

PIV Reader Output Selection Application Note

Rev. 02

Contents

- 0. Overview of the formats**
 - 1. 75-bit PIV**
 - 2. 107-bit: 75-bit PIV + 32-bit HMAC**
 - 3. 200-bit FASC-N**
 - 4. 200-bit FASC-N with embedded HMAC**
 - 5. 200-bit FASC-N with embedded expiration date**
 - 6. 245-bit: FASC-N with appended expiration date**

0. Overview of the formats

The following table summarizes the various Wiegand output formats available in the XceedID readers:

Format #	Format Name/Description	Available in
01	75-bit PIV	Reader XF1100-PIV Reader XF2100-PIV Reader XF2110-PIV
02	107-bit: 75-bit PIV + 32-bit HMAC	
03	200-bit FASC-N	
04	200-bit FASC-N with embedded HMAC	
05	200-bit FASC-N with embedded expiration date	
06	245-bit: FASC-N with appended expiration date	

1. 75-bit PIV

This Wiegand format is the most compact format available and combines all the required elements of the CHID to be transmitted by the reader:

The 75-bit PIV is represented as:

E AAAAAAAAAAAAAA SSSSSSSSSSSS CCCCCCCCCCCCCCCCCC DDDDDDDDDDDDDDDDDDDDDDDDDDDDD O

Where:

E: *Even parity bit computed over the first 37 bits of data – this is the first bit transmitted*

AAAAAAAAAAAAAAAA: *Agency code (14 bits)*

SSSSSSSSSSSSSS: *Site code (14 bits)*

CCCCCCCCCCCCCCCC: *Credential number (20 bits)*

DDDDDDDDDDDDDDDDDDDDDDDDDDDD: *expiration date YYYYMMDD (25 bits)*

O: *Odd parity bit computed over the last 36 bits of data*

Example of 75-bit PIV Wiegand output:

1 00010100111101 00000000000001 11110001001000000110 1001100101101110001001011 1

Agency code 1341

Site code 1

Credential number 987654

expiration date (YYYYMMDD) 20110411

resulting

2. 107-bit: 75-bit PIV + 32-bit HMAC

This format consists of 107 bits. The 75-bit portion is the same as the portion described in section 1. The 32-bit portion is the HMAC (hash message authentication code) computed for medium assurance. Both portions are concatenated to create a 107-bit output.

3. 200-bit FASC-N

This format outputs the entire FASC-N.

Example of FASC-N:

AC (agency code – 4 digits):	1111
SC (site code – 4 digits):	2222
C# (credential number – 6 digits):	333333

CS (credential series – 1 digit): 4
 ICI (individual credential issue – 1 digit): 5
 PI (person Identifier – 10 digits): 6666666666
 OC (organizational category – 1 digit): 7
 OI (organizational identifier – 4 digits): 8888
 POA (person/organization association – 1 digit): 9

SS: Start sentinel
 FS: Field separator
 ES: End Sentinel
 LRC: Longitudinal redundancy check

Bits 1 thru 50	11010 SS	10000 AGENCY CODE	10000 1111	10000 1111	10000 1111	10110 FS	01000 Site Code	01000 2222	01000 2222	01000 2222
Bits 51 thru 100	10110 FS	11001 CREDENTIAL NUMBER	11001 1111	11001 1111	11001 1111	11001 1111	11001 1111	10110 FS	00100 CS	10110 FS
Bits 101 thru 150	10101 ICI	10110 FS	01101 PI	01101 1111	01101 1111	01101 1111	01101 1111	01101 1111	01101 1111	01101 1111
Bits 151 thru 200	01101 PI	01101 1111	11100 OC	00010 00010	00010 00010	00010 00010	00010 00010	10011 POA	11111 ES	01101 LRC

4. 200-bit FASC-N with embedded HMAC

This format outputs the FASC-N with the HMAC. The HMAC is represented in a 10 digit decimal number and replaces the PI. The LRC is recomputed to account for the change.

Example:

AC (agency code – 4 digits): 1111
 SC (site code – 4 digits): 2222
 C# (credential number – 6 digits): 333333
 CS (credential series – 1 digit): 4
 ICI (individual credential issue – 1 digit): 5
 HMAC (10 digits): 1571179234
 OC (organizational category – 1 digit): 7
 OI (organizational identifier – 4 digits): 8888
 POA (person/organization association – 1 digit): 9

SS: Start sentinel
 FS: Field separator
 ES: End Sentinel
 LRC: Longitudinal redundancy check

Bits 1 thru 50	11010 SS	10000 AGENCY CODE	10000 1111	10000 1111	10000 1111	10110 FS	01000 Site Code	01000 2222	01000 2222	01000 2222
Bits 51 thru 100	10110 FS	11001 CREDENTIAL NUMBER	11001 1111	11001 1111	11001 1111	11001 1111	10110 FS	00100 CS	10110 FS	10110 FS
Bits 101 thru 150	10101 ICI	10110 FS	10000 HMAC	10101 1111	11100 1111	10000 1111	10000 1111	11100 1111	10011 1111	01000 1111
Bits 151 thru 200	11001 HMAC	00100 OC	11100 OC	00010 OI	00010 OI	00010 OI	00010 OI	10011 POA	11111 ES	01110 LRC

5. 200-bit FASC-N with embedded expiration date

This format outputs the FASC-N with the expiration date. The expiration is represented in a 8 digit number (YYYY MM DD) and replaces the 8 least significant digits of the PI. The 2 most significant digits of the PI are replaced with zeros. The LRC is recomputed to account for the change.

Example:

AC (agency code – 4 digits): 1111
 SC (site code – 4 digits): 2222
 C# (credential number – 6 digits): 333333
 CS (credential series – 1 digit): 4
 ICI (individual credential issue – 1 digit): 5
 Expiration date (10 digits): 0020110416 (2011, April 16)
 OC (organizational category – 1 digit): 7
 OI (organizational identifier – 4 digits): 8888
 POA (person/organization association – 1 digit): 9

SS: Start sentinel
 FS: Field separator
 ES: End Sentinel
 LRC: Longitudinal redundancy check

Bits 1 thru 50	11010 SS	10000 AGENCY CODE	10000 1111	10000 1111	10000 1111	10110 FS	01000 Site Code	01000 2222	01000 2222	01000 2222
Bits 51 thru 100	10110 FS	11001 CREDENTIAL NUMBER	11001 1111	11001 1111	11001 1111	11001 1111	10110 FS	00100 CS	10110 FS	10110 FS
Bits 101 thru 150	10101 ICI	10110 FS	00001 Expiration	00001 1111	01000 1111	00001 1111	10000 1111	10000 1111	00001 1111	00100 1111
Bits 151 thru 200	10000 Date	01101 OC	11100 OC	00010 OI	00010 OI	00010 OI	00010 OI	10011 POA	11111 ES	11100 LRC

6. 245-bit: FASC-N with appended expiration date

This output format consists of the entire FASC-N followed by the expiration date. A field separator is placed between the FASC-N and the expiration date. An end sentinel and an updated LRC follow the expiration date.

Example:

AC (agency code – 4 digits): 1341
 SC (site code – 4 digits): 0001
 C# (credential number – 6 digits): 987654
 CS (credential series – 1 digit): 1
 ICI (individual credential issue – 1 digit): 1
 PI (person Identifier – 10 digits): 123456790
 OC (organizational category – 1 digit): 1
 OI (organizational identifier – 4 digits): 1341
 POA (person/organization association – 1 digit): 1
 Expiration Date (8 digits): 20110411 (2011 April 11th)

SS: Start sentinel

FS: Field separator

ES: End Sentinel

LRC: Longitudinal redundancy check

Bits 1 thru 50	11010 SS	10000 AGENCY CODE	11001	00100	10000	10110 <i>FS</i>	00001	00001 Site Code	00001	10000
Bits 51 thru 100	10110 <i>FS</i>	10011	00010	11100	01101	10101	00100	10110 <i>FS</i>	10000 CS	10110 <i>FS</i>
Bits 101 thru 150	10000 ICI	10110 <i>FS</i>	10000	01000	11001	00100	10101 PI	01101	11100	00010
Bits 151 thru 200	10011 PI	00001	10000 OC	10000	11001	00100 OI	10000	10000 POA	10110 <i>FS</i>	01000
Bits 201 thru 245	00001	10000	10000	00001	00100	10000	10000	11111 ES	11000	LRC