ENDL
TEXAS

Date: 10 January 2008
To: T10 Technical Committee
From: Ralph O. Weber
Subject: SA Creation corrections and clarifications

Introduction

Revision History

r0 Initial revision

Unless otherwise indicated additions are shown in blue, deletions in ~~red strikethrough~~, and comments in green.

The subclause and table numbers in this revision may not match SPC-4 r12. An r1 will be uploaded to correct this as soon as SPC-4 r12 is uploaded.

Proposed Changes in SPC-4

{{Sorry. The first change is too big to fit on this page.}}

18484 Preston Road, Suite 102 PMB 178, Dallas, TX 75252 214-912-1373 972-596-2775 Fx ENDL_TX@computer.org

Change 1 – SK_xx key names too narrowly defined

{{Several of the SK_xx key names have meanings beyond those applied in IKEv2-SCSI SA creation. The following minimal changes should be made to reflect this in 5.13.4.4. A more complex change would be to add a second table for the SA key names, but this might not be helpful because the SK_xx names are the same in both cases.}}

Table 54 — IKEv2-SCSI shared key and SA shared key names

Name	Description	SA parameter (see 3.1.113) that stores this shared key
Shared keys used only during Authentication step		
SK_pi	The shared key used to construct the Authentication payload (see 7.6.3.5.6) for the SECURITY PROTOCOL OUT parameter list in the Authentication step (see 5.13.4.9.2).	shall not be stored in any SA parameter
SK_pr	The shared key used to construct the Authentication payload for the SECURITY PROTOCOL IN parameter data in the Authentication step.	
Shared keys used during IKEv2-SCSI SA creation and management		
SK_ai [a]	The shared key used to integrity check the Encrypted payload in the SECURITY PROTOCOL OUT parameter list in the: a) Authentication step; and b) IKEv2-SCSI Delete operation (see 5.13.4.13).	MGMT_DATA
SK_ar [a]	The shared key used to integrity check the Encrypted payload (see 7.6.3.5.10) in the SECURITY PROTOCOL IN parameter data in the Authentication step (see 5.13.4.9.3).	
SK_ei [a]	The shared key used to encrypt the Encrypted payload in the SECURITY PROTOCOL OUT parameter list in the: a) Authentication step; and b) IKEv2-SCSI Delete operation.	
SK_er [a]	The shared key used to encrypt the Encrypted payload in the SECURITY PROTOCOL IN parameter data in the Authentication step.	
Shared key used to construct the SA keys (see 3.1.112)		
SK_d	The shared key material that is used as input to the KDF that generates the KEYMAT SA parameter (see 3.1.113) bytes for the SA.	KEY_SEED

[a] The SA shared keys (see 3.1.112) SK_ai, SK_ar, SK_ei, and SK_er are stored in the KEYMAT SA parameter. SK_ai is intended to be used for integrity checking data in a Data-Out Buffer. SK_ar is intended to be used for integrity checking data in a Data-In Buffer. SK_ei is intended to be used for encrypting data in a Data-Out Buffer. SK_er is intended to be used for encrypting data in a Data-In Buffer.

Change 2 – Use Header DS SAI, not cryptographic algorithms

5.13.4.8.3 Key Exchange step SECURITY PROTOCOL IN command

…

If the Key Exchange step SECURITY PROTOCOL IN command (see 5.13.4.8.3) completes with GOOD status, the application client should copy the device server's SAI from the IKE_SA DEVICE SERVER SAI field in the IKEv2-SCSI header ~~SAI field in the IKEv2-SCSI SA Cryptographic Algorithms payload~~ to the state it is maintaining for the IKEv2-SCSI CCS.

Except for the SAI field, the ~~The~~ application client should compare the ~~other~~ fields in the IKEv2-SCSI SA Cryptographic Algorithms payload and the IKEv2-SCSI SAUT Cryptographic Algorithms payload, if any, to the values sent in the Key Exchange step SECURITY PROTOCOL OUT command (see 5.13.4.8.2). If the application client detects differences in the contents of the payloads other than in the SAI field, the application client should abandon the IKEv2-SCSI CCS and notify the device server that the IKEv2-SCSI CCS is being abandoned as described in 5.13.4.12.

…

5.13.4.9.3 Authentication step SECURITY PROTOCOL IN command

…

The application client should compare the ~~other~~ fields in the IKEv2-SCSI SAUT Cryptographic Algorithms payload to the values sent in the Authentication step SECURITY PROTOCOL OUT command (see 5.13.4.9.2). If the application client detects differences in the contents of the payloads ~~other than in the SAI field~~, the application client should abandon the IKEv2-SCSI CCS and notify the device server that the IKEv2-SCSI CCS is being abandoned as described in 5.13.4.12.

{{This change assumes that by the time of the Authentication step the application client should be expected to populate the Cryptographic Algorithms payload with the right SAI.}}

Change 3 – Clarify Usage Data

5.13.2.2 SA parameters

…

The USAGE_TYPE SA parameter shall be one of the values shown in table 48.

Table 48 — USAGE_TYPE SA parameter values

Value	Description	Usage data description	Reference
0000h - 0080h	Reserved		
0081h	Tape Data Encryption	None [a]	SSC-3
0082h - FFFFh	Reserved		

[a] The usage data length field in the IKEv2-SCSI SAUT Cryptographic Algorithms payload (see 7.6.3.5.13) shall contain zero.

{{The intent is that the Usage data description column contain 'see x.x.x' if the usage data format is defined in SPC-x or 'see UAS-x' if the usage data format is defined in another standard.}}

…

5.13.4.11 IKEv2-SCSI SA generation

…

K) USAGE_DATA shall contain at least the following values from of the usage data field in the IKEv2-SCSI SAUT Cryptographic Algorithms payload in the Key Exchange step SECURITY PROTOCOL OUT command:
   ~~a) The USAGE DATA field;~~
   a) The ALGORITHM IDENTIFIER field (see 7.6.3.6) in the IKEv2-SCSI SAUT Cryptographic Algorithm descriptor (see 7.6.3.6) for the ENCR algorithm type;
   b) The KEY LENGTH field (see 7.6.3.6.2) in the ALGORITHM ATTRIBUTES field in the IKEv2-SCSI SAUT Cryptographic Algorithm descriptor for the ENCR algorithm type; ~~and~~
   c) The ALGORITHM IDENTIFIER field (see 7.6.3.6) in the IKEv2-SCSI SAUT Cryptographic Algorithm descriptor for the INTEG algorithm type; and
   d) The contents, if any, of the USAGE DATA field;

…

7.6.3.5.13 IKEv2-SCSI SAUT Cryptographic Algorithms payload

…

The SA TYPE field specifies the usage type for the SA and is selected from among those listed in table 48 (see 5.13.2.2). If a device server receives an SA TYPE field that contains an SA usage type whose use the device server does not allow, then the error shall be processed as described in 7.6.3.8.3.

The method for changing which of the device server supported SA usage types are allowed is outside the scope of this standard.

The USAGE DATA LENGTH field specifies number of bytes of usage data that follow.

~~NOTE 69 - The contents of the USAGE DATA LENGTH field differ from those found in most SCSI length fields, however, they are consistent with the IKEv2 usage (see RFC 4306).~~

{{The contents appear to be consistent with most SCSI length fields, now.}}

The size and format of the usage data depends on the SA type (see table 48 in 5.13.2.2). If the device server receives a USAGE DATA LENGTH field that contains a value that is inconsistent with the SA type, then the error shall be processed as described in 7.6.3.8.3.

The USAGE DATA field contains information to be stored in the USAGE_DATA SA parameter (see 3.1.113) if the SA is generated (see 5.13.4.11).

Change 4 – Use 4-byte SAIs throughout IKEv2-SCSI and ESP-SCSI

7.6.3.4 IKEv2-SCSI parameter data format

Table 360 shows the parameter list format used by a SECURITY PROTOCOL OUT command and the parameter data format used by a SECURITY PROTOCOL IN command when the SECURITY PROTOCOL field is set to IKEv2-SCSI (i.e., 41h).

Table 360 — IKEv2-SCSI SECURITY PROTOCOL OUT and SECURITY PROTOCOL IN parameter data

Bit / Byte	7	6	5	4	3	2	1	0
IKEv2-SCSI header								
~~0~~	~~(MSB)~~			~~IKE_SA APPLICATION CLIENT SAI~~				
~~7~~								~~(LSB)~~
~~8~~	~~(MSB)~~			~~IKE_SA DEVICE SERVER SAI~~				
~~15~~								~~(LSB)~~
0				Restricted (see RFC 4306)				
3								
4	(MSB)			IKE_SA APPLICATION CLIENT SAI				
7								(LSB)
8				Restricted (see RFC 4306)				
11								
12	(MSB)			IKE_SA DEVICE SERVER SAI				
15								(LSB)
16	NEXT PAYLOAD							
17	MAJOR VERSION (2h)				MINOR VERSION			
18	EXCHANGE TYPE							
19	Reserved			INTTR	VERSION	RSPNS	Reserved	
20	(MSB)			MESSAGE ID				
23								(LSB)
24	(MSB)			IKE LENGTH (n+1)				
27								(LSB)
IKEv2-SCSI payloads								
28				IKEv2-SCSI payload [first] (see 7.6.3.5)				
	. . .							
				IKEv2-SCSI payload [last] (see 7.6.3.5)				
n								

…

7.6.3.5.8 Notify payload

This standard uses the Notify payload (see table 372) only to provide initial contact notification from the application client to the device server.

Table 372 — Notify payload format

Bit / Byte	7	6	5	4	3	2	1	0
0	NEXT PAYLOAD							
1	CRIT (1b)	Reserved						
2	(MSB)	IKE PAYLOAD LENGTH (0010h)						
3								(LSB)
4	PROTOCOL ID (01h)							
5	SAI SIZE (08h)							
6	(MSB)	NOTIFY MESSAGE TYPE (4000h)						
7								(LSB)
~~8~~	~~SAI~~							
~~15~~								
8	Restricted (see RFC 4306)							
11								
12	(MSB)	SAI						
15								(LSB)

{{The other choice is to reduce the value in the SAI SIZE field to four.}}

The NEXT PAYLOAD field, CRIT bit, and IKE PAYLOAD LENGTH field are described in 7.6.3.5.1.

The CRIT bit is set to one in the Notify payload.

The PROTOCOL ID field contains one. If the device server receives a PROTOCOL ID field set to a value other than one, then the IKEv2-SCSI CCS state maintained for the I_T_L nexus shall be abandoned as described in 7.6.3.8.3.

The SAI SIZE field contains eight. If the device server receives a value other than eight in the SAI SIZE field, then the IKEv2-SCSI CCS state maintained for the I_T_L nexus shall be abandoned as described in 7.6.3.8.3.

The NOTIFY MESSAGE TYPE field contains 16 384 (i.e., INITIAL_CONTACT). If the device server receives a value other than 16 384 in the NOTIFY MESSAGE TYPE field, then the IKEv2-SCSI CCS state maintained for the I_T_L nexus shall be abandoned as described in 7.6.3.8.3.

The SAI field contains the device server's SAI. If the contents of the SAI field are not identical to the contents of the IKE_SA DEVICE SERVER SAI field in the IKEv2-SCSI header (see 7.6.3.4), then the IKEv2-SCSI CCS state maintained for the I_T_L nexus shall be abandoned as described in 7.6.3.8.3.

…

7.6.3.5.9 Delete payload

The Delete payload (see table 373) requests the deletion of an existing SA or the abandonment of an IKEv2-SCSI CCS that is in progress.

Table 373 — Delete payload format

Bit / Byte	7	6	5	4	3	2	1	0
0	NEXT PAYLOAD							
1	CRIT (1b)	Reserved						
2	(MSB)	IKE PAYLOAD LENGTH (0018h)						
3								(LSB)
4	PROTOCOL ID (01h)							
5	SAI SIZE (08h)							
6	(MSB)	NUMBER OF SAIS (0002h)						
7								(LSB)
~~8~~	AC_SAI							
~~15~~								
~~16~~	DS_SAI							
~~23~~								
8	Restricted (see RFC 4306)							
11								
12	(MSB)	AC_SAI						
15								(LSB)
16	Restricted (see RFC 4306)							
19								
20	(MSB)	DS_SAI						
23								(LSB)

{{The other choice is to reduce the value in the SAI SIZE field to four.}}

The NEXT PAYLOAD field, CRIT bit, and IKE PAYLOAD LENGTH field are described in 7.6.3.5.1.

The CRIT bit is set to one in the Delete payload.

The PROTOCOL ID field contains one. If the device server receives a PROTOCOL ID field set to a value other than one, then the error shall be processed as described in 7.6.3.8.3.

The SAI SIZE field contains eight. If the device server receives a value other than eight in the SAI SIZE field, then the error shall be processed as described in 7.6.3.8.3.

The AC_SAI field contains the AC_SAI SA parameter value (see 3.1.113) for the SA to be deleted. If the contents of the AC_SAI field do not match the contents of the IKE_SA APPLICATION CLIENT SAI field in the IKEv2-SCSI header (see 7.6.3.4), then the error shall be processed as described in 7.6.3.8.3.

The DS_SAI field contains the DS_SAI SA parameter value (see 3.1.113) for the SA to be deleted. If the contents of the DS_SAI field do not match the contents of the IKE_SA DEVICE SERVER SAI field in the IKEv2-SCSI header (see 7.6.3.4), then the error shall be processed as described in 7.6.3.8.3.

…

7.6.3.5.12 IKEv2-SCSI SA Cryptographic Algorithms payload

The IKEv2-SCSI SA Cryptographic Algorithms payload (see table 377) lists the security algorithms that are being used in the creation and management (e.g., deletion) of an SA using an IKEv2-SCSI CCS.

Table 377 — IKEv2-SCSI SA Cryptographic Algorithms payload format

Bit / Byte	7	6	5	4	3	2	1	0
0	NEXT PAYLOAD							
1	CRIT (1b)	Reserved						
2	(MSB)	IKE PAYLOAD LENGTH (n+1)						
3								(LSB)
4		Reserved						
5								
6	(MSB)	USAGE DATA LENGTH (0000h)						
7								(LSB)
8	(MSB)	SAI						
15								(LSB)
16		Reserved						
18								
19	NUMBER OF ALGORITHM DESCRIPTORS							
IKEv2-SCSI cryptographic algorithm descriptors								
20		IKEv2-SCSI cryptographic algorithm descriptor [first] (see 7.6.3.6)						
		. . .						
n		IKEv2-SCSI cryptographic algorithm descriptor [last] (see 7.6.3.6)						

The NEXT PAYLOAD field, CRIT bit, and IKE PAYLOAD LENGTH field are described in 7.6.3.5.1.

The CRIT bit is set to one in the IKEv2-SCSI SA Cryptographic Algorithms payload.

The USAGE DATA LENGTH field is set to zero in the IKEv2-SCSI SA Cryptographic Algorithms payload.

The SAI field is reserved.

{{No changes are suggested because the SAI field is reserved.}}

…

7.6.3.5.13 IKEv2-SCSI SAUT Cryptographic Algorithms payload

The IKEv2-SCSI SAUT Cryptographic Algorithms payload (see table 378) lists the usage type of and security algorithms to be used by the SA that is created as a result of an IKEv2-SCSI CCS.

Table 378 — IKEv2-SCSI SAUT Cryptographic Algorithms payload format

Bit / Byte	7	6	5	4	3	2	1	0
0	NEXT PAYLOAD							
1	CRIT (1b)	Reserved						
2	(MSB)	IKE PAYLOAD LENGTH (n+1)						
3								(LSB)
4	(MSB)	SAI						
11								(LSB)
12	(MSB)	SA TYPE						
13								(LSB)
14	(MSB)	USAGE DATA LENGTH (j)						
15								(LSB)
16		USAGE DATA						
16+j-1								
16+j		Reserved						
16+j+2								
16+j+3	NUMBER OF ALGORITHM DESCRIPTORS							
IKEv2-SCSI cryptographic algorithm descriptors								
16+j+4		IKEv2-SCSI cryptographic algorithm descriptor [first] (see 7.6.3.6)						
		. . .						
n		IKEv2-SCSI cryptographic algorithm descriptor [last] (see 7.6.3.6)						

The NEXT PAYLOAD field, CRIT bit, and IKE PAYLOAD LENGTH field are described in 7.6.3.5.1.

The CRIT bit is set to one in the IKEv2-SCSI SAUT Cryptographic Algorithms payload.

The SAI field is reserved.

{{No changes are suggested because the SAI field is reserved.}}

…

Change 5 – Multiple Certificates Are Good

7.6.3.5.5 Certificate payload and Certificate Request payload

…

The relationship between the Certificate payload and the Identification payload is described in 7.6.3.5.4.

Device servers that support certificates should support a mechanism outside the scope of this standard for replacing certificates and have the ability to store more than one certificate to facilitate such replacements.

Change 6 – How to hash Authentication payload RSAs

7.6.3.6.6 IKEv2-SCSI authentication algorithm IKEv2-SCSI cryptographic algorithm descriptors

…

The ALGORITHM IDENTIFIER field (see table 391) specifies Authentication payload authentication algorithm to which the SA_AUTH_OUT IKEv2-SCSI cryptographic algorithm descriptor or SA_AUTH_IN IKEv2-SCSI cryptographic algorithm descriptor applies.

Table 391 — SA_AUTH_OUT and SA_AUTH_IN ALGORITHM IDENTIFIER field

Code	Description	Support	Reference
00F9 0000h	SA_AUTH_NONE	Optional	this subclause
00F9 0001h	RSA Digital Signature with SHA-1 [a]	Optional	RFC 4306
00F9 0002h	Shared Key Message Integrity Code	Optional	RFC 4306 [b, c]
00F9 0009h	ECDSA with SHA-256 on the P-256 curve [a]	Optional	RFC 4754
00F9 000Bh	ECDSA with SHA-512 on the P-521 curve [a]	Optional	RFC 4754
00F9 00C9h – 00F9 00FFh	Vendor Specific	Optional	
0000 0000h – 0000 FFFFh	Restricted	Prohibited	IANA
All others	Reserved		

[a] Use of certificates with this digital signature authentication algorithm is optional.

[b] The 17 ASCII character non-terminated pre-shared key (see 3.1.94) pad string "Key Pad for IKEv2" specified by RFC 4306 is replaced by the 22 ASCII character non-terminated pre-shared key pad string "Key Pad for IKEv2-SCSI".

[c] The pre-shared key (see 3.1.94) requirements used by this standard (see 5.13.4.5) apply in addition to those found in RFC 4306.

Change 7 – Provide the sizes of Initialization Vectors

7.6.3.5.10 Encrypted payload

7.6.3.5.10.1 Introduction

…

The INITIALIZATION VECTOR field contains the initialization vector encryption algorithm input value. The size of the initialization vector is defined by the encryption algorithm.

{{Changes are clearly needed here but the details are TBD.}}

7.6.3.6.2 Encryption algorithm (ENCR) IKEv2-SCSI cryptographic algorithm descriptors

…

The ALGORITHM IDENTIFIER field (see table 383) specifies the encryption algorithm to which the ENCR IKEv2-SCSI cryptographic algorithm descriptor applies.

Table 383 — ENCR ALGORITHM IDENTIFIER field (Sheet 1 of 2)

Code	Description	Salt [a] length (bytes)	IV [b] length (bytes)	Key length (bytes)	Support	Reference
8001 000Bh	ENCR_NULL [c]	n/a		0	Mandatory	
8001 000Ch	AES-CBC [c]	n/a	16	16	Optional	RFC 3602
				24	Prohibited	
				32	Optional	
8001 0010h	AES-CCM with a 16 byte MAC [d]	3	8	16	Optional	RFC 4309
				24	Prohibited	
				32	Optional	
8001 0014h	AES-GCM with a 16 byte MAC [d]	4	8	16	Optional	RFC 4106
				24	Prohibited	
				32	Optional	
8001 0400h – 8001 FFFFh	Vendor Specific					

[a] See RFC 4106 and RFC 4309.

[b] Initialization Vector.

[c] If the INTEG cryptographic algorithm descriptor (see 7.6.3.6.4) in the same IKEv2-SCSI SA Cryptographic Algorithms payload or the same IKEv2-SCSI SAUT Cryptographic Algorithms payload as this ENCR cryptographic algorithm descriptor has the ALGORITHM IDENTIFIER field set to AUTH_COMBINED, then the error shall be processed as described in 7.6.3.8.3.

[d] If the INTEG cryptographic algorithm descriptor (see 7.6.3.6.4) in the same IKEv2-SCSI SA Cryptographic Algorithms payload or the same IKEv2-SCSI SAUT Cryptographic Algorithms payload as this ENCR cryptographic algorithm descriptor does not have the ALGORITHM IDENTIFIER field set to AUTH_COMBINED, then the error shall be processed as described in 7.6.3.8.3.

Table 383 — ENCR ALGORITHM IDENTIFIER field (Sheet 2 of 2)

Code	Description	Salt [a] length (bytes)	IV [b] length (bytes)	Key length (bytes)	Support	Reference
0000 0000h – 0000 FFFFh	Restricted					IANA
All others	Reserved					

[a] See RFC 4106 and RFC 4309.

[b] Initialization Vector.

[c] If the INTEG cryptographic algorithm descriptor (see 7.6.3.6.4) in the same IKEv2-SCSI SA Cryptographic Algorithms payload or the same IKEv2-SCSI SAUT Cryptographic Algorithms payload as this ENCR cryptographic algorithm descriptor has the ALGORITHM IDENTIFIER field set to AUTH_COMBINED, then the error shall be processed as described in 7.6.3.8.3.

[d] If the INTEG cryptographic algorithm descriptor (see 7.6.3.6.4) in the same IKEv2-SCSI SA Cryptographic Algorithms payload or the same IKEv2-SCSI SAUT Cryptographic Algorithms payload as this ENCR cryptographic algorithm descriptor does not have the ALGORITHM IDENTIFIER field set to AUTH_COMBINED, then the error shall be processed as described in 7.6.3.8.3.

Change 8 – 'this subclause'?

7.6.3.7 Errors in IKEv2-SCSI security protocol commands

For a single I_T_L nexus, the device server shall ensure that the two or four IKEv2-SCSI CCS commands are processed in the order described in 5.13.4.1 based only on the contents of the CDB (i.e., the SECURITY PROTOCOL OUT parameter data shall not be processed unless the tests in table 392 specify the processing of the command) using the tests and responses shown in table 392

Table 392 — IKEv2-SCSI command ordering processing requirements on a single I_T_L nexus

{{Big, hairy table whose contents are not relevant to the issue and that does not need to be changed.}}

The processing shown in table 392 shall be performed before the parameter data ~~any other~~ error handling described in 7.6.3.8 ~~this subclause~~.

7.6.3.8 Errors in IKEv2-SCSI security protocol parameter data

7.6.3.8.1 Overview

Errors in the parameter data transferred to the device sever by an IKEv2-SCSI SECURITY PROTOCOL OUT command are classified (see table 393) based on the ease with which they may be used to mount denial of service attacks against IKEv2-SCSI SA creation operations by an attacker that has not participated as the application client or device server in the Key Exchange step SECURITY PROTOCOL OUT command (see 5.13.4.8.2) that started the IKEv2-SCSI CCS.