ENDL
TEXAS

Date: 8 March 2008
To: T10 Technical Committee
From: Ralph O. Weber
Subject: Constraints on SPC-4 SA creation based on Usage Type

Introduction

One of the issues raised by CbCS is the requirement that SAs created for its Usage Type should be usable only if the Authentication Step is performed during in the SA creation process (i.e., SA_AUTH_NONE is not selected).

As currently written, this constraint is applied only when an application client attempts to use an SA in a RECEIVE CREDENTIAL command, an event that occurs a very long time (in computer terms) after the SA is created. It seems like a substantial waste of effort to create an SA and then not allow its use, especially when the Usage Type specified for the SA to be created could clearly indicate that SA_AUTH_NONE is not an option.

It is not clear whether other future SA Usage Types will place other constraints on how an SA is created, but precluding such options seems ill advised.

This proposal suggests changes in the IKEv2-SCSI protocol that are intended to provide a framework in which Usage-Type based constraints can be defined for specific SA Usage Types, as well as to address the specific needs of CbCS.

Revision History

r0 Initial revision

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

Proposed Changes in SPC-4 r13

5.13.2.2 SA parameters

…

The USAGE_TYPE SA parameter shall be one of the values shown in table 49.

Table 49 — USAGE_TYPE SA parameter values

Value [a]	Description	Usage model	Usage data description	Reference
0000h - 0080h	Reserved			
0081h	Tape data encryption	ESP-SCSI [b]	None [c]	SSC-3
0082h - 8000h	Reserved			
~~0082h~~ 8001h	CbCS authentication and credential encryption	ESP-SCSI [b]	None [c]	5.13.6.8
~~0083h~~ 8002h - FFFFh	Reserved			

[a] USAGE_TYPE values between 8000h and CFFFh inclusive place additional constraints on how an SA is to be created as described in 7.6.3.5.13.

[b] ESP-SCSI usage is defined in 7.6.4.

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

…

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 49 (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~~ An error shall be processed as described in 7.6.3.8.3~~.~~ if any of the following conditions occur:

a) The device server receives an SA usage type whose use the device server does not allow;
b) An SA usage type between 8000h and BFFFh inclusive is received in a Key Exchange step SECURITY PROTOCOL OUT command (see 5.13.4.8.2); or
c) An SA usage type between A000h and CFFFh inclusive is received for which the device server is unable to verify the applicable usage type constraints.

{{The intent is to define three ranges of constrained usage types, with room to grow above and below based on other usage type issues:

- **8000h - AFFFh:** Authentication step required but no other constraints (hopefully, the most common case)
- **B000h - BFFFh:** Authentication step required and other constraints too
- **C000h - CFFFh:** Authentication step may be skipped but other constraints apply

When a usage type in the B000h to CFFFh range is defined a new item would be added to the list referencing a table in which the specific additional constraints are described.
}}