

To: INCITS Technical Committee T10  
 From: Kevin Butt and Sivan Tal, IBM Corporation  
 Date: February 12, 2008  
 Document: T10/08-101r0 : SPC-4 – CbCS field byte alignment changes

# Introduction

Several fields in CbCS structures are not aligned for efficient use. In general, aligning fields of size X to X byte boundary makes implementations more efficient.

Key:

Added or changed text

Deleted text

{{Proposer's note}}

# Revision History

r0 Initial revision

# Proposed changes in SPC-4

## 7.6.x Capabilities CbCS page

Table x1 the format of the Capabilities CbCS page.

{{Added some reserved field padding to make all the 4 byte fields 4 byte aligned.

The total addition is 4 bytes plus 2 bytes per supported CbCS method.}}

Table x1 – Capabilities CbCS page format

Byte \ Bit	7	6	5	4	3	2	1	0
0	(MSB) PAGE CODE (0010h) -----							
1	(LSB)							
2	(MSB) PAGE LENGTH ( $i*4+j*4+k*4+12$ ) -----							
3	(LSB)							
4	GKS	LUKS	GCMS	LUCMS	Reserved			
5	Reserved							
6	(MSB) Number of supported CbCS methods (i) -----							
7	(LSB)							
8	Reserved (first) -----							
9								
10	(MSB) SUPPORTED CBCS METHOD (first) -----							

Byte \ Bit	7	6	5	4	3	2	1	0	
11	(LSB)								
	.								
$i*4+4$	(MSB)	Reserved (last)						(LSB)	
$i*4+5$									
$i*4+6$	SUPPORTED CBCS METHOD (last)								
$i*4+7$									
$i*4+8$	Reserved								
$i*4+9$									
$i*4+10$	(MSB)	Number of supported integrity check value algorithms (j)						(LSB)	
$i*4+11$									
$i*4+12$	(MSB)	SUPPORTED INTEGRITY CHECK VALUE ALGORITHM						(LSB)	
$i*4+15$	(first)								
	.								
$i*4+j*4+8$	(MSB)	SUPPORTED INTEGRITY CHECK VALUE ALGORITHM						(LSB)	
$i*4+j*4+11$	(last)								
$i*4+j*4+12$	Reserved								
$i*4+j*4+13$									
$i*4+j*4+14$	(MSB)	Number of supported D-H groups (k)						(LSB)	
$i*4+j*4+15$									
$i*4+j*4+16$	SUPPORTED D-H GROUP (first)								
$i*4+j*4+19$	(LSB)								
	.								
$i*4+j*4+k*4+12$	SUPPORTED D-H GROUP (last)								
$i*4+j*4+k*4+15$	(LSB)								

## 7.6.y Attributes CbCS page

Table x2 specifies the format of the Attributes CbCS page.

{{Added 'reserved' fields to make fields byte aligned for their size.}}

{{Do we want to make the key identifier 8 byte aligned? Or can we assume they're strings?}}

Table x2 – Attributes CbCS page format

Byte \ Bit	7	6	5	4	3	2	1	0
0	(MSB)	PAGE CODE (0010h)						(LSB)
1								
2	(MSB)	PAGE LENGTH (n-3)						(LSB)
3								
4	(MSB)	CBCS METHOD						(LSB)
5								
6		Reserved						
7								
8	(MSB)	POLICY ACCESS TAG						(LSB)
11								
12		Reserved						
15								
16	(MSB)	MASTER KEY IDENTIFIER						(LSB)
23								
24	(MSB)	WORKING KEY IDENTIFIER 0						(LSB)
31								
		.						
		.						
		.						
144	(MSB)	WORKING KEY IDENTIFIER 15						(LSB)
151								
152	(MSB)	CLOCK						(LSB)
157								
158		Reserved						
159		SECURITY TOKEN LENGTH						
160	(MSB)	SECURITY TOKEN						(LSB)
n								

### 7.6.z Set attributes CbCS page

Table x3 specifies the format of the Set Attributes CbCS page.

{{Added 2 reserved bytes to make POLICY ACCESS TAG 4 byte aligned.}}

Table x3 – Set attributes CbCS page format

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB) PAGE CODE (0011h) -----							
1	----- (LSB)							
2	(MSB) PAGE LENGTH (8) -----							
3	----- (LSB)							
4	(MSB) CBCS METHOD -----							
5	----- (LSB)							
6	-----							
7	----- Reserved -----							
8	(MSB) POLICY ACCESS TAG -----							
11	----- (LSB)							

### 7.6.w Set Key CbCS page

Table x4 specifies the Set Key CbCS page format.

{{Added 2 reserved bytes to make KEY IDENTIFIER 8 byte aligned.}}

Table x4 - Key CbCS page format

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB) PAGE CODE (0012h) -----							
1	----- (LSB)							
2	(MSB) PAGE LENGTH (32) -----							
3	----- (LSB)							
4	-----							
6	----- Reserved -----							
7	----- Reserved -----				KEY VERSION			
8	-----							
15	----- KEY IDENTIFIER -----							
16	-----							
35	----- SEED -----							

### 7.6.v Set Master Key, Seed Exchange CbCS page

Table x5 specifies the Set Master Key, Seed Exchange CbCS page format.

{{Added 2 reserved bytes to make DH DATA LENGTH 4 byte aligned.}}

Table x5 - Set Master Key, Seed Exchange CbCS page format

Byte \ Bit	7	6	5	4	3	2	1	0
0	(MSB) PAGE CODE (0013h) (LSB)							
1								
2	(MSB) PAGE LENGTH (n-3) (LSB)							
3								
4	(MSB) DH GROUP (LSB)							
5								
6	Reserved							
7								
8	(MSB) DH DATA LENGTH (LSB)							
11								
12	DH DATA							
n								

### 7.6.u Set Master Key, Change Master Key CbCS page

Table x6 specifies the format of the Set Master Key, Change Master Key CbCS page.

{{Added 4 reserved bytes to make KEY IDENTIFIER 8 byte aligned.}}

Table x6 – Set Master Key, Change Master Key CbCS page format

Bit Byte	7	6	5	4	3	2	1	0	
0	(MSB)	PAGE CODE (0014h)							
1								(LSB)	
2	(MSB)	PAGE LENGTH (n-3)							
3								(LSB)	
4		Reserved							
7									
8	(MSB)	KEY IDENTIFIER							
15								(LSB)	
16	(MSB)	APPLICATION CLIENT DATA LENGTH (k-19)							
19								(LSB)	
20		APPLICATION CLIENT DH DATA							
k									
k+1	(MSB)	DEVICE SERVER DATA LENGTH (n-(k+4))							
k+4								(LSB)	
k+5		DEVICE SERVER DH DATA							
n									

## 6.x.2 CbCS capability format

The format of the CbCS capability descriptor is defined in Table x7.

{{Reordered fields to improve alignment.}}

Table 20 - Capability descriptor format

Bit Byte	7	6	5	4	3	2	1	0	
0	DESIGNATION TYPE				KEY VERSION				
1	CBCS METHOD								
2	(MSB)	<del>INTEGRITY CHECK VALUE ALGORITHM</del>							
7		CAPABILITY EXPIRATION TIME						(LSB)	
8	(MSB)	<del>CAPABILITY EXPIRATION TIME</del>							
11		INTEGRITY CHECK VALUE ALGORITHM						(LSB)	
12		PERMISSIONS BIT MASK descriptor							
15									
16	(MSB)	POLICY ACCESS TAG							
19								(LSB)	
20		Designation descriptor							
55									
56		DISCRIMINATOR							
71									

END OF DOCUMENT