TCG Storage
Opal SSC Feature Set: PSID

Specification Version 1.00
Revision 1.00

August 5, 2015

Contact: admin@trustedcomputinggroup.org

TCG

PUBLISHED

TABLE OF CONTENTS

Tables

1 Introduction

1.1 Document Purpose

The Storage Workgroup specifications provide a comprehensive architecture for putting Storage Devices under policy control as determined by the trusted platform host, the capabilities of the Storage Device to conform with 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 the PSID Feature Set for the Opal Security Subsystem Class (SSC). Any Storage Device that claims Opal SSC PSID Feature Set 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", see [3] for the applicable specification version

[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 Storage Interface Interactions Specification", see [3] for the applicable specification version

1.5 Document Precedence

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

1. This specification and TCG Storage Security Subsystem Class: Opal [3] (these two documents are at the same level of precedence, and SHALL NOT conflict with each other)

2. Storage Interface Interactions Specification [4]
3. 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 has no interactions with other feature sets.

1.8 Terminology

This section provides special definitions that are not defined in the Core Specification.

Table 1 PSID Feature Set Terminology

Term	Definition
PSID	Physical Presence SID

1.9 Legend

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

Table 2 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
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 PSID Feature Set Overview

Begin Informative Content

The goal of the PSID Feature Set is to:

- Define an authority/credential pair whose C_PIN object's PIN column value is not discoverable via the interface.
- Provide access control settings that permit invocation of the Revert method if the PSID authority has been successfully authenticated.

The primary use case for this is one where the SID is not known, or manageability of the device has been lost, and the owner wishes to attempt to reset the device to OFS via the Revert method defined in [3].

Because the PSID credential value is specified such that it is not discoverable via the interface, it is necessary that the credential value be delivered via an alternative mechanism. Examples of these mechanisms include printing the PSID credential on a device label; or including the value as an insert in the device packaging. The delivery mechanism is vendor unique.

End Informative Content

3 SSC Specific Functionality

This feature set requires no additional SSC-specific functionality.

4 Feature Set Requirements

This section defines the Mandatory (M) and Optional (O) requirements for the PSID Feature Set, when it is implemented in an Opal-compliant device.

4.1 Level 0 Discovery

No Level 0 Feature Descriptor is needed for this feature set. Support for the PSID Feature Set can be determined by inspection of the Admin SP's `Authority` table.

4.2 Admin SP

An Opal-compliant SD that contains the PSID Feature Set SHALL contain the additions to the Admin SP specified in this section, in addition to the Admin SP requirements defined in [3].

4.2.1 PSID Authority (M)

The PSID authority SHALL have the characteristics defined in this section.

Table 1 PSID Authority

UID	Name	CommonName	IsClass	Class	Enabled	Secure	HashAndSign	PresentCertificate	Operation	Credential	ResponseSign	ResponseExch	ClockStart	ClockEnd	Limit	Uses	Log	LogTo
00 00 00 09 00 01 FF 01	"PSID"	"PhysicalDrive Owner"	F	Null	T	None	None	F	Password	C_PIN_PSID	Null	Null						

4.2.1.1 PSID Authority Object Access Control

Access control on methods applicable to the PSID authority object are as defined in this section.

Table 2 PSID Authority Access Control Settings

Table Association - informative oly	UID	InvokingID	InvokingID Name - informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
Authority																
		00 00 00 09 00 01 FF 01	PSID	Get		ACE_Anybody				ACE_Anybody						

4.2.2 PSID Authority Associated Credential

This section defines the attributes of the credential associated with the PSID authority, C_PIN_PSID. Support for this credential is Mandatory (M) if the PSID authority is supported.

The PIN column value SHALL contain a vendor unique value that is a statistically unique value for each device.

Table 3 PSID C_PIN

UID	Name	CommonName	PIN	CharSet	TryLimit	Tries	Persistence
00 00 00 0B 00 01 FF 01	"C_PIN_PSID"	"PhysicalDriveOwner"	VU	Null	VU	VU	FALSE

4.2.2.1 PSID C_PIN Object Access Control

Access control on methods applicable to the PSID C_PIN object are as defined in this section.

Table 4 PSID C_PIN Access Control Settings

Table association - Informative text	UID	InvokingID	InvokingID Name - Informative text	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
C_PIN																
		00 00 00 0B 00 01 FF 01	C_PIN_PSID	Get		ACE_C_PIN_Get_PSID_NoPIN				ACE_Anybody						

4.2.3 New ACEs

This section defines new ACEs to be added in conjunction with the PSID authority/credential.

4.2.3.1 ACE_C_PIN_Get_PSID_NoPIN

This section defines the ACE that enables retrieval of the attributes of C_PIN_PSID.

Support for this ACE is Mandatory (M) if the PSID authority is supported.

Table 5 ACE_C_PIN_Get_PSID_NoPIN ACE

Table Assocuiation - Informative text	UID	Name	CommonName	BooleanExpr	Columns
ACE					
	00 00 00 08 00 01 00 E1	"ACE_C_PIN_Get_PSID_NoPIN"		Anybody	UID, CharSet, TryLimit, Tries, Persistence

4.2.3.1.1 ACE_C_PIN_Get_PSID_NoPIN Access Control

Get access to ACE objects is as defined by [3].

4.2.3.2 ACE_SP_PSID

This section defines the ACE that allows the PSID authority to be used to perform a device reversion operation.

Support for this ACE is Mandatory (M) if the PSID authority is supported.

Table 6 ACE_SP_PSID ACE

Table Assocuiation - Informative text	UID	Name	CommonName	BooleanExpr	Columns
ACE					
	00 00 00 08 00 01 00 E0	"ACE_SP_PSID"		PSID	All

4.2.3.2.1 ACE_SP_PSID Access Control

Get access to ACE objects is as defined by [3].

4.2.4 Performing Device Reversion

This section details the access control settings for using the PSID authority to invoke the Revert method.

Support for this capability is Mandatory (M) if the PSID authority is supported.

Table 7 Device Reversion Access Control Settings

Table Association - informative oly	UID	InvokingID	InvokingID Name - informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
ACE																
		00 00 02 05 00 00 00 01	AdminSPObj	Revert		ACE_SP_SID, ACE_SP_PSID				ACE_Anybody						

4.3 Locking SP

This feature set requires no additions to the Locking SP.

4.4 Additional SPs

This feature set requires no additional SPs.