the HMAC at the access controller instead of the reader. (See HMAC Example, page 9)

14.1 CHUID (Card Holder Unique ID)

Data Element	Length (bytes)	Description
Buffer Length	2	Optional 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	Mandatory TLV Record.
Agency Code	4	Optional TLV Record. Recommended when the FIPS-95 code for the government agency issuing the credential contains alpha characters
Organizational Identifier	4	Optional TLV Record. Recommended when the FIPS-95 code for the FASC-N OI field contains alpha characters
DUNS	9	Optional TLV Record. Recommended when the FASC-N Agency Code = 9999. D&B DUNS number for non-federal FASC-N issuer
GUID	16	Optional TLV Record. Issuer defined binary data field may follow formats IPV6, ICON or ICAO
Authentication Key MAP	TBD	Optional TLV Record. May exist for High Assurance Profile applications.
Issuer Asymmetric Signature	TBD	Optional TLV Record. Issuer defined algorithm, public key and signature. May exist for Medium Assurance Profile applications.
LRC	1	Optional TLV Record Longitudinal Redundancy Code