Disclaimers, Notices, and License Terms

THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

This document is copyrighted by Trusted Computing Group (TCG), and no license, express or implied, is granted herein other than as follows: You may not copy or reproduce the document or distribute it to others without written permission from TCG, except that you may freely do so for the purposes of (a) examining or implementing TCG specifications or (b) developing, testing, or promoting information technology standards and best practices, so long as you distribute the document with these disclaimers, notices, and license terms.

Contact the Trusted Computing Group at www.trustedcomputinggroup.org for information on specification licensing through membership agreements.

Any marks and brands contained herein are the property of their respective owners.
## TABLE OF CONTENTS

1 **INTRODUCTION** ............................................................................................................................................... 1  
1.1 **DOCUMENT PURPOSE** .......................................................................................................................... 1  
1.2 **SCOPE AND INTENDED AUDIENCE** ........................................................................................................ 1  
1.3 **KEY WORDS** ........................................................................................................................................... 1  
1.4 **DOCUMENT REFERENCES** ....................................................................................................................... 1  
1.5 **DOCUMENT PRECEDENCE** ....................................................................................................................... 1  
1.6 **DEPENDENCIES ON OTHER FEATURE SETS** .......................................................................................... 2  
1.7 **INTERACTIONS WITH OTHER FEATURE SETS** ....................................................................................... 2  
1.8 **TERMINOLOGY** ........................................................................................................................................ 2  
1.9 **LEGEND** .................................................................................................................................................. 3  

2 **PSID FEATURE SET OVERVIEW** ................................................................................................................. 4  

3 **SSC SPECIFIC FUNCTIONALITY** ................................................................................................................ 5  

4 **FEATURE SET REQUIREMENTS** ............................................................................................................... 6  

4.1 **LEVEL 0 DISCOVERY** ............................................................................................................................... 6  
4.2 **ADMIN SP** ............................................................................................................................................... 6  
4.2.1 **PSID Authority (M)** ............................................................................................................................. 6  
4.2.1.1 **PSID Authority Object Access Control** .......................................................................................... 6  
4.2.2 **PSID Authority Associated Credential** .............................................................................................. 7  
4.2.2.1 **PSID C_PIN Object Access Control** ............................................................................................ 7  
4.2.3 **New ACES** .......................................................................................................................................... 7  
4.2.3.1 **ACE_C_PIN_Get_PSID_NoPIN** ..................................................................................................... 7  
4.2.3.1.1 **ACE_C_PIN_Get_PSID_NoPIN Access Control** ....................................................................... 8  
4.2.3.2 **ACE_SP_PSID** ............................................................................................................................... 8  
4.2.3.2.1 **ACE_SP_PSID Access Control** .................................................................................................. 8  
4.2.4 **Performing Device Reversion** ............................................................................................................ 8  
4.3 **LOCKING SP** .......................................................................................................................................... 9  
4.4 **ADDITIONAL SPS** ................................................................................................................................. 9
Tables

Table 1  PSID Authority.................................................................................................................................6
Table 2  PSID Authority Access Control Settings ..........................................................................................6
Table 3  PSID C_PIN ................................................................................................................................7
Table 4  PSID C_PIN Access Control Settings ...........................................................................................7
Table 5  ACE_C_PIN_Get_PSID_NoPIN ACE..............................................................................................8
Table 6  ACE_SP_PSID ACE .........................................................................................................................8
Table 7  Device Reversion Access Control Settings ................................................................................9
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”


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


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)
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>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSID</td>
<td>Physical Presence SID</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Table Cell Legend</th>
<th>R-W</th>
<th>Value</th>
<th>Access Control</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arial-Narrow</td>
<td>Read-only</td>
<td>Opal SSC specified</td>
<td>Fixed</td>
<td>• Cell content is Read-Only. &lt;br&gt;• Access control is fixed. &lt;br&gt;• Value is specified by the Opal SSC</td>
</tr>
<tr>
<td>Arial Narrow bold-under</td>
<td>Read-only</td>
<td>VU</td>
<td>Fixed</td>
<td>• Cell content is Read-Only. &lt;br&gt;• Access Control is fixed. &lt;br&gt;• Values are Vendor Unique (VU). A minimum or maximum value may be specified.</td>
</tr>
<tr>
<td>Arial-Narrow Not Defined</td>
<td>(N)</td>
<td>Not Defined</td>
<td>Not Defined</td>
<td>• Cell content content is (N). &lt;br&gt;• Access control is not defined. &lt;br&gt;• Any text in table cell is informative only. &lt;br&gt;• A Get MAY omit this column from the method response.</td>
</tr>
<tr>
<td>Arial Narrow bold-under</td>
<td>Write</td>
<td>Preconfigured, user personalizable</td>
<td>Preconfigured, user personalizable</td>
<td>• Cell content is writable. &lt;br&gt;• Access control is personalizable &lt;br&gt;• Get Access Control is not described by this color coding</td>
</tr>
<tr>
<td>Arial-Narrow</td>
<td>Write</td>
<td>Preconfigured, user personalizable</td>
<td>Fixed</td>
<td>• Cell content is writable. &lt;br&gt;• Access control is fixed. &lt;br&gt;• Get Access Control is not described by this color coding</td>
</tr>
</tbody>
</table>
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 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.
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>
<thead>
<tr>
<th>Table 1 PSID Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>UID</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>00 00 00 09</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Table 2 PSID Authority Access Control Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table Association</td>
</tr>
</tbody>
</table>
| Authority | 00 00 00 09 | PSID | Get | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_Anybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybody | ACE_A nybo
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>
<thead>
<tr>
<th>UID</th>
<th>Name</th>
<th>CommonName</th>
<th>PIN</th>
<th>CharSet</th>
<th>TryLimit</th>
<th>Tries</th>
<th>Persistence</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 00 00 0B 00 01 FF 01</td>
<td>&quot;C_PIN_PSID&quot;</td>
<td>&quot;PhysicalDriveOwner&quot;</td>
<td>VU</td>
<td>NULL</td>
<td>VU</td>
<td>VU</td>
<td>FALSE</td>
</tr>
</tbody>
</table>

### 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>
<thead>
<tr>
<th>Table association</th>
<th>UID</th>
<th>InvokingID</th>
<th>InvokingID.Name</th>
<th>MethodID</th>
<th>CommonName</th>
<th>ACL</th>
<th>AddACEACL</th>
<th>RemoveACEACL</th>
<th>GetACLACL</th>
<th>DeleteMethodACL</th>
<th>AddACELog</th>
<th>RemoveACELog</th>
<th>GetACLLog</th>
<th>DeleteMethodLog</th>
<th>LogTo</th>
</tr>
</thead>
<tbody>
<tr>
<td>C_PIN</td>
<td></td>
<td>00 00 00 0B 00 01 FF 01</td>
<td>C_PIN_PSID</td>
<td>Get</td>
<td>ACE.C_PIN.Get.PSID_NoPIN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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>
<thead>
<tr>
<th>Table Association - Informative text</th>
<th>UID</th>
<th>Name</th>
<th>CommonName</th>
<th>BooleanExpr</th>
<th>Columns</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACE</td>
<td>00 00 00 08 00 01 00 E1</td>
<td>“ACE_C_PIN_Get_PSID_NoPIN”</td>
<td>Anybody</td>
<td>UID, CharSet, TryLimit, Tries, Persistence</td>
<td></td>
</tr>
</tbody>
</table>

#### 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>
<thead>
<tr>
<th>Table Association - Informative text</th>
<th>UID</th>
<th>Name</th>
<th>CommonName</th>
<th>BooleanExpr</th>
<th>Columns</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACE</td>
<td>00 00 00 08 00 01 00 E0</td>
<td>“ACE_SP_PSID”</td>
<td>PSID</td>
<td>All</td>
<td></td>
</tr>
</tbody>
</table>

#### 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.
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.