TCG Storage

Opal 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 Opal Security Subsystem Class (SSC). Any Storage Device that claims Opal 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 2.01

[3]. Trusted Computing Group (TCG), "TCG Storage Security Subsystem Class: Opal", Versions 1.00, 2.00, 2.01, or compatible

[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: Opal [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.

1.8 Legend

The following legend defines SP table cell coloring coding. This color coding is informative only. The table cell content is normative.

Table 1. SP Table Legend

Table Cell Legend	R-W	Value	Access Control	Comment
Arial-Narrow	Read-only	Opal SSC specified	Fixed	• Cell content is Read-Only. • Access control is fixed. • Value is specified by the Opal SSC
Arial Narrow bold-under	Read-only	VU	Fixed	• Cell content is Read-Only. • Access Control is fixed. • Values are Vendor Unique (VU). A minimum or maximum value may be specified.
Arial-Narrow	Not Defined	(N)	Not Defined	• Cell content content is (N). • Access control is not defined. • Any text in table cell is informative only. • A `Get` MAY omit this column from the method response.
Arial Narrow bold-under	Write	Preconfigured, user personalizable	Preconfigured, user personalizable	• Cell content is writable. • Access control is personalizable • `Get` Access Control is not described by this color coding

Table Cell Legend	R-W	Value	Access Control	Comment
Arial-Narrow	Write	Preconfigured, user personalizable	Fixed	• Cell content is writable. • Access control is fixed. • `Get` Access Control is not described by this color coding

2 PSK Secure Messaging Overview

Begin Informative Content

The Pre-Shared Key (PSK) Secure Messaging feature set for Opal 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 Opal 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 Methods

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

3.1.1 New Methods

This feature set requires the `StartTLS` and `SyncTLS` methods as defined in [5].

3.1.2 Modified Methods

There are no modified methods defined by this feature set.

3.2 Tables

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

3.2.1 New Tables

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

3.2.2 Modified Tables

There are no tables modified by this feature set.

3.3 Types

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

3.3.1 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.

3.3.2 Modified Types

There are no types modified by this feature set.

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], 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 implementing 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 3.1.1) SHALL implement the following parameters:

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

4.2.1.2 SyncTLS (M)

The `SyncTLS` method (see section 3.1.1) SHALL implement the following parameters:

- HostSessionID;
- SPSessionID.

4.3 Admin SP

A SD implementing 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 3.2.1) SHALL be supported and contain at least one row. The SD MAY support additional rows.

Table 2. Admin SP – C_TLS_PSK Table Preconfiguration

UID	Name	CommonName	Enabled	PSK	CipherSuite
00 00 00 1E 00 00 00 01	"TLS_PSK_ Key1"		F	VU	00 AA
00 00 00 1E 00 00 (00 01 + N)	"TLS_PSK_ Key(N+1)"		F	VU	VU

Where N = 1,2,3, …represents each optional row in the table.

Begin Informative Content

This specification requires at least one row be present in the C_TLS_PSK table and allows for vendors to add one or more additional rows. The UIDs for those rows will increment monotonically for each additional row, e.g. the UID for object with name "TLS_PSK_Key2" should be "00 00 00 1E 00 00 00 02".

End Informative Content

4.3.1.2 Table table (M)

One new row is added to the Table table for the required C_TLS_PSK table.

Table 3. Admin SP – Additions to Table Table Preconfiguration

UID	Name	CommonName	TemplateID	Kind	Column	NumColumns	Rows	RowsFree	RowBytes	LastID	MinSize	MaxSize
00 00 00 01 00 00 00 1E	"C_TLS_PSK"			Object			*TT1					

*TT1: min. number of supported rows is one.

4.3.1.3 ACE table (M)

Two additional ACEs are added to the ACE table.

Table 4. Admin SP – ACE Table Preconfiguration

Table Association - Informative only	UID	Name	CommonName	BooleanExpr	Columns
C_TLS_PSK					
	00 00 00 08 00 03 FD 01	"ACE_TLS_PSK_Get_No_PSK"		Anybody	UID,Name,CommonName, Enabled,CipherSuite
	00 00 00 08 00 03 FD 02	"ACE_TLS_PSK_Set"		SID	Enabled, PSK, CipherSuite

4.3.1.4 AccessControl table (M)

At least three additional rows are required in the AccessControl table. Each additional row entry in the C_TLS_PSK table shall result in two additional entries in the AccessControl table, where N = 1,2,3,... is the number of additional rows in C_TLS_PSK table.

Table 5. Admin SP - AccessControl Table Preconfiguration

Table Association - informative only	UID	InvokingID	InvokingID Name - informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
C_TLS_PSK																
		00 00 00 1E 00 00 00 00	"C_TLS_PSK"	Next		ACE_Anybody				ACE_Anybody						
		00 00 00 1E 00 00 00 01	"TLS_PSK_Key1"	Get		ACE_TLS_PSK_Get_No_PSK				ACE_Anybody						

Table Association - informative only	UID	InvokingID	InvokingID Name - informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
		00 00 00 1E 00 00 (00 01 + N)	C_TLS_PSK Obj N+1	Get		ACE_TLS_PSK_Get_No_PSK				ACE_Anybody						
		00 00 00 1E 00 00 00 01	"TLS_PSK_ Key1"	Set		ACE_TLS_PSK_Set				ACE_Anybody						
		00 00 00 1E 00 00 (00 01 + N)	C_TLS_PSK Obj N+1	Set		ACE_TLS_PSK_Set				ACE_Anybody						

4.4 Locking SP

A SD implementing 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 3.2.1) SHALL be supported and contains at least one row. The SD MAY support additional rows.

Table 6. Locking SP – C_TLS_PSK Table Preconfiguration

UID	Name	CommonName	Enabled	PSK	CipherSuite
00 00 00 1E 00 00 00 01	"TLS_PSK_ Key1"		F	VU	00 AA
00 00 00 1E 00 00 (00 01 + N)	"TLS_PSK_ Key(N+1)"		F	VU	VU

Where N = 1,2,3, …represents each optional row in the table.

4.4.1.2 Table table (M)

One new row is added to the Table table for the required C_TLS_PSK table.

Table 7. Locking SP – Additions to Table Table Preconfiguration

UID	Name	CommonName	TemplateID	Kind	Column	NumColumns	Rows	RowsFree	RowBytes	LastID	MinSize	MaxSize
00 00 00 01 00 00 00 1E	"C_TLS_PSK"			Object			*TT1					

*TT1: min. number of supported rows is one.

4.4.1.3 ACE table (M)

Two additional ACEs are added to the ACE table.

Table 8. Locking SP – ACE Table Preconfiguration

Table Association – Informative only	UID	Name	CommonName	BooleanExpr	Columns
C_TLS_PSK					
	00 00 00 08 00 03 FD 01	"ACE_TLS_PSK_Get_No_PSK"		Anybody	UID,Name,CommonName, Enabled,CipherSuite
	00 00 00 08 00 03 FD 03	"ACE_TLS_PSK_Set"		Admins	Enabled, PSK, CipherSuite

4.4.1.4 AccessControl table (M)

At least three additional rows are required in the AccessControl table. Each additional row entry in the C_TLS_PSK table shall result in two additional entries in the AccessControl table, where n = 1,2,... is the number of additional rows in C_TLS_PSK table.

Table 9. Locking SP - AccessControl Table Preconfiguration

Table Association - informative only	UID	InvokingID	InvokingID Name - informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
C_TLS_PSK																
		00 00 00 1E 00 00 00 00	"C_TLS_PSK"	Next		ACE_Anybody				ACE_Anybody						
		00 00 00 1E 00 00 00 01	"TLS_PSK_ Key1"	Get		ACE_TLS_PSK_Get_No_PSK				ACE_Anybody						
		00 00 00 1E 00 00 (00 01 + N)	C_TLS_PSK Obj N+1	Get		ACE_TLS_PSK_Get_No_PSK				ACE_Anybody						
		00 00 00 1E 00 00 00 01	"TLS_PSK_ Key1"	Set		ACE_TLS_PSK_Set				ACE_Anybody						

Table Association - informative only	UID	InvokingID	InvokingID Name - informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
		00 00 00 1E 00 00 (00 01 + N)	C_TLS_PSK Obj N+1	Set		ACE_TLS_PSK_Set				ACE_Anybody						

4.5 Additional SPs

This feature set requires no additional SPs.