TCG Storage

Enterprise SSC Feature Set: PSK Secure Messaging

Specification Version 1.00

Revision 1.00

August 5, 2015

Contact: admin@trustedcomputinggroup.org

TCG

PUBLISHED

Disclaimers, Notices, and License Terms

TABLE OF CONTENTS

Tables

1 Introduction

1.1 Document Purpose

The Storage Workgroup specifications provide a comprehensive architecture for Storage Devices under policy control as determined by the trusted platform host, the capabilities of the Storage Device to conform to the policies of the trusted platform, and the lifecycle state of the Storage Device as a Trusted Peripheral.

1.2 Scope and Intended Audience

This specification defines PSK Secure Messaging for the Enterprise Security Subsystem Class (SSC). Any Storage Device that claims Enterprise SSC PSK Secure Messaging compatibility SHALL conform to this specification.

The intended audience for this specification is both trusted Storage Device manufacturers and developers that want to use these Storage Devices in their systems.

1.3 Key Words

Key words are used to signify SSC requirements.

The Key Words "**SHALL**", "**SHALL NOT**", "**SHOULD**," and "**MAY**" are used in this document. These words are a subset of the RFC 2119 key words used by TCG, and have been chosen since they map to key words used in T10/T13 specifications. These key words are to be interpreted as described in [1].

In addition to the above key words, the following are also used in this document to describe the requirements of particular features, including tables, methods, and usages thereof.

- **Mandatory (M):** When a feature is Mandatory, the feature SHALL be implemented. A Compliance test SHALL validate that the feature is operational.
- **Optional (O):** When a feature is Optional, the feature MAY be implemented. If implemented, a Compliance test SHALL validate that the feature is operational.
- **Excluded (X):** When a feature is Excluded, the feature SHALL NOT be implemented. A Compliance test SHALL validate that the feature is not operational.
- **Not Required (N)** When a feature is Not Required, the feature MAY be implemented. No Compliance test is required.

1.4 Document References

[1]. IETF RFC 2119, 1997, "Key words for use in RFCs to Indicate Requirement Levels"

[2]. Trusted Computing Group (TCG), "TCG Storage Architecture Core Specification", Version 1.00

[3]. Trusted Computing Group (TCG), "TCG Storage Security Subsystem Class: Enterprise", Version 1.01

[4]. Trusted Computing Group (TCG), "TCG Storage Interface Interactions Specification", Version 1.04

[5]. Trusted Computing Group (TCG), "TCG Storage Core Spec Addendum: Secure Messaging", Version 1.00

1.5 Document Precedence

In the event of conflicting information in this specification and other documents, the precedence for requirements is:

1. This specification;
2. TCG Storage Core Spec Addendum: Secure Messaging [5];

3. TCG Storage Security Subsystem Class: Enterprise [3];
4. TCG Storage Interface Interactions Specification [4];
5. TCG Storage Architecture Core Specification [2].

1.6 Dependencies on Other Feature Sets

This feature set has no dependencies on other feature sets.

1.7 Interactions with Other Feature Sets

This feature set does not define any interactions with other feature sets.

2 PSK Secure Messaging Overview

Begin Informative Content

The Pre-Shared Key (PSK) Secure Messaging feature set for Enterprise SSC compliant storage devices provides the ability by the host to setup a secure communication channel between host and TPer. It uses TLS v1.2 as the underlying protocol to establish session keys and protect TCG protocol payloads, see [5] for more information.

This version of the feature set relies solely on use of pre-shared keys (PSKs) for the establishment of session keys. The PSKs must be written to the appropriate table within the SP for which the host wants to use secure messaging. The initial transfer of those keys might be in the clear in case the shipping device does not contain a set of pre-loaded PSKs.

The TCG Storage Core Spec Addendum: Secure Messaging [5] mandates device support for one TLS ciphersuite but devices may support additional ones. Note that, unless the device supports table row insertion (not mandated by Enterprise SSC), the number of keys and supported cipher suites is determined by the number of pre-allocated rows in the `C_TLS_PSK` table.

End Informative Content

3 SSC Specific Functionality

This section specifies the additional SSC-specific functionality in support of the PSK Secure Messaging feature set.

3.1 Secure Messaging Functionality

The methods and protocol mapping defined in [5] and this specification supersede the secure session start up methods (`StartTrustedSession`, `SyncTrustedSession`) and “Secure Messaging Packet Format” as specified in [2] and [3].

3.2 Methods

This section defines new methods and modifications to existing methods required for this feature set.

3.2.1 New Methods

This feature set requires the `StartTLS` and `SyncTLS` methods as defined in [5], with the additional requirement to follow method parameter definitions and encoding as defined in [3]. `StartTLS` and `SyncTLS` methods SHALL use the Session number (comprised of the TSN and HSN) as described in [3]. Modified Methods

There are no modified methods defined by this feature set.

3.3 Tables

This section defines new tables and modifications to existing tables required for this feature set.

3.3.1 New Tables

This feature set requires the `C_TLS_PSK` table as defined in [5].

3.3.2 Modified Tables

There are no tables modified by this feature set.

3.4 Types

This section defines new types and modifications to existing types required for this feature set.

3.4.1 New Types

This feature set requires the `bytes_2` and `psk` types as defined in [5]. The minimum supported size for `psk` type SHALL be 16 bytes.

3.4.2 Modified Types

There are no types modified by this feature set.

3.5 TLS Interactions

3.5.1 Sessions

If the SD receives a TLS close_notify alert prior to receiving EOS in the TCG session, the SD SHALL abort the TCG Session, and SHALL perform all side effects of aborting a session as described in [2] and [3].

When the SD receives a TLS Fatal Alert from the host, the SD SHALL immediately abort the session (see [2] and [3]).

3.5.2 Padding

This feature set requires padding of TLS records as defined in [5] with the added clarification:

- Data Subpackets within the TLS application record(s) SHALL be padded as defined in [3].

4 Feature Set Requirements

This section defines the Mandatory (M) and Optional (O) requirements for the PSK Secure Messaging feature set.

4.1 Level 0 Discovery

A SD implementing the PSK Secure Messaging feature set SHALL, in addition to the Level 0 Discovery response requirements defined in [3], return the Secure Messaging Feature Descriptor as defined in [5] and with the following modifications:

- Version = 0x01 (M);
- Activated = 1 (M);
- TLS Features (M):
  - Bit 4 = 0;
  - Bit 3 = 0;
  - Bit 2 = 0;
- Number of SPs = 0x02 (M);
- SP1 = 0x0000 0x0205 0x0000 0x0001 (M);
- SP2 = 0x0000 0x0205 0x0000 0x0002 (M);
- Number of Supported Cipher Suites is at least 0x01 (M);
- Cipher Suite 1 = 0x0000 0x00AA (M);
- Cipher Suite 2 .. n are optional (O).

4.2 Session Manager

4.2.1 Methods

A SD that implements the PSK Secure Messaging feature set SHALL support the method additions as outlined in this subsection.

4.2.1.1 StartTLS (M)

The `StartTLS` method (see section 3.2.1) SHALL implement the following parameters:

- HostSessionID;
- SPID;
- Write (support of Write = True mandatory).

4.2.1.2 SyncTLS (M)

The `SyncTLS` method (see section 3.2.1) SHALL implement the following parameters:

- HostSessionID;
- SPSessionID.

4.3 Admin SP

A SD that implements the PSK Secure Messaging feature set SHALL support the additions to the Admin SP specified in this section, in addition to the Admin SP requirements defined in [3].

4.3.1 Tables

4.3.1.1 C_TLS_PSK table (M)

The C_TLS_PSK (see section 3.3.1) SHALL be supported and contains 4 rows.

Table 1. Admin SP – C_TLS_PSK Table

UID	Name	CommonName	Enabled	PSK	CipherSuite
00 00 00 1E 00 00 00 01	"TLS_PSK_ Key0"	""	F	VU	VU
•	•	•	•	•	•
00 00 00 1E 00 00 00 04	"TLS_PSK_ Key3"	""	F	VU	VU

4.3.1.2 ACE table (M)

Three additional ACEs are added to the ACE table.

Table 2. Admin SP – ACE Table Addition

UID	Name	CommonName	BooleanExpr	RowStart	RowEnd	ColStart	ColEnd

UID	Name	CommonName	BooleanExpr	RowStart	RowEnd	ColStart	ColEnd
00 00 00 08 00 03 FD 01	"ACE_TLS_PSK_Get_UID_Enabled"	""	00 00 00 08 00 00 00 01 (Anybody)	Null	Null	UID	Enabled
00 00 00 08 00 03 FD 02	"ACE_TLS_PSK_Get_CipherSuite"	""	00 00 00 08 00 00 00 01 (Anybody)	Null	Null	CipherSuite	CipherSuite
00 00 00 08 00 03 FD 03	"ACE_TLS_PSK_Set"	""	00 00 00 09 00 00 00 06 (SID)	Null	Null	Enabled	CipherSuite

4.3.1.3 AccessControl table (M)

Additional rows are required in the AccessControl table.

Table 3. Admin SP - AccessControl Table

RowNumber	UID	InvokingID	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL
VU	VU	00 00 00 1E 00 00 00 00 (PSK_table)	00 00 00 06 00 00 00 08 (Next)		00 00 00 08 00 00 00 01 (Anybody)	None	Null	Null	00 00 00 08 00 00 00 01 (Anybody)
VU	VU	00 00 00 1E 00 00 00 01 (TLS_PSK_ Key0)	00 00 00 06 00 00 00 06 (Get)		00 00 00 08 00 03 FD 01 (ACE_TLS_PSK_Get_UID_Enabled) or 00 00 00 08 00 03 FD 02 (ACE_TLS_PSK_Get_CipherSuite)	None	Null	Null	00 00 00 08 00 00 00 01 (Anybody)
VU	VU	00 00 00 1E 00 00 00 01 (TLS_PSK_ Key0)	00 00 00 06 00 00 00 07 (Set)		00 00 00 08 00 03 FD 03 (ACE_TLS_PSK_Set)	None	Null	Null	00 00 00 08 00 00 00 01 (Anybody)
•	•	•	•	•	•	•	•	•	•
VU	VU	00 00 00 1E 00 00 00 04 (TLS_PSK_ Key3)	00 00 00 06 00 00 00 06 (Get)		00 00 00 08 00 03 FD 01 (ACE_TLS_PSK_Get_UID_Enabled) or 00 00 00 08 00 03 FD 02 (ACE_TLS_PSK_Get_CipherSuite)	None	Null	Null	00 00 00 08 00 00 00 01 (Anybody)

RowNumber	UID	InvokingID	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL
VU	VU	00 00 00 1E 00 00 00 04 (TLS_PSK_Key3)	00 00 00 06 00 00 00 07 (Set)		00 00 00 08 00 03 FD 03 (ACE_TLS_PSK_Set)	None	Null	Null	00 00 00 08 00 00 00 01 (Anybody)

4.4 Locking SP

A SD that implements the PSK Secure Messaging feature set SHALL support the additions to the Locking SP specified in this section, in addition to the Locking SP requirements defined in [3].

4.4.1 Tables

4.4.1.1 C_TLS_PSK table (M)

The C_TLS_PSK (see section 3.3.1) SHALL be supported and contains one row for each supported BandMaster Authority plus an additional row for the EraseMaster Authority.

Table 4. Locking SP – C_TLS_PSK Table

UID	Name	CommonName	Enabled	PSK	CipherSuite
00 00 00 1E 00 00 00 01	"TLS_PSK_Key0"	""	F	VU	VU
•	•	•	•	•	•
00 00 00 1E 00 00 04 01	"TLS_PSK_Key1024"	""	F	VU	VU

Begin Informative Content

Linking the number of rows in the C_TLS_PSK table to the number of BandMaster and EraseMaster Authorities provides the host with a way to determine the number of rows in the table. It also allows for a flexible mapping of PSKs. E.g., the host can decide to assign a dedicated PSK value to each Authority in the Locking SP or share PSK values between authorities while assigning different PSK values to different cipher suites.

Example: device with four Bandmasters will have five rows in the C_TLS_PSK table.

In this scenario the host can setup a unique PSK value for BandMaster0 – BandMaster3, plus one for EraseMaster by mapping each TLS psk_identity to one individual Authority. This scenario provides for a dedicated secure TLS session for each individual Authority; downside is that only one cipher suite can be used with each Authority.

Alternatively, the host can set one or more unique PSK values in each of the five rows and assign a different cipher suite to each PSK value. In this case the host links each TLS psk_identity to a specific cipher suite. This scenario provides for a larger selection of enabled cipher suites.

End Informative Content

4.4.1.2 ACE Table (M)

Additional ACEs are required in the ACE table.

Table 5. Locking SP – ACE Table Addition

UID	Name	CommonName	BooleanExpr	RowStart	RowEnd	ColStart	ColEnd
00 00 00 08 00 03 FD 01	"ACE_TLS_PSK_Get_UID_ Enabled"	""	00 00 00 08 00 00 00 01 (Anybody)	Null	Null	UID	Enabled
00 00 00 08 00 03 FD 02	"ACE_TLS_PSK_Get_ CipherSuite"	""	00 00 00 08 00 00 00 01 (Anybody)	Null	Null	CipherSuite	CipherSuite

UID	Name	CommonName	BooleanExpr	RowStart	RowEnd	ColStart	ColEnd
00 00 00 08 00 03 FD 03	"ACE_TLS_PSK_Set_ EraseMaster"	""	00 00 00 09 00 00 84 01 (EraseMaster)	Null	Null	Enabled	CipherSuite
00 00 00 08 00 03 FD 04	"ACE_TLS_PSK_Set_ BandMaster0"	""	00 00 00 09 00 00 80 01 (BandMaster0)	Null	Null	Enabled	CipherSuite
•	•	•	•	•	•		
00 00 00 08 00 04 01 03	"ACE_TLS_PSK_Set_ BandMaster1023"	""	00 00 00 09 00 00 84 00 (BandMaster1023)	Null	Null	Enabled	CipherSuite

4.4.1.3 AccessControl table (M)

Additional rows are required in the AccessControl table.

Table 6. Locking SP - AccessControl Table

RowNumber	UID	InvokingID	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL
VU	VU	00 00 00 1E 00 00 00 00 (PSK_table)	00 00 00 06 00 00 00 08 (Next)		00 00 00 08 00 00 00 01 (Anybody)	None	Null	Null	00 00 00 08 00 00 00 01 (Anybody)

RowNumber	UID	InvokingID	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL
VU	VU	00 00 00 1E 00 00 00 01 (TLS_PSK_Key0)	00 00 00 06 00 00 00 06 (Get)		00 00 00 08 00 03 FD 01 (ACE_TLS_PSK_Get_UID_Enabled) or 00 00 00 08 00 03 FD 02 (ACE_TLS_PSK_Get_CipherSuite)	None	Null	Null	00 00 00 08 00 00 00 01 (Anybody)
VU	VU	00 00 00 1E 00 00 00 01 (TLS_PSK_Key0)	00 00 00 06 00 00 00 07 (Set)		00 00 00 08 00 03 FD 03 (ACE_TLS_PSK_Set_ EraseMaster)	None	Null	Null	00 00 00 08 00 00 00 01 (Anybody)
VU	VU	00 00 00 1E 00 00 00 02 (TLS_PSK_Key1)	00 00 00 06 00 00 00 06 (Get)		00 00 00 08 00 03 FD 01 (ACE_TLS_PSK_Get_UID_Enabled) or 00 00 00 08 00 03 FD 02 (ACE_TLS_PSK_Get_CipherSuite)	None	Null	Null	00 00 00 08 00 00 00 01 (Anybody)
•	VU	00 00 00 1E 00 00 00 02 (TLS_PSK_Key1)	00 00 00 06 00 00 00 07 (Set)		00 00 00 08 00 03 FD 03 (ACE_TLS_PSK_Set_ BandMaster0)	None	Null	Null	00 00 00 08 00 00 00 01 (Anybody)
•	•	•	•	•	•	•	•	•	•

RowNumber	UID	InvokingID	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL
VU	VU	00 00 00 1E 00 00 40 01 (TLS_PSK_Key1024)	00 00 00 06 00 00 00 06 (Get)		00 00 00 08 00 03 FD 01 (ACE_TLS_PSK_Get_UID_Enabled) or 00 00 00 08 00 03 FD 02 (ACE_TLS_PSK_Get_CipherSuite)	None	Null	Null	00 00 00 08 00 00 00 01 (Anybody)
VU	VU	00 00 00 1E 00 00 40 01 (TLS_PSK_Key1024)	00 00 00 06 00 00 00 07 (Set)		00 00 00 08 00 03 FD 04 (ACE_TLS_PSK_Set_ BandMaster1023)	None	Null	Null	00 00 00 08 00 00 00 01 (Anybody)

4.4.2 Methods

4.4.2.1 Erase Method

Begin Informative Content

As defined in [3] the reset of a LBA Range by invoking the Erase method on the Locking object representing that Range also resets the associated BandMaster credential. The result is that the BandMaster credential value is set to a known value (MSID) and as such could be used to overwrite the associated row in the C_TLS_PSK table. It is recommended that after the host has taken ownership of the reset BandMaster credential value the associated row data in the C_TLS_PSK table are validated and/or updated.

End Informative Content

4.5 Additional SPs

This feature set requires no additional SPs.