z/OS

Cryptographic Services Integrated Cryptographic Service Facility Visa Format Preserving Encryption Updates APAR OA50408

Contents

Chapter 1. Overview

This document describes changes to the Integrated Cryptographic Service Facility (ICSF) product in support of the following Visa format preserving encryption updates:

- Alphabet tables used by Visa Format Preserving Encryption (FPE) for the Visa Data Secure Platform with Point-to-Point Encryption are changed:
  - The Track 1 alphabet is replaced with two alphabet tables:
    - FPE track 1 cardholder name alphabet.
    - FPE track 1 discretionary data alphabet.
  - The VFPE track 2 discretionary data alphabet is new.
  - The base-16 alphabet is changed to an FPE base-15 alphabet.

These changes apply to FMID HCR77B1 and HCR77B0.

This document contains alterations to information previously presented in *z/OS Cryptographic Services ICSF Application Programmer's Guide*, SC14-7508-04.

The technical changes are indicated in this document by a vertical line to the left of the change.

Chapter 2. Update of z/OS Cryptographic Services ICSF Application Programmer's Guide, SC14-7508-04, information

This topic contains updates to the document *z/OS Cryptographic Services ICSF Application Programmer's Guide*, SC14-7508-04, for the Visa format preserving encryption updates provided by this APAR. Refer to this source document if background information is needed.

Format preserving encryption

Format preserving encryption (FPE) is a method of encryption where the resulting cipher text has the same form as the input clear text. The form of the text can vary according to use and the application. One example is a 16 digit credit card number. After using FPE to encrypt a credit card number, the resulting cipher text is another 16 digit number. In this example of the credit card number, the output cipher text is limited to numeric digits only.

The FPE services require some knowledge of the input clear text character set in order to create the appropriate output ciphertext. The CSNBFPEE, CSNBFPED, CSNBFPET, and CSNBPTRE callable services use the following tables to determine valid character sets for the clear text input parameters:

Base-10 alphabet

This alphabet is used when the character set only consists of numbers 0 through 9. The original data type of the source field may be of any type. This alphabet requires the following values to be used in the VFPE algorithm:

```
Number of characters in alphabet('n'): 10
```

Table 1. Base-10 alphabet

FPE alphabet number	Character	ISO 7811 modified 5-bit ASCII	ISO 7811 modified 7-bit ASCII	Normal data type encoding		
				4-bit binary coded decimal	7-bit ASCII	8-bit EBCDIC
0	0	10000	0010000	0000	0110000	11110000
1	1	00001	1010001	0001	0110001	11110001
2	2	00010	1010010	0010	0110010	11110010
3	3	10011	0010011	0011	0110011	11110011
4	4	00100	1010100	0100	0110100	11110100
5	5	10101	0010101	0101	0110101	11110101
6	6	10110	0010110	0110	0110110	11110110
7	7	00111	1010111	0111	0110111	11110111
8	8	01000	1011000	1000	0111000	11111000
9	9	11001	0011001	1001	0111001	11111001

FPE base-15 alphabet

Cards are encoded with the special ISO 7811 modified 5-bit ASCII encoding for track 2. This data type allows parity checking of the digits. Many systems require this encoding to be converted into standard data types for processing. Other data fields may use FPE base-15 encoding and would use this same alphabet when performing VFPE. These data types support values of 0 through 9 and A through F.

VFPE requires translation of the characters of the FPE alphabet number prior to encryption. Therefore, any of the data types shown in Table 2 are supported. Decryption may use the same or a different data type than the original encoding. This alphabet requires the following values to be used in the VFPE algorithm:

```
Number of characters in alphabet('n'): 15
```

Table 2. FPE base-15 alphabet

FPE alphabet number	ISO 7811 modified 5-bit ASCII encoding		Normal data type encoding			
	Character	Binary	Character	4-bit binary coded decimal	7-bit ASCII	8-bit EBCDIC
0	0	10000	0	0000	0110000	11110000
1	1	00001	1	0001	0110001	11110001
2	2	00010	2	0010	0110010	11110010
3	3	10011	3	0011	0110011	11110011
4	4	00100	4	0100	0110100	11110100
5	5	10101	5	0101	0110101	11110101
6	6	10110	6	0110	0110110	11110110
7	7	00111	7	0111	0110111	11110111
8	8	01000	8	1000	0111000	11111000
9	9	11001	9	1001	0111001	11111001
10	:	11010	A	1010	1000001	11000001
11	;	01011	B	1011	1000010	11000010
12	<	11100	C	1100	1000011	11000011
13	=	01101	D	1101	1000100	11000100
14	>	01110	E	1110	1000101	11000101

FPE track 1 cardholder name alphabet

This alphabet requires the following values to be used in the VFPE algorithm:

```
Number of characters in alphabet('n'): 45
```

Table 3. FPE track 1 cardholder name alphabet

FPE alphabet number	Character	ISO 7811 modified 7-bit ASCII	Standard data types 7-bit ASCII	Standard data types 8-bit ASCII
0	space	1000000	0100000	01000000
1	#	1000011	0100011	01111011

Table 3. FPE track 1 cardholder name alphabet (continued)

FPE alphabet number	Character	ISO 7811 modified 7-bit ASCII	Standard data types 7-bit ASCII	Standard data types 8-bit ASCII
2	$	0000100	0100100	01011011
3	(	0001000	0101000	01001101
4	)	1001001	0101001	01011101
5	-	0001101	0101101	01100000
6	0	0010000	0110000	11110000
7	1	1010001	0110001	11110001
8	2	1010010	0110010	11110010
9	3	0010011	0110011	11110011
10	4	1010100	0110100	11110100
11	5	0010101	0110101	11110101
12	6	0010110	0110110	11110110
13	7	1010111	0110111	11110111
14	8	1011000	0111000	11111000
15	9	0011001	0111001	11111001
16	A	1100001	1000001	11000001
17	B	1100010	1000010	11000010
18	C	0100011	1000011	11000011
19	D	1100100	1000100	11000100
20	E	0100101	1000101	11000101
21	F	0100110	1000110	11000110
22	G	1100111	1000111	11000111
23	H	1101000	1001000	11001000
24	I	0101001	1001001	11001001
25	J	0101010	1001010	11010001
26	K	1101011	1001011	11010010
27	L	0101100	1001100	11010011
28	M	1101101	1001101	11010100
29	N	1101110	1001110	11010101
30	O	0101111	1001111	11010110
31	P	1110000	1010000	11010111
32	Q	0110001	1010001	11011000
33	R	0110010	1010010	11011001
34	S	1110011	1010011	11100010
35	T	0110100	1010100	11100011
36	U	1110101	1010101	11100100
37	V	1110110	1010110	11100101
38	W	0110111	1010111	11100110
39	X	0111000	1011000	11100111

Table 3. FPE track 1 cardholder name alphabet (continued)

FPE alphabet number	Character	ISO 7811 modified 7-bit ASCII	Standard data types 7-bit ASCII	Standard data types 8-bit ASCII
40	Y	1111001	1011001	11101000
41	Z	1111010	1011010	11101001
42	[	0111011	1011011	10111010
43	\	1111100	1011100	11100000
44	]	111110	1011101	10111011

FPE track 1 discretionary data alphabet

This alphabet requires the following values to be used in the VFPE algorithm:

```
Number of characters in alphabet('n'): 47
```

Table 4. FPE track 1 discretionary data alphabet

FPE alphabet number	Character	ISO 7811 modified 7-bit ASCII	Standard data types 7-bit ASCII	Standard data types 8-bit ASCII
0	space	1000000	0100000	01000000
1	#	1000011	0100011	01111011
2	$	0000100	0100100	01011011
3	(	0001000	0101000	01001101
4	)	1001001	0101001	01011101
5	-	0001101	0101101	01100000
6	.	0001110	0101110	01001011
7	/	1001111	0101111	01100001
8	0	0010000	0110000	11110000
9	1	1010001	0110001	11110001
10	2	1010010	0110010	11110010
11	3	0010011	0110011	11110011
12	4	1010100	0110100	11110100
13	5	0010101	0110101	11110101
14	6	0010110	0110110	11110110
15	7	1010111	0110111	11110111
16	8	1011000	0111000	11111000
17	9	0011001	0111001	11111001
18	A	1100001	1000001	11000001
19	B	1100010	1000010	11000010
20	C	0100011	1000011	11000011
21	D	1100100	1000100	11000100
22	E	0100101	1000101	11000101
23	F	0100110	1000110	11000110
24	G	1100111	1000111	11000111

Table 4. FPE track 1 discretionary data alphabet (continued)

FPE alphabet number	Character	ISO 7811 modified 7-bit ASCII	Standard data types 7-bit ASCII	Standard data types 8-bit ASCII
25	H	1101000	1001000	11001000
26	I	0101001	1001001	11001001
27	J	0101010	1001010	11010001
28	K	1101011	1001011	11010010
29	L	0101100	1001100	11010011
30	M	1101101	1001101	11010100
31	N	1101110	1001110	11010101
32	O	0101111	1001111	11010110
33	P	1110000	1010000	11010111
34	Q	0110001	1010001	11011000
35	R	0110010	1010010	11011001
36	S	1110011	1010011	11100010
37	T	0110100	1010100	11100011
38	U	1110101	1010101	11100100
39	V	1110110	1010110	11100101
40	W	0110111	1010111	11100110
41	X	0111000	1011000	11100111
42	Y	1111001	1011001	11101000
43	Z	1111010	1011010	11101001
44	[	0111011	1011011	10111010
45	\	1111100	1011100	11100000
46	]	0111110	1011101	10111011

VFPE track 2 discretionary data alphabet

This alphabet requires the following values to be used in the VFPE algorithm:

```
Number of characters in alphabet('n'): 10
```

Table 5. VFPE track 2 discretionary data alphabet

VFPE alphabet number	Character	ISO 7811 modified 5-bit ASCII	ISO 7811 modified 7-bit ASCII	Normal data type encoding		
				4-bit	7-bit ASCII	8-bit EBCDIC
0	0	10000	0010000	0000	0110000	11110000
1	1	00001	1010001	0001	0110001	11110001
2	2	00010	1010010	0010	0110010	11110010
3	3	10011	0010011	0011	0110011	11110011
4	4	00100	1010100	0100	0110100	11110100
5	5	10101	0010101	0101	0110101	11110101
6	6	10110	0010110	0110	0110110	11110110
7	7	00111	1010111	0111	0110111	11110111

Table 5. VFPE track 2 discretionary data alphabet (continued)

VFPE alphabet number	Character	ISO 7811 modified 5-bit ASCII	ISO 7811 modified 7-bit ASCII	Normal data type encoding		
				4-bit	7-bit ASCII	8-bit EBCDIC
8	8	01000	1011000	1000	0111000	11111000
9	9	11001	0011001	1001	0111001	11111001

Printed in USA