TCG Storage
Opal SSC Feature Set:
Single User Mode

Specification Version 1.00
Revision 1.00

February 24, 2012

Contact: admin@trustedcomputinggroup.org
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.
## Change History

<table>
<thead>
<tr>
<th>Version 1.00</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rev 1.00</td>
<td>February 24, 2012</td>
<td>First publication</td>
</tr>
</tbody>
</table>
TABLE OF CONTENTS

1 INTRODUCTION ........................................................................................................................................7
  1.1 DOCUMENT PURPOSE ..................................................................................................................7
  1.2 SCOPE AND INTENDED AUDIENCE ..............................................................................................7
  1.3 KEY WORDS ....................................................................................................................................7
  1.4 DOCUMENT REFERENCES ...............................................................................................................7
  1.5 DOCUMENT PRECEDENCE ............................................................................................................7
  1.6 DEPENDENCIES ON OTHER FEATURE SETS ..............................................................................8
  1.7 INTERACTIONS WITH OTHER FEATURE SETS ............................................................................8
  1.8 LEGEND .........................................................................................................................................9

2 SINGLE USER MODE OVERVIEW .......................................................................................................10

3 SSC SPECIFIC FUNCTIONALITY ..........................................................................................................11
  3.1 METHODS ....................................................................................................................................11
    3.1.1 New Methods ..........................................................................................................................11
      3.1.1.1 Reactivate ..........................................................................................................................11
      3.1.1.2 Erase ...................................................................................................................................12
    3.1.2 Modified Methods ....................................................................................................................13
      3.1.2.1 Activate ..............................................................................................................................13
  3.2 TABLES ........................................................................................................................................14
    3.2.1 New Tables ...............................................................................................................................14
    3.2.2 Modified Tables ........................................................................................................................14

3.3 TYPES ............................................................................................................................................15
  3.3.1 New Types ................................................................................................................................15
    3.3.1.1 Locking_object_ref ................................................................................................................15
    3.3.1.2 single_user_ranges ................................................................................................................15
    3.3.1.3 policy_enum ............................................................................................................................15
  3.3.2 Modified Types ..........................................................................................................................16

4 FEATURE SET REQUIREMENTS .........................................................................................................17
  4.1 REQUIREMENTS OVERVIEW .........................................................................................................17
  4.2 LEVEL 0 DISCOVERY .....................................................................................................................19
    4.2.1 Single User Mode Feature Descriptor (Feature Code = 0x0201) ....................................................19
      4.2.1.1 Number of Locking Objects Supported ..............................................................................19
      4.2.1.2 Any ....................................................................................................................................19
      4.2.1.3 All ......................................................................................................................................19
      4.2.1.4 Policy ................................................................................................................................19
      4.2.1.5 Level 0 requirements for the Single User Mode Fixed Access Control Feature Descriptor ......19
  4.3 ADMIN SP ....................................................................................................................................19
    4.3.1 Activate Method .........................................................................................................................19
  4.4 LOCKING SP ................................................................................................................................20
    4.4.1 Authority -> Locking Association ...............................................................................................20
    4.4.2 MethodID (M) ............................................................................................................................20
    4.4.3 LockingInfo Table ......................................................................................................................20
      4.4.3.1 SingleUserModeRanges column .........................................................................................21
      4.4.3.2 RangeStartRangeLengthPolicy column .............................................................................21
    4.4.4 Single User Mode ......................................................................................................................22
      4.4.4.1 General Changes ..................................................................................................................22
      4.4.4.1.1 Method – Reactivate ........................................................................................................22
      4.4.4.1.2 Authority – Admin1 .........................................................................................................23
4.4.4.1.3 ACEs ........................................................................................................23
4.4.4.1.4 Table – LockingInfo ................................................................................24
4.4.4.2 Single User Mode Specific Changes ..........................................................24
  4.4.4.2.1 Global Range in Single User Mode .........................................................24
  4.4.4.2.2 RangeNNNN in Single User Mode .........................................................28
4.5 ADDITIONAL SPs..........................................................................................33
# Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>SP Table Legend</td>
<td>9</td>
</tr>
<tr>
<td>Table 2</td>
<td>Locking_object_ref</td>
<td>15</td>
</tr>
<tr>
<td>Table 3</td>
<td>single_user_ranges</td>
<td>15</td>
</tr>
<tr>
<td>Table 4</td>
<td>policy_enum</td>
<td>15</td>
</tr>
<tr>
<td>Table 5</td>
<td>policy_enum Enumeration Values</td>
<td>15</td>
</tr>
<tr>
<td>Table 6</td>
<td>Level 0 Discovery - Single User Mode Feature Descriptor</td>
<td>19</td>
</tr>
<tr>
<td>Table 7</td>
<td>User Authority/Locking Object Associations</td>
<td>20</td>
</tr>
<tr>
<td>Table 8</td>
<td>MethodID Table Modifications For Single User Mode Support</td>
<td>20</td>
</tr>
<tr>
<td>Table 9</td>
<td>LockingInfo Table Description</td>
<td>21</td>
</tr>
<tr>
<td>Table 10</td>
<td>AccessControl Table Modifications for Reactivate Method Support</td>
<td>22</td>
</tr>
<tr>
<td>Table 11</td>
<td>New/Modified ACEs for Reactivate Method Support</td>
<td>23</td>
</tr>
<tr>
<td>Table 12</td>
<td>Admin1 Authority AccessControl Table Changes</td>
<td>23</td>
</tr>
<tr>
<td>Table 13</td>
<td>General AccessControl Table Changes</td>
<td>24</td>
</tr>
<tr>
<td>Table 14</td>
<td>Access Control Table Modifications for Global Range Single User Mode</td>
<td>25</td>
</tr>
<tr>
<td>Table 15</td>
<td>New/Modified ACEs for Global Range Single User Mode</td>
<td>27</td>
</tr>
<tr>
<td>Table 16</td>
<td>Authority Table Modifications for Global Range Single User Mode</td>
<td>28</td>
</tr>
<tr>
<td>Table 17</td>
<td>AccessControl Table Modifications for RangeNNNN Single User Mode</td>
<td>29</td>
</tr>
<tr>
<td>Table 18</td>
<td>New/Modified ACEs for RangeNNNN Single User Mode</td>
<td>32</td>
</tr>
<tr>
<td>Table 19</td>
<td>Authority Table Modifications for RangeNNNN Single User Mode</td>
<td>33</td>
</tr>
</tbody>
</table>
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 Single User Mode for the Opal Security Subsystem Class (SSC). Any Storage Device that claims Opal SSC Single User Mode 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"
[4]. Trusted Computing Group (TCG), "TCG Storage Interface Interactions Specification", Version 1.02

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 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>
<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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Access control is fixed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Access Control is fixed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Values are Vendor Unique (VU). A minimum or maximum value may be specified.</td>
</tr>
<tr>
<td>Arial-Narrow</td>
<td>Not Defined</td>
<td>(N)</td>
<td>Not Defined</td>
<td>• Cell content content is (N).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Access control is not defined.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Any text in table cell is informative only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Access control is personalizable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• A 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Access control is fixed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• A Get Access Control is not described by this color coding</td>
</tr>
</tbody>
</table>
# 2 Single User Mode Overview

**Begin Informative Content**

The goal of the Single User Mode feature set is to provide a mechanism that addresses the following use cases:

1. The IT rep provisions the Storage Device and controls the partitions, but gives complete control over the access to at least one of the partitions to the VP. The VP is able to lock/unlock and enable/disable locking for the private partition(s) given to him. The IT rep should be able to repurpose the SD by reclaiming the storage, but only in a destructive way for the private partition(s) and should never be able to access to the data on the private partition(s) unless unlocked by the VP.

2. The Storage Device is used in a system where all user management is performed by host software. Multiple software agents may exist and each one has exclusive control over a range of the LBAs in the Storage Device. Each software agent has its own user management models and authentication mechanisms and there is no agent with control over another’s LBA ranges.

The feature set describes a mechanism whereby, upon successful invocation of the **Activate** method or the **Reactivate** method, the Locking SP enters either

1. The configurable access control mode defined in the Opal SSC, OR

2. A mixture of configurable and fixed access control modes where for some number of Locking objects, a single User authority is assigned sole ownership of a select Locking object, and the User’s associated password. Along with the Admins authority, that single User authority is also assigned the ability to cryptographically erase its associated LBA range.

**End Informative Content**
3  SSC Specific Functionality

This section defines the SSC-specific functionality (not contained in [2], [3], or [4]) required to support the Single User Mode feature set.

3.1  Methods

This section defines new methods and modifications to existing methods that are required to support the Single User Mode feature set.

3.1.1  New Methods

This section defines the new methods that are required to support the Single User Mode feature set.

3.1.1.1  Reactivate

The Reactivate method is a Locking Template-specific method.

```plaintext
ThisSP.Reactivate [ 
    SingleUserModeSelectionList = typeOr { 
        EntireLockingTable : LockingTableUID, 
        SelectedLockingObjects : list [ LockingObjectUIDs ] }, 
    RangeStartRangeLengthPolicy = enum{ 0 => User only, 1 => Admins only }, 
    Admin1PIN = bytes 
] => [ ]
```

Method UID: 00 00 00 06 00 00 08 01

The Reactivate method has three optional parameters:

1. SingleUserModeSelectionList
2. RangeStartRangeLengthPolicy
3. Admin1PIN

The following are the definitions of the parameters:

1. SingleUserModeSelectionList (Parameter Number 0x060000) –
   a. This TypeOr parameter allows the host to select which Locking object ranges to be controlled by a single User authority
      i. The EntireLockingTable alternative SHALL be used if the entire Locking table is to be put into Single User Mode. If this alternative is used in the Reactivate method, the parameter value SHALL be the UID of the Locking table (00 00 08 02 00 00 00 00).
      ii. The SelectedLockingObjects alternative SHALL be used if a subset of the Locking table is to be put into Single User Mode. If this alternative is used in the Reactivate method, the parameter value SHALL be a list of UIDs of Locking table objects.

2. RangeStartRangeLengthPolicy (Parameter Number 0x060001) –
   a. This parameter allows the host to select the ownership policy for the RangeStart and RangeLength columns of non-Global Range Locking objects and the ownership policy for the CommonName column of all Locking objects that have been selected in the SingleUserModeSelectionList parameter. This policy SHALL be applied to all of the Locking objects identified in the SingleUserModeSelectionList parameter except the Global Range (either a list of Locking objects, or all objects in the Locking table).
      i. A value of 0 indicates that the User authority associated with the Locking object SHALL be given sole ownership of the RangeStart, RangeLength, and CommonName of the selected Locking objects.
ii. A value of 1 indicates that the Admin’s authority SHALL maintain ownership of the 
RangeStart, RangeLength, and CommonName of the selected Locking objects.

3. Admin1PIN (Parameter Number 0x060002) –
   a. This parameter allows the host to define the Admin1 authority’s credential value upon 
      successful invocation of the Reactivate method.
      i. If this parameter is omitted, then upon successful invocation of the Reactivate 
         method, the Admin1 PIN SHALL remain at its current value.
      ii. If this parameter is included, then upon successful invocation of the Reactivate 
          method, the PIN column of the C_PIN object associated with the Admin1 authority 
          SHALL be set to the value of this parameter.

The following conditions apply to invocation of the Reactivate method with these parameters:

1. If the SingleUserModeSelectionList parameter is omitted or is included but is an empty list, the method 
   SHALL restore the SP to its Original Factory State, with the exceptions of the C_PIN Admin1.PIN value 
   if the Admin1PIN parameter is also omitted; the RangeStart and RangeLength column values of all 
   Locking objects; and the Life Cycle State of the SP.

2. If the SingleUserModeSelectionList parameter is included and the RangeStartRangeLengthPolicy 
   parameter is omitted, the method SHALL behave as if RangeStartRangeLengthPolicy was included and 
   set to 0.

For successful completion of the Reactivate method, the ReadLockEnabled and WriteLockEnabled column 
values SHALL be False for all Locking objects. If either of those column values of any Locking object is not 
False, the method SHALL fail with FAIL.

Successful method invocation restores the Locking SP to its Original Factory State with the following 
exceptions:

1. The Life Cycle State of the SP does not change. The LifeCycleState column of the SP’s object in the 
   Admin SP’s SP table remains the same.

2. The C_PIN.PIN column value of the C_PIN object associated with the Admin1 credential 
   (“C_PIN_Admin1”) is dependent on the presence and value of the Reactivate method’s Admin1PIN 
   parameter.

3. The RangeStart and RangeLength column values in the Locking table remain at their current values.

4. The media encryption keys in the K_AES_128 and K_AES_256 tables remain at their current values.

The method then applies the Single User Mode customizations to either the entire Locking table or to the 
individual Locking objects enumerated in the method.

This method operates within a Read-Write session to the Locking SP. The TPer SHALL reactivate the SP 
immediately after the method is successfully invoked outside of a transaction. Upon completion of reactivation 
of the SP, the TPer SHALL report status of the method invocation if invoked outside of a transaction, and then 
immediately abort the session. The TPer MAY prepare a CloseSession method for retrieval by the host to 
indicate that the session has been aborted.

Support for Reactivate within transactions is (N), and the behavior is out of the scope of this document.

3.1.1.2 Erase
The UID for the Erase method is: 00 00 00 06 00 00 08 03
This method is used to cryptographically erase user data within a specific LBA Range and to reset the locking states of that LBA Range, as well as the C_PIN column value of the User authority associated with that range.

The **Erase** method is an object method and is defined as:

```
LockingObjectUID.Erase [ ]
=> [ ]
```

When the **Erase** method is invoked, the TPer SHALL:

1. Eradicate the current media encryption key for the LBA Range managed by the Locking object on which the method is invoked;
2. Generate a new media encryption key for the LBA Range managed by the Locking object on which the method is invoked;
3. Set the ReadLockEnabled, WriteLockEnabled, ReadLocked, and WriteLocked column values to "False" for the Locking object on which the method is invoked;
4. Set the credential value of the associated User authority to its default value of "" as defined in the Opal SSC and set Tries for that credential to zero.

The TPer SHALL NOT change the values of the invoking Locking object’s RangeStart and RangeLength columns.

The method call fails with status NOTAUTHORIZED if:

1. The invoking object does not exist;
2. The invoking object is not a Locking object configured in Single User Mode.

### 3.1.2 Modified Methods

This section defines modifications to existing methods that are required to support the Single User Mode features set.

#### 3.1.2.1 Activate

The **Activate** method is modified as follows:

```
SPObjectUID.Activate[
    SingleUserModeSelectionList = typeOr { EntireLockingTable : LockingTableUID, SelectedLockingObjects : list [ LockingObjectUIDs ] },
    RangeStartRangeLengthPolicy = enum{ 0 => User only, 1 => Admins only }
]=> [ ]
```

Two optional parameters are added to the **Activate** method:

1. SingleUserModeSelectionList
2. RangeStartRangeLengthPolicy

The following are the definitions of the parameters:

1. **SingleUserModeSelectionList** (Parameter Number 0x060000) –
   a. This TypeOr parameter allows the host to select which Locking object ranges to be controlled by a single User authority
i. The EntireLockingTable alternative SHALL be used if the entire Locking table is to be put into Single User Mode. If this alternative is used in the Activate method, the value SHALL be the UID of the Locking table (00 00 08 02 00 00 00 00).

ii. The SelectedLockingObjects alternative SHALL be used if only a subset of the Locking table is to be put into Single User Mode. If this alternative is used in the Activate method, the value SHALL be a list of UIDs of Locking objects.

2. RangeStartRangeLengthPolicy (Parameter Number 0x060001) –

   a. This parameter allows the host to select the ownership policy for the RangeStart and RangeLength columns of non-Global Range Locking objects and the ownership policy for the CommonName column of all Locking objects that have been selected in the SingleUserModeSelectionList parameter. This policy SHALL be applied to all of the Locking objects identified in the SingleUserModeSelectionList parameter except for the Global Range (either a list of Locking objects, or all objects in the Locking table).

   i. A value of 0 indicates that the User authority associated with the Locking object SHALL be given sole ownership of the RangeStart, RangeLength, and CommonName of the selected Locking objects.

   ii. A value of 1 indicates that the Admins authority SHALL maintain ownership of the RangeStart, RangeLength, and CommonName of the selected Locking objects.

The following conditions apply to invocation of the Activate method with these parameters:

1. If neither parameter is included in Activate, the method SHALL behave as defined in Opal SSC.

2. If either parameter is included in Activate invoked on an SP object that does not include the Locking Template, the Activate method SHALL fail with INVALID_PARAMETER.

3. If the SingleUserModeSelectionList parameter is omitted, or is included but is an empty list, the method SHALL behave as defined in Opal SSC.

4. If the SingleUserModeSelectionList parameter is included and the RangeStartRangeLengthPolicy parameter is omitted, the method SHALL behave as if RangeStartRangeLengthPolicy was included and set to 0.

Per the Opal SSC, if the Activate method is invoked on an SP Object that is in any state other than Manufactured-Inactive, and access control has been satisfied, the method SHALL succeed and SHALL have no effect. Parameters submitted to an Activate method invocation on an SP Object that is in any state other than Manufactured-Inactive SHALL be ignored.

3.2 Tables
This section defines new tables and modifications to existing tables that are required to support the Single User Mode feature set.

3.2.1 New Tables
There are no new tables defined by this feature set.

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 that are required to support the Single User Mode feature set.

3.3.1 New Types
This section defines the new types that are required to support the Single User Mode feature set.

3.3.1.1 Locking_object_ref
This section describes the type that is a uidref to an object in the Locking table.

<table>
<thead>
<tr>
<th>UID</th>
<th>Name</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 00 00 05 00 00 0C 0E</td>
<td>Locking_object_ref</td>
<td>Restricted_Reference_Type(6), uidref {LockingTableUID}</td>
</tr>
</tbody>
</table>

3.3.1.2 single_user_ranges
This section describes the type used in the SingleUserModeRanges column.

<table>
<thead>
<tr>
<th>UID</th>
<th>Name</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 00 00 05 00 00 06 07</td>
<td>single_user_ranges</td>
<td>Alternative_Type, Locking_object_ref, Table_object_ref</td>
</tr>
</tbody>
</table>

3.3.1.3 policy_enum
This section describes the type used in the RangeStartLengthPolicy column.

<table>
<thead>
<tr>
<th>UID</th>
<th>Name</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 00 00 05 00 00 04 1E</td>
<td>policy_enum</td>
<td>Enumeration_Type, 0, 7</td>
</tr>
</tbody>
</table>

The enumeration values are associated as defined in Table 5.

<table>
<thead>
<tr>
<th>Enumeration Value</th>
<th>Associated Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>User authority RangeStart/RangeLength ownership policy</td>
</tr>
<tr>
<td>1</td>
<td>Admins authority RangeStart/RangeLength ownership policy</td>
</tr>
</tbody>
</table>
### 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 Single User Mode feature set, when it is implemented in an Opal-compliant device.

4.1 Requirements Overview
The following are the general requirements of the Single User Mode Feature Set. The specific table/object additions/modifications to support these requirements are detailed in later sections.

1. Single User Mode Locking ranges SHALL be assigned either upon successful invocation of the Activate method on the Locking SP’s SP object (in the Admin SP’s SP table) or successful invocation of the Reactivate method in a session to the Locking SP.

2. For the Reactivate method, all of the personalization of the SP to which the method was successfully invoked SHALL be reset to Original Factory State, with the following exceptions:
   a. The Life Cycle State of the SP does not change. The LifeCycleState column of the SP’s object in the Admin SP’s SP table remains the same.
   b. The C_PIN.PIN column value of the C_PIN object associated with the Admin1 credential (“C_PIN_Admin1”) is dependent on the presence and value of the Reactivate method’s Admin1PIN parameter.
   c. The RangeStart and RangeLength column values in the Locking table remain at their current values.
   d. The media encryption keys in the K_AES_128 and K_AES_256 tables remain at their current values.

3. The BooleanExpr column of the ACE that controls access to the Reactivate method SHALL be modifiable by Admins.

4. For each Locking object identified in the Activate or Reactivate method, the associated User authority SHALL have its Enabled column set to True.
   a. The User authorities participating in Single User Mode are Enabled.
   b. The default password for User authorities is “” (as defined in Opal SSC).

5. For each Locking object identified in the Activate or Reactivate method, a single User authority SHALL be given sole ownership over the capability to successfully invoke the Set method on the ReadLockEnabled, WriteLockEnabled, ReadLocked, WriteLocked, and LockOnReset columns of that Locking object. Admins access to Set these columns SHALL be removed.
   a. Only that User controls the range’s locking properties.

6. For each User authority assigned as a Single User Mode Locking object owner, that authority SHALL be given sole ownership over the ability to successfully invoke the Set method on the PIN column of its C_PIN object. Admins access to Set this column SHALL be removed.
   a. Only that User has access to change its PIN.

7. For each User authority assigned as a Single User Mode Locking object owner, that authority SHALL be given sole ownership over the ability to successfully invoke the Set method on the CommonName column of its Authority object. Admins access to Set this column SHALL be removed.
   a. Only that User has access to change its CommonName.

8. For each Locking object identified in the Activate or Reactivate method, the associated User and the Admins class authority SHALL both be given access to successfully invoke the Erase method on that Locking object.
a. Either the associated User or Admins has access to successfully invoke Erase on its range. The BooleanExpr column of the controlling ACE SHALL be modifiable by Admins.

b. Upon invocation of Erase on a Locking object, the associated User authority’s C_PIN object’s PIN column SHALL be set to the default ""

9. For each Locking object identified in the Activate or Reactivate method, the associated User SHALL be given access to successfully invoke GenKey on the media encryption key (K_AES_* object) associated with that Locking object.

a. The User is able to cause the storage device to directly generate a new media encryption key for that User’s range (without any of the additional changes that would occur if the Erase method were to be used).

b. The ACE controlling access to the GenKey method for that User’s range becomes non-modifiable.

10. User authorities that are assigned as Single User Mode Locking object owners SHALL NOT be permitted to be added to any other Locking object-related ACEs.

a. Single User Mode User authorities SHALL have access to manage only the Locking objects to which each is assigned.

b. Attempts to assign Single User Mode User authorities to ACEs that are used to control access to Get or Set on non-Single User Mode Locking object attributes; that enable invocation of the GenKey method; or that enable invocation of Erase on another Locking object other than their own SHALL result in a method failure with status INVALID_PARAMETER.

11. User authorities that are assigned as Single User Mode Locking object owners are removed from the Users class.

a. Single User Mode User authorities SHALL have their Class column set to the NULL UID.

12. User authorities that are assigned as Single User Mode fixed Locking object owners are not able to be disabled.

a. The ACE_Authority_Set_Enabled SHALL be removed from the ACL column of the access control association for Set on each Single User Mode User authority.

13. The Admin1 authority’s Enabled column SHALL be modifiable by Admins.

14. The ownership access to successfully invoke Set on RangeStart and RangeLength of non-Global Range columns identified in the Activate or Reactivate method SHALL be selectable for all participating Locking objects upon invocation of the Activate or Reactivate method

a. Modification of RangeStart and RangeLength is assigned in the Activate or Reactivate method to either Admins or the User associated with the Locking object. This assignment is global for all Single User Mode Locking objects.

15. The ownership access to successfully invoke Set on CommonName of Locking objects identified in the Activate or Reactivate method SHALL be selectable for all participating Locking objects upon invocation of the Activate or Reactivate method

a. Modification of CommonName is assigned in the Activate or Reactivate method to either Admins or the User associated with the Locking object. This assignment is global for all Single User Mode Locking objects.

16. The Locking object ownership assignment SHALL only be undone by Locking SP reversion (via Revert/RevertSP), or via subsequent successful invocation(s) of the Reactivate method.
4.2 Level 0 Discovery

An Opal-compliant SD that contains the Single User Mode feature set SHALL return the Single User Mode Feature Descriptor as described in 4.2.1, in addition to the Level 0 Discovery response requirements defined in [3].

4.2.1 Single User Mode Feature Descriptor (Feature Code = 0x0201)

This feature descriptor SHALL be returned when the Opal-compliant SD supports the Single User Mode feature set. The contents of the feature descriptor are defined in Table 6.

| Table 6 Level 0 Discovery - Single User Mode Feature Descriptor |
|---|---|---|---|---|---|---|---|---|
| Bit Byte | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 0 (MSB) | Feature Code | | | | | | | |
| 1 | | Version | Reserved | | | | | |
| 2 | Number of Locking Objects Supported | | | | | | | |
| 3 | Length | | | | | | | |
| 8 | Reserved | Policy | All | Any |
| 9-15 | Reserved | | | | | | |

4.2.1.1 Number of Locking Objects Supported

This value indicates the number of Locking objects supported in the Locking table of the Locking SP.

4.2.1.2 Any

This bit is 1 if any Locking objects are in Single User Mode. Otherwise, this bit is 0.

4.2.1.3 All

This bit is 1 if all Locking objects are in Single User Mode. Otherwise, this bit is 0.

4.2.1.4 Policy

This bit is 1 if Admins authority maintains ownership of the RangeStart and RangeLength of Locking objects in Single User Mode, or if the Locking SP is in any life cycle state other than Manufactured or Issued.

This bit is 0 if User authorities of Locking objects in Single User Mode have ownership of their associated RangeStart and RangeLength columns.

4.2.1.5 Level 0 requirements for the Single User Mode Fixed Access Control Feature Descriptor

- **Feature Code**: 0x0201
- **Version**: 0x1 or any version that supports the defined features in this specification
- **Length**: 0x0C

4.3 Admin SP

An Opal-compliant SD that contains the Single User Mode feature set SHALL contain the additions to the Admin SP specified in this section, in addition to the Admin SP requirements defined in [3].

4.3.1 Activate Method

An Opal-compliant SD that contains the Single User Mode feature set SHALL support the modifications to the Activate method defined in section 3.1.2.1.
4.4 Locking SP
An Opal-compliant SD that contains the Single User Mode feature set SHALL contain the additions to the Locking SP specified in this section, in addition to the Locking SP requirements defined in [3].

4.4.1 Authority -> Locking Association
For each Locking object identified in the Activate or Reactivate method, a single User authority is given sole ownership over the capability to successfully invoke the Set method on the ReadLockEnabled, WriteLockEnabled, ReadLocked, WriteLocked, and LockOnReset columns of that Locking object (Admins access to Set these columns is removed).

User Authorities and Locking Objects are associated as indicated in Table 7.

<table>
<thead>
<tr>
<th>Locking Object UID</th>
<th>Locking Object Name</th>
<th>Associated User Authority UID</th>
<th>Associated User Authority Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 00 08 02</td>
<td>Locking_GlobalRange</td>
<td>00 00 00 09</td>
<td>User1</td>
</tr>
<tr>
<td>00 00 00 01</td>
<td></td>
<td>00 03 00 01</td>
<td></td>
</tr>
<tr>
<td>00 00 08 02</td>
<td>Locking_Range1</td>
<td>00 00 00 09</td>
<td>User2</td>
</tr>
<tr>
<td>00 03 00 01</td>
<td></td>
<td>00 03 00 02</td>
<td></td>
</tr>
<tr>
<td>00 00 08 02</td>
<td>Locking_RangeNNNN</td>
<td>00 00 00 09</td>
<td>User(NNNN+1)</td>
</tr>
<tr>
<td>00 03 NN NN</td>
<td></td>
<td>00 03 (NN NN+1)</td>
<td></td>
</tr>
</tbody>
</table>

4.4.2 MethodID (M)
Table 8 lists the additional entries in the Locking SP's MethodID table that are required for the Single User Mode feature set.

<table>
<thead>
<tr>
<th>UID</th>
<th>Name</th>
<th>CommonName</th>
<th>TemplateID</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 00 00 06 00 00 08 01</td>
<td>&quot;Reactivate&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00 00 00 06 00 00 08 03</td>
<td>&quot;Erase&quot;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.4.3 LockingInfo Table
This section details the addition of columns to the LockingInfo table that enable the host to discover the Locking objects activated in Single User Mode. The updated format of the LockingInfo table is as defined in Table 9. The description of the new columns is found in 4.4.3.1 and 4.4.3.2. The description of the types of the new columns is found in 3.3.1.

Two new columns are added to the LockingInfo table. The value of the first column is a list of UIDs that identify the Locking objects that are in Single User Mode. The value of the second column is an enumeration value that identifies the RangeStart/RangeLength management policy.
Table 9 LockingInfo Table Description

<table>
<thead>
<tr>
<th>Column Number</th>
<th>Column Name</th>
<th>IsUnique</th>
<th>Column Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>UID</td>
<td></td>
<td>uid</td>
</tr>
<tr>
<td>0x01</td>
<td>Name</td>
<td></td>
<td>name</td>
</tr>
<tr>
<td>0x02</td>
<td>Version</td>
<td></td>
<td>uinteger_4</td>
</tr>
<tr>
<td>0x03</td>
<td>EncryptSupport</td>
<td></td>
<td>enc_supported</td>
</tr>
<tr>
<td>0x04</td>
<td>MaxRanges</td>
<td></td>
<td>uinteger_4</td>
</tr>
<tr>
<td>0x05</td>
<td>MaxReEncryptions</td>
<td></td>
<td>uinteger_4</td>
</tr>
<tr>
<td>0x06</td>
<td>KeysAvailableCfg</td>
<td></td>
<td>keys_avail_conds</td>
</tr>
<tr>
<td>0x060000</td>
<td>SingleUserModeRanges</td>
<td></td>
<td>single_user_ranges</td>
</tr>
<tr>
<td>0x060001</td>
<td>RangeStartLengthPolicy</td>
<td></td>
<td>policy_enum</td>
</tr>
</tbody>
</table>

4.4.3.1 SingleUserModeRanges column
1. Column Number: 0x060000
2. Name: SingleUserModeRanges
3. Contents: List of Locking object UIDs OR the Locking Table UID
   a. List of Locking object UIDs identifies the Locking objects activated in Single User Mode.
   b. Locking table UID indicates all of the Locking objects in the Locking table are activated in Single User Mode
   c. Empty list indicates no Locking objects are activated in Single User Mode.
4. Special: Column is READ-ONLY
5. Column Type: single_user_ranges

4.4.3.2 RangeStartRangeLengthPolicy column
1. Column Number: 0x060001
2. Name: RangeStartRangeLengthPolicy
3. Contents: an enumeration with one of the following defined values:
   a. 0 : the associated User authorities own access to modify the RangeStart and RangeLength columns of Single User Mode Locking objects.
   b. 1 : the Admins authority maintains ownership of the RangeStart and RangeLength of the selected Locking objects.
4. Special: Column is READ-ONLY
5. Column Type: policy_enum

If there are no Locking objects in Single User Mode, then the RangeStartRangeLengthPolicy column value in the LockingInfo table SHALL be 1.
4.4.4 Single User Mode

This section describes specific additions and modifications to tables and objects defined by Opal to support functionality required to support the Single User Mode Feature Set.

4.4.4.1 General Changes

This section describes general additions and modifications to tables and objects defined by Opal to support the Single User Mode Feature Set.

4.4.4.1.1 Method – Reactivate

Devices that implement the Single User Mode Feature Set SHALL support the Reactivate method as defined in 3.1.1.1.

4.4.4.1.1 Reactivate Method AccessControl Table Changes

This section details the modifications/additions to the AccessControl table to support the Reactivate method.

<table>
<thead>
<tr>
<th>InvokingID</th>
<th>MethodID</th>
<th>CommonName</th>
<th>ACL</th>
<th>Log</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>00 00 00 00 00 00 00 01</td>
<td>ThisSP</td>
<td>Reactivate</td>
<td>ACE_SP_Reactivate_Admin</td>
<td>ACE_Anybody</td>
<td>ACE_SP_Reactivate_Admin</td>
<td>ACE_Anybody</td>
<td>ACE_Anybody</td>
<td>ACE_Anybody</td>
<td>ACE_Anybody</td>
<td>ACE_Anybody</td>
<td>ACE_Anybody</td>
<td>ACE_Anybody</td>
<td>ACE_Anybody</td>
</tr>
<tr>
<td>00 00 00 00 00 04 20 01</td>
<td>ACE_SP_Reactivate_Admin</td>
<td>Set</td>
<td>ACE_ACE_Set_BooleanExpression</td>
<td>ACE_Anybody</td>
<td>ACE_ACE_Set_BooleanExpression</td>
<td>ACE_Anybody</td>
<td>ACE_ACE_Set_BooleanExpression</td>
<td>ACE_Anybody</td>
<td>ACE_ACE_Set_BooleanExpression</td>
<td>ACE_Anybody</td>
<td>ACE_ACE_Set_BooleanExpression</td>
<td>ACE_Anybody</td>
<td>ACE_ACE_Set_BooleanExpression</td>
</tr>
</tbody>
</table>

Table 10 AccessControl Table Modifications for Reactivate Method Support
4.4.4.1.2 ACE

This section details the modifications/additions to the ACE table to support the Reactivate method.

Table 11 New/Modified ACEs for Reactivate Method Support

<table>
<thead>
<tr>
<th>UID</th>
<th>Name</th>
<th>CommonName</th>
<th>BooleanExpr</th>
<th>Columns</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 00 00 08</td>
<td>* ACE_SP_Reactivate_Admin</td>
<td></td>
<td>Admins</td>
<td></td>
</tr>
<tr>
<td>00 04 20 01</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.4.4.1.2 Authority – Admin1

In an Opal-compliant SD that supports the Single User Mode Feature Set, the Admin1 authority’s Enabled column SHALL be modifiable by Admins.

Table 12 Admin1 Authority AccessControl Table Changes

<table>
<thead>
<tr>
<th>InvokingID</th>
<th>InvokingID Name</th>
<th>MethodID</th>
<th>CommonName</th>
<th>ACL</th>
<th>Log</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>00 00 00 09</td>
<td>Admin1</td>
<td>Set</td>
<td>ACE_Authority_Set Enabled</td>
<td>ACE_Anybody</td>
<td>ACE_Anybody</td>
<td>ACE_Anybody</td>
<td>ACE_Anybody</td>
<td>ACE_Anybody</td>
<td>ACE_Anybody</td>
<td>ACE_Anybody</td>
<td>ACE_Anybody</td>
<td>ACE_Anybody</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00 01 00 01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.4.4.1.3 ACEs

For each ACE added by activation of 1 or more single user mode ranges, that ACE SHALL have an entry in the AccessControl table to allow invocation of the Get method on it, as defined by the following table.
Table 13 General AccessControl Table Changes

<table>
<thead>
<tr>
<th>InvokingID</th>
<th>InvokingID Name</th>
<th>MethodID</th>
<th>CommonName</th>
<th>ACL</th>
<th>Log</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>00 00 00 08</td>
<td>ACE Name</td>
<td>Get</td>
<td>ACE_ACE_Get_All</td>
<td>ACE_Anybody</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.4.4.1.4 Table – LockingInfo
An Opal-compliant SD that contains the Single User Mode feature set SHALL support the LockingInfo table with the addition of the columns described in 4.4.3.

4.4.4.2 Single User Mode Specific Changes
The following subsections detail the modifications/changes that support Locking ranges identified in the Activate or Reactivate method as Single User Mode ranges.

4.4.4.2.1 Global Range in Single User Mode
The following subsections identify the additions/modifications to the settings defined in the Opal SSC if the Global Range is identified in the Activate or Reactivate method as a Single User Mode range.

4.4.4.2.1.1 AccessControl Table Modifications
If the Global Range is in Single User Mode, the following access control associations are removed from the AccessControl table:

1. ACE_Locking_GlobalRange_Get_RangeStartToActiveKey.Set
2. ACE_K_AES_*_GlobalRange_GenKey.Set
3. ACE_User1_Set_CommonName.Set
4. ACE_C_PIN_User1_Set_PIN.Set

The following table outlines additions/modifications to the AccessControl table to support the Global Range in Single User Mode.

1. *Policy0 – identifies that this access control association is present if the RangeStartRangeLengthPolicy parameter of the last Activate or Reactivate method was set to 0, indicating User1 has ownership over the Global Range's CommonName and LockOnReset columns.

2. *Policy1 – identifies that this access control association is present if the RangeStartRangeLengthPolicy parameter of the last Activate or Reactivate method was set to 1, indicating Admins has ownership over the Global Range's CommonName and LockOnReset columns.
### Table 14 Access Control Table Modifications for Global Range Single User Mode

<table>
<thead>
<tr>
<th>InvokingID</th>
<th>MethodID</th>
<th>CommonName</th>
<th>ACL</th>
<th>Log</th>
<th>GetACLACL</th>
<th>DeleteMethodACL</th>
<th>AddACEACL</th>
<th>RemoveACEACL</th>
<th>GetACLLog</th>
<th>DeleteMethodLog</th>
<th>LogTo</th>
</tr>
</thead>
<tbody>
<tr>
<td>User1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00 00 00 09</td>
<td>00 03 00 01</td>
<td>Informative only</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00 00 08 02</td>
<td>00 00 00 01</td>
<td>ACE_User1_Set_CommonName</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Locking_GlobalRange</td>
<td>Set</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00 00 08 02</td>
<td>00 00 00 01</td>
<td>ACE_Locking_GlobalRange_Set_CommonName</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00 00 08 02</td>
<td>00 00 00 01</td>
<td>ACE_Locking_GlobalRange_Set_CommonName</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Locking_GlobalRange</td>
<td>Set</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InvokingID</td>
<td>InvokingID Name</td>
<td>MethodID</td>
<td>CommonName</td>
<td>ACL</td>
<td>Log</td>
<td>AddACEACL</td>
<td>RemoveACEACL</td>
<td>GetACLACL</td>
<td>DeleteMethodACL</td>
<td>AddACELog</td>
<td>RemoveACELog</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>----------</td>
<td>------------</td>
<td>-----</td>
<td>-----</td>
<td>-----------</td>
<td>--------------</td>
<td>-----------</td>
<td>----------------</td>
<td>-----------</td>
<td>--------------</td>
</tr>
<tr>
<td>00 00 08 02</td>
<td>00 00 08 01</td>
<td>Locking_GlobalRange</td>
<td>Erase</td>
<td>ACE_Locking_GlobalRange_Erase</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00 00 08 08</td>
<td>00 04 30 00</td>
<td>ACE_Locking_GlobalRange_Erase</td>
<td>Set</td>
<td>ACE_ACE_Set_BooleanExpression</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00 00 08</td>
<td>00 03 00 01</td>
<td>C_PIN_User1</td>
<td>Get</td>
<td>ACE_C_PIN_Anybody_Get_NoPIN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.4.4.2.1.2 ACE Table Modifications

The following table outlines additions/modifications to the ACE table to support the Global Range in Single User Mode.

Notes:

1. *Modified – indicates this is an Opal-defined ACE whose BooleanExpr column value is modified by this Feature Set.
2. *New – indicates that this is an ACE defined by this Feature Set.

Table 15 New/Modified ACEs for Global Range Single User Mode

<table>
<thead>
<tr>
<th>UID</th>
<th>Name</th>
<th>CommonName</th>
<th>BooleanExpr</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 00 00 08</td>
<td>&quot;ACE_Locking_GlobalRange_Set_Read</td>
<td>User1</td>
<td>ReadLockEnabled, WriteLockEnabled, ReadLocked, WriteLocked, LockOnReset</td>
</tr>
<tr>
<td>00 04 00 00</td>
<td>&quot;ACE_Locking_GlobalRange_Set_LockEnabledToLOR*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00 00 00 08</td>
<td>&quot;ACE_Locking_GlobalRange_Get_RangeStartToActiveKey*</td>
<td>Anybody</td>
<td>RangeStart, RangeLength, ReadLockEnabled, WriteLockEnabled, ReadLocked, WriteLocked, LockOnReset, ActiveKey</td>
</tr>
<tr>
<td>00 00 00 08</td>
<td>&quot;ACE_C_PIN_Anybody_Get_NoPIN &quot;</td>
<td>Anybody</td>
<td>UID, CharSet, TryLimit, Tries, Persistence</td>
</tr>
<tr>
<td>00 00 00 08</td>
<td>&quot;ACE_C_PIN_User1_Set_PIN&quot;</td>
<td>User1</td>
<td>PIN</td>
</tr>
<tr>
<td>00 00 00 08</td>
<td>&quot;ACE_K_AES_*_GlobalRange_GenKey&quot;</td>
<td>User1</td>
<td>All</td>
</tr>
<tr>
<td>00 00 00 08</td>
<td>&quot;ACE_Locking_GlobalRange_Erase&quot;</td>
<td>Admins OR</td>
<td></td>
</tr>
<tr>
<td>00 04 30 00</td>
<td>&quot;ACE_User1_Set_CommonName&quot;</td>
<td>User1</td>
<td>CommonName</td>
</tr>
<tr>
<td>** **</td>
<td>** *** depends on AES key size</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.4.4.2.1.3 Authority Table Modifications

The following table outlines additions/modifications to the Authority table to support the Global Range in Single User Mode.
Table 16 Authority Table Modifications for Global Range Single User Mode

<table>
<thead>
<tr>
<th>UID</th>
<th>Name</th>
<th>IsClass</th>
<th>Class</th>
<th>Enabled</th>
<th>Secured</th>
<th>HashAndSign</th>
<th>PresentCertificate</th>
<th>Operation</th>
<th>Credential</th>
<th>ResponseSign</th>
<th>ResponseExch</th>
<th>ClockStart</th>
<th>ClockEnd</th>
<th>Limit</th>
<th>Uses</th>
<th>Log</th>
<th>LogTo</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 00 00 09</td>
<td>&quot;User1&quot;</td>
<td>F</td>
<td>T</td>
<td>None</td>
<td>None</td>
<td>F</td>
<td>None</td>
<td>Password</td>
<td>C_PIN_User1</td>
<td>Null</td>
<td>Null</td>
<td>ClockStart</td>
<td>ClockEnd</td>
<td>Limit</td>
<td>Uses</td>
<td>Log</td>
<td>LogTo</td>
</tr>
</tbody>
</table>

4.4.4.2.2 RangeNNNN in Single User Mode

The following subsections identify the additions/modifications to the settings defined in the Opal SSC if Locking RangeNNNN is identified in the Activate or Reactivate method as a Single User Mode range. See 4.4.1 for mapping of Ranges to Users.

4.4.4.2.2.1 AccessControl Table Modifications

For each Locking RangeNNNN in Single User Mode, the following access control associations in the AccessControl table are removed:

1. ACE_Locking_RangeNNNN_Get_RangeStartToActiveKey.Set
2. ACE_K_AES_*_RangeNNNN_GenKey.Set
3. ACE_UserNNNN+1_Set_CommonName.Set
4. ACE_C_PIN_UserNNNN+1_Set_PIN.Set

The following table outlines additions/modifications to the AccessControl table to support Locking RangeNNNN in Single User Mode.

1. *Policy0 – identifies that this access control association is present if the RangeStartRangeLengthPolicy parameter of the last Activate or Reactivate method was set to 0, indicating User1 has ownership over RangeNNNN's RangeStart, RangeLength, CommonName, and LockOnReset columns.

2. *Policy1 – identifies that this access control association is present if the RangeStartRangeLengthPolicy parameter of the last Activate or Reactivate method was set to 1, indicating Admins has ownership over RangeNNNN's RangeStart, RangeLength, CommonName, and LockOnReset columns.
<table>
<thead>
<tr>
<th>InvokingID</th>
<th>InvokingID Name - informative only</th>
<th>MethodID</th>
<th>CommonName</th>
<th>ACL</th>
<th>Log</th>
<th>AddACEACL</th>
<th>RemoveACEACL</th>
<th>GetACLEACL</th>
<th>DeleteMethodACLEACL</th>
<th>AddACELog</th>
<th>RemoveACELog</th>
<th>GetACLLog</th>
<th>DeleteMethodACLLog</th>
<th>LogTo</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 00 00 09</td>
<td>UserNNNN+1</td>
<td>Set</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00 03 00 00 (+NNNN+1)</td>
<td>00 03 00 00 (+NNNN+1)</td>
<td>Set</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AddACEACL</td>
<td>RemoveACEACL</td>
<td>GetACLEACL</td>
<td>DeleteMethodACLEACL</td>
<td>AddACELog</td>
<td>RemoveACELog</td>
</tr>
<tr>
<td>00 00 08 02</td>
<td>Locking_RangeNNNN</td>
<td>Set</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00 03 00 00 (+NN NN)</td>
<td>Policy1</td>
<td>Set</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InvokingID</td>
<td>MethodID</td>
<td>CommonName</td>
<td>ACL</td>
<td>Log</td>
<td>AddACEACL</td>
<td>RemoveACEACL</td>
<td>GetACLACL</td>
<td>DeleteMethodACL</td>
<td>AddACELog</td>
<td>RemoveACELog</td>
<td>GetACLLog</td>
<td>DeleteMethodLog</td>
<td>LogTo</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>------------</td>
<td>-----</td>
<td>-----</td>
<td>----------</td>
<td>--------------</td>
<td>-----------</td>
<td>----------------</td>
<td>----------</td>
<td>---------------</td>
<td>---------</td>
<td>-----------------</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td>00 00 00 08 00 04 30 01 +NNNN</td>
<td>ACE_Locking_RangeNNNN_Erase</td>
<td>Locking_RangeNNNN</td>
<td>Locking_RangeNNNN</td>
<td>+Policy0</td>
<td>InvokingID Name - informative only</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 4.4.4.2.2 ACE Table Modifications

The following table outlines additions/modifications to the ACE table to support Locking Range NNNN in Single User Mode.

**Notes:**

1. *Modified* – indicates this is an Opal-defined ACE whose BooleanExpr column value is modified by this Feature Set.
2. *New* – indicates that this is an ACE defined by this Feature Set.
3. *Policy0* – indicates that the ability to modify RangeStart and RangeLength is owned by the associated User authority.
4. *Policy1* – indicates that the ability to modify RangeStart and RangeLength is owned by the Admins class authority.

<table>
<thead>
<tr>
<th>InvokingID</th>
<th>InvokingID Name - informative only</th>
<th>MethodID</th>
<th>CommonName</th>
<th>ACL</th>
<th>Log</th>
<th>AddACEACL</th>
<th>RemoveACEACL</th>
<th>GetACLACL</th>
<th>DeleteMethodACL</th>
<th>AddACELog</th>
<th>RemoveACELog</th>
<th>GetACELog</th>
<th>DeleteMethodLog</th>
<th>LogTo</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 00 00 0B 00 03 00 00 (+NNNN+1)</td>
<td>C_PIN_UserNNNN+1</td>
<td>Get</td>
<td>ACE_C_PIN_Anybody_Get_NoPIN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th>UID</th>
<th>Name</th>
<th>CommonName</th>
<th>BooleanExpr</th>
<th>Columns</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 00 00 08 00 04 00 00 + NNNN *New</td>
<td>&quot;ACE_Locking_RangeNNNN_Set_ReadLockEnabledToLOR&quot;</td>
<td>UserNNNN+1</td>
<td>ReadLockEnabled, WriteLockEnabled, ReadLocked, WriteLocked, LockOnReset</td>
<td></td>
</tr>
<tr>
<td>00 00 00 08 00 04 10 00 + NNNN *Policy0 *New</td>
<td>&quot;ACE_Locking_RangeNNNN_Set_RangeStartToRangeLength&quot;</td>
<td>UserNNNN+1</td>
<td>RangeStart, RangeLength</td>
<td></td>
</tr>
<tr>
<td>00 00 00 08 00 04 10 00 + NNNN *Policy1 *New</td>
<td>&quot;ACE_Locking_RangeNNNN_Set_RangeStartToRangeLength&quot;</td>
<td>Admins</td>
<td>RangeStart, RangeLength</td>
<td></td>
</tr>
<tr>
<td>00 00 00 08 00 03 D0 00 (+NNNN) *Modified</td>
<td>&quot;ACE_Locking_RangeNNNN_Get_RangeStartToActiveKey&quot;</td>
<td>Anybody</td>
<td>RangeStart, RangeLength, ReadLockEnabled, WriteLockEnabled, ReadLocked, WriteLocked, LockOnReset, ActiveKey</td>
<td></td>
</tr>
<tr>
<td>00 00 00 08 00 04 20 00 *New</td>
<td>&quot;ACE_C_PIN_Anybody_Get_NoPIN &quot;</td>
<td>Anybody</td>
<td>UID, CharSet, TryLimit, Tries, Persistence</td>
<td></td>
</tr>
<tr>
<td>00 00 00 08 00 03 A8 00 (+NNNN) *Modified</td>
<td>&quot;ACE_C_PIN_UserNNNN+1_Set_PIN&quot;</td>
<td>UserNNNN+1</td>
<td>PIN</td>
<td></td>
</tr>
<tr>
<td>00 00 00 08 00 03 ** ** (+NNNN) *Modified</td>
<td>&quot;ACE_K_AES_*_RangeNNNN_GenKey&quot;</td>
<td>UserNNNN+1</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>00 00 00 08 00 04 30 00 +NNNN *New</td>
<td>&quot;ACE_Locking_RangeNNNN_Erase&quot;</td>
<td>Admins OR UserNNNN+1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00 00 00 08 00 04 40 00 +NNNN *Modified</td>
<td>ACE_UserNNNN+1_Set_CommonName</td>
<td>UserNNNN+1</td>
<td>CommonName</td>
<td></td>
</tr>
</tbody>
</table>

** ** depends on the AES key size
4.4.4.2.2.3 Authority Table Modifications

The following table outlines additions/modifications to the Authority table to support Locking Range NNNN in Single User Mode.

<table>
<thead>
<tr>
<th>UID</th>
<th>Name</th>
<th>IsClass</th>
<th>Class</th>
<th>Enabled</th>
<th>Secure</th>
<th>HashAndSign</th>
<th>PresentCertificate</th>
<th>Operation</th>
<th>Credential</th>
<th>ResponseSign</th>
<th>ResponseExch</th>
<th>ClockStart</th>
<th>ClockEnd</th>
<th>Limit</th>
<th>Uses</th>
<th>Log</th>
<th>LogTo</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 00 00 09</td>
<td>UserNNNN+1</td>
<td>F</td>
<td>T</td>
<td>None</td>
<td>None</td>
<td>F</td>
<td>Password</td>
<td>C_PIN_User1</td>
<td>Null</td>
<td>Null</td>
<td>Null</td>
<td>C_PIN_User1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00 03 00 00</td>
<td>(+NNNN+1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.5 Additional SPs

This feature set requires no additional SPs.